The London School of Economics and Political Science

Interception: Law, Media, and Techniques

Bernard Keenan

A thesis submitted to the Department of Law of the London School of Economics for the degree of Doctor of Philosophy, London, September 2017

Declaration

I certify that the thesis I have presented for examination for the MPhil/PhD degree of the London School of Economics and Political Science is solely my own work.

I warrant that this authorisation does not, to the best of my belief, infringe the rights of any third party.

I declare that my thesis consists of 99,962 words.

Abstract

In 2013, Edward Snowden provided journalists with copies of classified documents detailing the operations of the National Security Agency of the United States and its allies; in particular, the UK's Government Communications Headquarters. Snowden explained that he hoped to set the conditions for a new technical literacy that would alter understandings of the relationship between digital communications and law. This thesis asks whether or not law is capable of repaying Snowden's faith. To that end, it offers a media-theoretical genealogy of the interception of communication in the UK. Interception is presented as an effect of different sets of technical operations, mediated and processed by communication devices and networks. The thesis traces interception techniques: from their beginnings in the General Post Office; in their evolution through the operations of technical media; to their reappearance in the operations of digital media that constitute the internet. The authorisation of interception, meanwhile, has always depended upon legal techniques mediated by interception warrants. A genealogy of the interception warrant is presented through an archival study of the distinctly different practices of document production that manufactured and programmed warrants in different media epochs; from the medieval Chancery and paper bureaucracies of state institutions to the graphical user interface, which mediates between interception techniques and law today. Finally, the thesis addresses the function of legislation as it in turn addresses warrants and interception techniques. Law and legislation, it is argued, are incapable of constraining technical operations of interception because, like interception, law is already an effect of media-technical operations. The law operates not by controlling interception, but by processing it, assigning meaning to it, and protecting the secrecy of ongoing interception operations.

Acknowledgements

I submit this thesis precisely ten years since I moved to London to study a master's degree at the LSE. It is a good way to end a decade. My thesis supervisors, Alain Pottage and Conor Gearty, taught me that year on topics and theories that are central to this dissertation. Conor's advice and encouragement gave me the confidence to follow the files wherever they led. Alain patiently read and commented on countless drafts, some barely more than lists of documents, offering corrections, provocations, and drawing connections that would otherwise have been lost.

Andrew Murray and Orla Lynskey trusted me to teach their students about law and information systems. Without them, my understanding of digital media would never have advanced beyond the user interface. Rachel Yarham, Linda Mulcahy, and Susan Marks created an intellectual environment at LSE that encourages doctoral students to see themselves as academics-in-training rather than students. Laura Knöpfel, Alex Damianos, Ross McElwain, and Priya Gupta provided friendship, criticism, and detailed comments at vital moments. To all I am very grateful.

Thank you also to my parents.

Above all, Prudence Ivey's love and support made this possible.

1. Introduction

1.1 Technical literacy

> … we need to think of it in terms of literacy, because technology is a new system of communication, it's a new set of symbols that people have to intuitively understand. It's like something that you learn … just like how you learn to write letters in school. You've learned to use computers and how they interact, how they communicate. And technical literacy in our society is a rare and precious resource.[1]

In June 2013, *The Guardian* newspaper began publishing a series of articles based on documents provided by former intelligence contractor Edward Snowden. Similar reports soon appeared in other news outlets in the United States and Germany. All concerned the capabilities and activities of the National Security Agency of the United States (NSA) and allied organisations, particularly the United Kingdom's Government Communications Headquarters (GCHQ), in relation to the interception and exploitation of data derived from digital communication systems on a planetary scale.

Snowden's aim was to generate the conditions for a new technical literacy that would ultimately encode personal privacy and governmental accountability into law. The problem, as he saw it, was that all critical decisions regarding the agencies and their operations were taken in secret by senior civil servants, who because they "have been around longer than the furniture… feel [the agencies] can be trusted" to act in the public interest without public knowledge of their operations.[2] Bypassing these ineffective oversight regimes and organisational chains of command, he sought to provide citizens and legislatures with the material that would change the frame of reference regarding the relationship between law, governmental power and communication media. The first step towards improving the law regarding the

[1] Alan Rusbridger and Ewen MacAskill, 'Edward Snowden Interview - the Edited Transcript', ***The Guardian***, 18 July 2014, sec. World news, http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript.

[2] Ibid.

collection and use of information, as Snowden saw it, was to improve technical literacy so that people would better understand how digital media devices and networks are complicit in enabling governments to collect and analyse private data. Once they realised this, the public would demand changes to the law to make such powers accountable and transparent.

Hence he distributed the cache of documents he downloaded from NSA servers to journalists and news organisations in several countries, creating a network of mass media sources that could not be dismantled by targeting what network engineers call a SPOF, that is, a 'single point of failure'.[3] This did not discourage GCHQ from sending technicians to the offices of *The Guardian* to preside over the physical destruction of hard drives containing copies of the leaked materials in a demonstrative mode of governmental file erasure,[4] nor did it stop the police from detaining one journalist's partner under counter-terrorism laws in order to search his computer as he transited Heathrow airport.[5]

During the following three years, the news organisations that reported on the programs and systems described in the cache provided by Snowden published the relevant supporting documents their articles were based on. The material they have selected and published from the cache of documents came to constitute what we shall refer to as the 'Snowden archive'.[6] The documents are redacted where they mention names of officials or individual targets, mirroring the blacked-out aesthetic of many

[3] Ibid.

[4] Luke Harding, 'Footage Released of Guardian Editors Destroying Snowden Hard Drives', ***The Guardian***, 31 January 2014, sec. UK news, http://www.theguardian.com/uk-news/2014/jan/31/footage-released-guardian-editors-snowden-hard-drives-gchq.

[5] Subsequently his detention was ruled unlawful, Owen Bowcott, 'Terrorism Act Incompatible with Human Rights, Court Rules in David Miranda Case', ***The Guardian***, 19 January 2016, sec. World news, http://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case.

[6] There are several online databases that collect and index published documents, such as the collaboration between the Courage Foundation and Transparency Toolkit, 'Snowden Doc Search', https://search.edwardsnowden.com/, accessed 8 July 2017.

officially disclosed government materials. The Snowden archive teaches us about technical communication systems and legal oversight mechanisms, not people.

In technical terms, there was much to learn. For instance, a GCHQ system codenamed Tempora provides access to over two hundred international fibre optic cables, intercepted where they come ashore at relay points in Britain and Oman. In 2012, data from up to forty-six cables could be actively processed at once, each providing ten gigabytes of data per second, and plans were in place to grow those figures. Tempora grants GCHQ access to a significant proportion of global internet traffic, automatically analysed and processed into a searchable form. The semantic content of intercepted material is stored for three days, and the 'metadata' – the computer-generated data that enables digital communication to occur – is stored for thirty days.[7] The NSA and other state agencies in the 'Five-Eyes' alliance (comprising the US, UK, Canada, New Zealand, Australia) also conduct this type of 'upstream' data collection at selected sites around the world. Each partner provides access to the data to the others, forming a global network of cable interception points and satellite receiving stations. Developing access to communication systems is an ongoing "iterative process" that aims to

> discover, anticipate, and/or enhance exploitation of current and emerging foreign communications and non-communications systems… [creating a] growing network of discovery networks.[8]

Directly accessing data streams is not the only option. Computers and computer networks are targeted with software 'implants' that exfiltrate data over the internet. By 'hacking' into networks belonging to commercial companies, such as SIM card manufacturers and telecommunications providers, GCHQ have effectively turned

[7] Figures correct as of May 2012. See, 'Tempora - GCWiki Entry', ***Snowden Doc Search***, 21 May 2012, https://search.edwardsnowden.com/docs/TEMPORA2014-06-18nsadocs.

[8] SID today (NSA newsletter), 'SIGINT Development: A Network of Discovery Networks', ***Snowden Doc Search***, 11 June 2003, https://search.edwardsnowden.com/docs/SIGINTDevelopmentANetworkofDiscoveryNetworks2016-05-16nsadocs.

other networks into appendages of its own.[9] Such 'network exploitation' operations constituted straightforward criminal offences under English law: at the time that they were exposed, the law criminalising interference with computers contained no exemptions for government agencies. Parliament quickly moved to amend the Computer Misuse Act, inserting a clause that prohibits interference, except where it has been "authorised".[10]

We learned that the NSA and GCHQ collect 'bulk' datasets containing personal data and communication records relating to millions of citizens collected from around the world, including on their own populations, in order to analyse the content for patterns of potential interest.[11] Using such datasets, experiments attempting to train machine-learning systems to automatically recognise changing patterns of movement and communication began, with the ambition of implementing computer systems that automatically select which data will be of interest to intelligence analysts and filter out everything else.[12] Global internet platforms like Google, Apple, Microsoft and Yahoo were secretly collaborating with the NSA by providing direct access to their servers, in obedience to broadly-drafted warrants, under a program called Prism.[13] At the same time, the NSA was secretly targeting those same companies' inter-datacentre communication links in order to collect yet more data in unencrypted form.[14]

[9] Ryan Gallagher, 'The Inside Story of How British Spies Hacked Belgium's Largest Telco', ***The Intercept***, accessed 16 October 2016, https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/; Jeremy Scahill, 'Gemalto Doesn't Know What It Doesn't Know', ***The Intercept***, 25 February 2015, https://theintercept.com/2015/02/25/gemalto-doesnt-know-doesnt-know/.

[10] Section 10, 'Serious Crime Act 2015', accessed 28 January 2017, http://www.legislation.gov.uk/ukpga/2015/9/section/44/enacted; see also, 'After Legal Claim Filed against GCHQ Hacking, UK Government Rewrite Law to Permit GCHQ Hacking', ***Privacy International***, 15 May 2015, https://www.privacyinternational.org/node/584.

[11] See David Anderson, 'A Question of Trust: Report of the Investigatory Powers Review' (Stationery Office, 2015).

[12] 'HIMR Data Mining Research GCHQ Problem Book', ***Snowden Doc Search***, 20 September 2011, https://search.edwardsnowden.com/docs/HIMRDataMiningResearchProblemBook2016-02-02nsadocs.

[13] Glenn Greenwald, ***No Place to Hide*** (New York: Macmillan US, 2014), 108–9.

[14] Barton Gellman and Ashkan Soltani, 'NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say', ***Washington Post***, 30 October 2013, sec. National Security,

According to cyber security expert Susan Landau, the most startling revelation of all was that the NSA had compromised the functions of a random-bit generator called Dual EC-DRBG. The software had been awarded a security certificate by the US National Institute of Standards and Technology (NIST). This certificate served to confirm that the US government had confirmed that the software met established cryptographic standards.[15] As a result of the NSA's attack, the values produced by the random-bit generator were not truly random. A DRBG program works by generating a set of values derived algorithmically from an initial random 'seed' value. The 'seed' is a random because it depends on taking a momentary measurement of the physical state of the computer's hardware at the moment the program is executed. The measurement observes various factors that are changeable and contingent within the physical apparatus itself. It is a snapshot of an entropic state of part of the material universe, and therefore, as predicted by quantum theory, cannot be determined before or after the fact of measurement by any set of predictable, programmable operations.[16]

Once compromised, all cryptographic codes generated by the software could be decrypted by the NSA, which alone knew that the values were not truly random. The NSA knew the true range of possible values within which the key code must lie. The difference between a secure cryptographic key and a compromised one, in this context, is measured by the probability of successfully guessing the key. As Landau explains, this compromised the security of all communication systems that depend on the assumption that their data is securely encrypted through the affected software. By

https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

[15] Susan Landau, 'Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations', *IEEE Security Privacy* 12, no. 1 (January 2014): 63; see also Susan Landau, 'Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations', *IEEE Security Privacy* 11, no. 4 (July 2013): 54–63; Whitfield Diffie and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, Updated (Cambridge, Massachusetts: MIT Press, 2007).

[16] See Elaine Barker and John Kelsey, 'Recommendation for Random Number Generation Using Deterministic Random Bit Generators' (Computer Security Resource Center, 2012), 13–15, https://csrc.nist.gov/publications/detail/sp/800-90a/archive/2012-01-23.

attacking a random-bit generator, the NSA attacked the material foundations of digital security.

For Landau, this damaged trust in the government agencies charged with approving technical standards, and demonstrated that the Foreign Intelligence Surveillance Court (FISC), responsible for authorising and 'overseeing' the agency's operations, did not understand the full repercussions of the authority it had granted.[17] But we ought to consider the implications of the relationship between technical media and political trust in this scenario. Trust is required in relation to the randomness of cryptographic key values precisely because no human can determine the value for themselves, nor observe how the value was actually generated. As the operations of digital media are humanly imperceptible, society depends upon trust generated in how the operations of digital media are represented – in this case, as technical standards. Put the other way around, trust and security in digital communications ultimately depend on semantic devices, like certificated standards, which stand in for our inability to observe the operations of computer hardware. If one cannot take for granted that encryption keys are as random as they are claimed to be, then the risks of communication are suddenly and imperceptibly multiplied.

Snowden's revelations confirmed what has long been known to computer programmers but hidden from 'users'. Ever since commercial computers were created for the mass market, a distinction has been drawn between what users perceive to be taking place and what the machine is really doing. Users are assigned certain levels of access to the machine's programming, and permitted operations are typically represented by a 'graphical user interface' (GUI), and the user is encouraged to take control of the operations that have been designed for them. All possible operations have thus been determined in advance by the configuration of hardware and root programming that form the basic processing architecture of the machine. Thus, the conditions have long been in place for computers to do more things than what their users can perceive or control. Users enjoy a prescribed degree of choice, insofar as a

[17] Landau, 'Highlights from Making Sense of Snowden, Part II', 63.

device is used as intended by the proprietors of the intellectual property represented in the hardware and code. But this is very different from the full range of operations that are possible with a digital computer. Anyone who has the expertise or permission to access the higher commands of a computer can therefore "set conditions for communication that its users cannot even perceive".[18]

1.2 Stating the law

While the American Foreign Intelligence Surveillance Court attracted condemnation and legal challenges in the United States in the aftermath of Snowden's revelations,[19] in the UK, there was no such judicial target of ire. All applications for warrants to authorise interception activities of the police, intelligence agencies, and other government bodies are approved by government ministers. The official title is 'Secretary of State'. A judicial body called the Investigatory Powers Tribunal (IPT) can review *post facto* claims of unlawful use of interception powers, but does not make decisions about authorisation. As of the time of the first Snowden publications in 2013, the IPT had never ruled against the intelligence services.[20]

A brief chronological overview of the 'official version' of legal history of interception power in the UK helps set the scene. It can be divided into three broad periods: the secret use of the royal prerogative, legislative obfuscation, and, since 2016, a contested notion of legislative transparency.

1.2.1 Prerogative 1590-1985

One could reasonably begin with what may be the first attempt to rule on the general status of written communication in England: Elizabeth I's proclamation of 1590

[18] Cornelia Vismann and Markus Krajewski, 'Computer Juridisms', *Grey Room* 29 (2008): 96.

[19] Rainey Reitman, '3 Years Later, the Snowden Leaks Have Changed How the World Sees NSA Surveillance', *Electronic Frontier Foundation*, 5 June 2016, https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance.

[20] See Ewen MacAskill et al., 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications', *The Guardian*, 21 June 2013, sec. UK news, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa; under the Investigatory Powers Act 2016, a group of 'Judicial Commissioners' will be created to review authorisations by ministers before they are implemented, but they will not take any primary decisions.

prohibiting all but the Royal Messengers from carrying letters in or out of the realm. In 1635, the Royal Messengers were opened to the general public by proclamation of Charles Stuart. The newly formed 'Letter Office' held a monopoly over carrying all letters.

The first statute establishing the General Post Office (GPO) was passed in 1657, during the 'Long Parliament' of the 'Interregnum', that is, England's brief period without a monarch. The legislation expressly stated in its preamble that a prime reason for monopoly was to obtain intelligence about 'plots' against the Commonwealth. Although all law made during the interregnum was formally abolished on the Restoration of the Crown in 1660, the administration of the Post Office as stipulated in the Act was maintained by proclamation.

A statute of 1710 was the first to stipulate that no one could lawfully open or delay letters unless they did so under a warrant signed by a Secretary of State. Intercepted material was used for intelligence, but it was also presented as evidence in the prosecution of several treason cases. However, since 1795, intercepted material has not been ordinarily entered as evidence in criminal prosecutions in the UK. It appears to have been used in 'special commissions' regarding labour unrest in the nineteenth century, and a British national was convicted under the Official Secrets Act for aiding German spies in London prior to the First World War on the basis of intercepted letters, but as a matter of policy, the information gained from intercepting communication has remained a secret source of intelligence in its procurement and use.[21]

In the mid-nineteenth century, the question of legality was addressed clearly for the first time. In 1844, a political scandal involving the interception of letters of an Italian refugee, Giuseppe Mazzini. A parliamentary Secret Committee was convened to examine the legality of the practice, concluding that a power existed under the royal prerogative. Domestic interception practices continued within Britain, but the secret

[21] Under section 17 of RIPA 2000, no interception evidence can be used in legal proceedings, subject to limited exceptions.

branch of the Post Office that intercepted foreign diplomatic letters was disbanded following the Mazzini scandal.

The Telegraph Act 1868 created a state monopoly over telegraphy, placing it under control of the GPO. Legislation stipulated that no one could disclose the contents of a telegram from the Post Office save under the authority of a warrant. The Official Secrets Act 1920 required all commercial telegraph companies in the UK to grant the government access to their telegrams if ordered to do so, and to keep all such orders secret. Under this provision, all international telegrams were collected and analysed on a permanent basis.

The GPO issued licenses allowing private companies to establish telephone networks in Britain. Unlike letters and telegrams, telephone calls had no legal protection from interference. Existing private telephone networks were nationalised in 1910 under the GPO. Telephone interception, also known as 'line-tapping', was performed without the use of warrants until 1937, when they were created as a matter of policy. A scandal concerning telephone tapping led to the Birkett Report of October 1957. The report described broadly the procedures and processes in place for telephone interception. It agreed with the findings of the Secret Committee of 1844, in that it found that the legal grounds for intercepting letters and telegrams lay in the royal prerogative and that legislation on the Post Office had implicitly recognised this power; but the report expressed some doubt as to whether the prerogative could apply to new technologies like the telephone in the absence of legislation. The prerogative is regarded as a 'residue' of the pre-revolutionary model of monarchical sovereignty. Legal theory regarding the British constitution developed so as to exclude the creation of any new prerogative powers. New administrative powers could only come from Parliament, or the common law. Telephone tapping, which had never been considered by Parliamentary legislation or by judges, was on unsteady legal ground.

The legal lacuna regarding the interception of telephone calls and communication in general continued until 1978, when a police telephone 'tap' was accidentally revealed in court during a routine criminal prosecution. The target, a man named James

Malone, argued that the practice was illegal and took the police to court. In a controversial judgment, the High Court ruled that, as there was nothing in law that expressly prevented the police or GPO from tapping telephones, they were free to do so.

Malone took his case to the European Court of Human Rights in Strasbourg, which ruled that the absence of any legislative basis for interception meant the United Kingdom was in violation of article 8 of the European Convention on Human Rights. Article 8, amongst other things, guarantees the right to privacy. The Court held that where privacy is interfered with by a public authority, it must be on the basis of publicly available law. Under the Convention, privacy is a qualified human right, meaning that any interference must be only what is necessary in order to achieve a legitimate aim, involve measures that are proportionate to that legitimate aim, and there must be some 'effective' means of obtaining judicial remedy for any unlawful breach of these conditions. The crucial point in relation to the normativity of allowing states to exercise inherently secret powers concerns 'foreseeability'. Intercepting communication for police and security purposes must be conducted in secrecy to be effective, and the law recognises this: individual cases need not be disclosed in any specific sense in order to be lawful. But the law must give the public the capacity to 'foresee' the circumstances in which their privacy might be lawfully infringed upon as a result of secret interception practices. Legislation serves this function, and the degree of detail required of legislation in order to make things 'foreseeable' is then the second-order question to consider.

In 1985, having anticipated this outcome, the UK government proposed legislation. The Interception of Communications Act 1985 was passed by Parliament, ending the era of prerogative power and beginning the second phase; that of legislative obfuscation.

1.2.2 Obfuscation 1985 - 2016

The Interception of Communication Act 1985 (IoCA) and the subsequent Regulation of Investigatory Powers Act 2000 (RIPA) were carefully drafted to satisfy the requirements of human rights law while keeping the substance, extent, and techniques of interception powers ambiguous. They established a legislative source of power for interception warrants, ending the theoretical reliance on the powers inherent in the royal prerogative, but they did so using clauses that seem deliberately difficult to understand.

The Interception of Communication Act 1985 was the first in a series of legislative acts that brought the intelligence and domestic security services of the UK onto a public legislative footing. Although popular culture, whistle-blowers, defectors, and unofficial historians had long fuelled the mystique of the British secret services – the Security Service (domestic security, known as MI5), the Secret Intelligence Service (foreign espionage, known as MI6), and GCHQ – their activities had generally been theorised by government lawyers as emanations of the royal prerogative for the purposes of the law. Legislation was presented as bringing them 'in from the cold'.[22]

RIPA replaced the Interception of Communications Act 1985, updating it for the era of digital communications. For instance, it introduced a concept of 'communications data', differentiated from 'content'. Broadly speaking, this captures the difference between digital 'metadata', produced in the transmission and processing of digital data, and the semantic data delivered to human users. RIPA was a much longer piece of legislation than the minimalist and obscure IoCA; it is notoriously difficult to understand. Its high degree of abstraction served to ensure it was 'technology-neutral', in that it established general rules applicable across different forms of digital media. Nonetheless, it appears to have been drafted in such a manner that its effects when implemented cannot be discerned from the text.[23]

[22] The most comprehensive analysis of the legislation passed during this period is that of Laurence Lustgarten and Ian Leigh, *In From the Cold: National Security and Parliamentary Democracy* (Oxford: Oxford University Press, 1994).

[23] Sir David Omand, who was involved in the drafting of RIPA, has alluded to it being deliberately 'obfuscatory' at public events. However, the former legal director of GCHQ has stated that the capacities it authorises were obvious to anyone who read it closely, see 'Former GCHQ Legal Director: Journalists' Communications Not Considered in RIPA Drafting', *The Bureau of Investigative Journalism*, accessed 25 September 2017,

1.2.3 Transparency

The Snowden disclosures described capacities and activities that seemed to go beyond what was permissible under the terms of RIPA 2000. A number of legal challenges were brought before the Investigatory Powers Tribunal (IPT) by NGOs concerned with privacy and human rights issues.

In order to review matters that are considered official secrets, the IPT adopts a unique procedure. It first determines a hypothetical factual scenario that mirrors the alleged unlawful activities that it has been asked to adjudicate. Using these hypothetical 'assumed facts', which concern some violations of law or human rights, it considers legal arguments and arrives at a determination of the correct interpretation of the law, which is publicly promulgated. The Tribunal then conducts 'closed' hearings with the government's lawyers alone, excluding the public, the press, and the complainants, in order to determine whether or not the law has in fact been violated.

Over a series of hearings between 2014 and 2016, the meaning that GCHQ and the government assigned to RIPA and other legislation was elucidated. The UK government, realising that many GCHQ practices described in the published Snowden documents were not described at all in publicly-available law, began to issue information, variously described as 'codes', 'arrangements' and 'guidelines'. These documents acknowledged previously secret activities, such as hacking into computer networks, obtaining and processing bulk data sets, and sharing intercepted data with foreign governments. Where the published law and secondary documents could be read compatibly with assumed facts, however abstractly, the Tribunal found that the assumed facts would indeed constitute lawful operations. But where no legal provision could be found to cover the hypothetical activity, the Tribunal ruled against the government on the basis that any such activities (if carried out in fact, not fiction) would have been legally unforeseeable infringements of article 8. However, in those rare instances, it simultaneously ruled that disclosures of governmental documents

https://www.thebureauinvestigates.com/stories/2015-02-09/former-gchq-legal-director-journalists-communications-not-considered-in-ripa-drafting.

during the course of proceedings had served to make the activities foreseeable, remedying the illegality.

Having decided that RIPA was no longer 'fit for purpose', new legislation was proposed in November 2015.[24] The Investigatory Powers Act 2016 passed into law in November 2016. It is supposedly 'world-leading' legislation.[25] It explicitly lists the categories of operations that it permits, and provides details of procedures for making warrants and other modes of authorisations in relation to those operations. However, many privacy campaigners, technologists, and journalists regard it as a repressive law.[26] Amongst their complaints they regard the law as problematically maintaining official secrecy in relation to all authorised operations even when they have ended, and criticise the persistence of the Secretary of State's political control over 'investigatory' powers, rather than allowing for judicial authorisation. Moreover, the Act does not curtail or outlaw any of the activities described in the Snowden archive. On the contrary, it maintains them and expands them, creating a new power allowing the government to compel technology companies in the UK to secretly compromise their hardware or software security standards – returning us to the question of technical media standards.[27]

[24] 'Draft Investigatory Powers Bill', CM 9152 (2015), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf.

[25] According to the current Home Secretary, see, Matt Burgess, 'What Is the IP Act and How Will It Affect You?', ***WIRED UK***, accessed 19 September 2017, http://www.wired.co.uk/article/ip-bill-law-details-passed.

[26] 'UK Parliament Passes Most Extreme Surveillance Law in UK History', ***Privacy International***, accessed 19 September 2017, https://www.privacyinternational.org/node/1005; Sophie Armour, 'Liberty Gets Go-Ahead to Challenge Snoopers' Charter in the High Court', ***Liberty Human Rights***, 30 June 2016, https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/liberty-gets-go-ahead-challenge-snoopers%E2%80%99-charter-high-court.

[27] 'Open Rights Group - Home Office Consultation: Investigatory Powers (Technical Capability) Regulations 2017', ***Open Rights Group***, accessed 23 May 2017, https://www.openrightsgroup.org/ourwork/reports/home-office-consultation:-investigatory-powers-(technical-capability)-regulations-2017.

1.3 The question of surveillance

This brief survey of legally-defined interception powers in Britain points to an origin point for organised, state-based interception sometime around the seventeenth century. This comports with various histories of political power that identify that period with the emergence of modern systems of thought and modern techniques of political power. One of the central themes often associated with the period is the birth of surveillance powers, particularly in Michel Foucault's genealogy of power and knowledge. Surveillance offers a useful departure point for situating the legal history of interception in a wider theoretical context.

Surveillance lies at the heart of Foucault's genealogy of modern governmental power. Practices of organised observation were central to the development of the forms of knowledge that differentiate modernity from pre-modernity. In Foucault's account, modern human science began with practices of surveillance exercised within 'disciplinary' institutions; the enclosed places where the living bodies of prisoners, pupils, labourers, the sick, the mad, and the needy were confined and placed under observation. Putting life under observation allowed behavioural knowledge to be gathered, new categories to be defined, and 'normalising' disciplinary processes developed. Such knowledge took effect through specific techniques and practices that were intensively applied to the bodies and minds of confined subjects.[28]

In *Discipline and Punish*, Foucault treats Jeremy Bentham's 1795 proposal for a new type of prison called the panopticon as a diagrammatic form of the disciplinary institution. For Bentham, the panopticon was not merely an idea for a prison; it was to be adopted as a model for thinking about the governance of society in general. If the population felt themselves to be under observation, then they would discipline themselves without the need for physical intervention by adapting their behaviours to meet whatever normative criteria they assumed were being used to observe and evaluate them. In the panopticon, surveillance is presented as a generalised system for both changing subjects and measuring the change. It could be materialised in any

[28] Michel Foucault, *Discipline and Punish: The Birth of the Prison*, trans. Alan Sheridan (London: Penguin, 1991).

number of diverse settings, in order to achieve different functions. Bentham suggested schools, asylums, hospitals, and factories, but the 'diagram' can easily be identified elsewhere, not least in the ubiquitous technologies of observation that exist in the twenty-first century. In this broad sense, modern government was founded upon techniques of surveillance and measurement.

In Foucault's genealogy, the knowledge produced in disciplinary institutions migrated and coalesced into organised disciplines. Governmental knowledge and practices – or 'governmentality' – came about through the management of complex techniques of power that were applied to the population as a whole, based on the notion of 'political economy'. The nascent social and human sciences were developed in order to determine the correct order of things and to achieve that order. Governmentality manifested itself clearly in the discourse of 'security', through which the permanent institutions of administrative state took shape.[29] Knowledge came to be applied institutionally, not just on individuals. Practiced on paper and in files, it developed diverse aims and strategies, and over the course of the eighteenth century its institutional manifestations greatly intensified their operations.

Part of the originality of Foucault's account is that it excludes the notion of an oppressive state, which was how the absolutist governments of the eighteenth century had typically been viewed in liberal historiographical terms. It further excludes any sense of political economy as a driving force in history, as the standard Marxist account assumes. For Foucault, the very concept of state repression was itself something that needed to be explained. How did it become possible to speak of 'repressive' forms of political power? How did political economy come to be considered a science? Existing historical accounts were themselves effects of the kinds of knowledge-production that had to be explained. Foucault shows that the discourse of repressive forms of political power first emerged in the revolutionary discourse of the late eighteenth century, and the historical philosophies of the nineteenth century, when repression was assumed to have ended. Political history became possible only

[29] Michel Foucault, 'Governmentality', in ***Power***, by James D. Faubion, trans. Robert Hurley & Ors., vol. 3, Essential Works of Foucault 1954 - 1984 (London: Penguin, 2002), 219–22.

once the notion of the 'State' had precipitated as a description of a universal model or structure of political power. Only then could one write the history of a given state's particular development, as if the entity of 'state' had recently crystallised and existed in the present moment but had a long history. The very possibility of speaking about the form of such a trans-historical 'state' is in itself the precipitate of two particular "grids of intelligibility" that overlapped at the point at which both history and philosophy sought to enquire about the "agent of the universal".[30] The state, in short, is the outcome of transformations in power and knowledge that had been developed not through historical forces, but in localised sites of disciplinary power.

Throughout Foucault's genealogical research, power is always productive, never repressive – which is not to say it is normatively 'good', or that it generates no resistance. Productivity and resistance go hand in hand. Similarly, the development of governmentality is expressly differentiated in Foucault's work from accounts of government ruled by law. Although governmental strategies are expressed in legal instruments, elsewhere one finds other statements and arguments that explain how and why the law came to be used as an instrument towards certain ends. The law does not determine the techniques used in its execution, nor does it have the capacity to evaluate the outcomes of its application. Foucault is describing a mode of government that permeates and actively defines *all* areas of life. The 'biopolitical' mode of power includes 'law' as one amongst other strategic options at its disposal.

Legal rights, which posit a relationship between a sovereign source of political power and individual rights-bearing subjects, are themselves outcomes of other processes. Individual rights expressed in opposition to state security provide a discursive vehicle with which to calibrate the application of different governing techniques. They articulate very real struggles, but these struggles are multiple and diverse, and have very little in common with each other in terms of the specific question of application. Hence, while an immigration lawyer and a family lawyer might share an office and an interest in human rights law, they must operate according to vastly different sets

[30] Michel Foucault, ***Society Must Be Defended***, trans. David Macey (London: Penguin, 2003), 228, 237.

of knowledge and specialisation. Biopolitical governmentality regards 'freedom' as both a regulator and resource of very different practices. 'Freedom' is a term for many things. Hence nineteenth century liberalism

> is not acceptance of freedom; it proposes to manufacture it constantly, to arouse it and produce it, with, of course [the system] of constraints and the problems of cost raised by this production.[31]

Strategies of 'security' are also diverse; they manage the diverse production of freedoms. Governmentality is not repressive or historical, rather it is the art of maintaining production. This means managing contingencies by taking action to influence the action of others. Rather than a direct application of force, or confinement, or physical punishment, governmental strategies encourage and manage choices with the overarching aim of keeping the future both open and free of danger.[32] Everything governmental involves risks: markets, healthcare, education, agriculture, communication, and the continuation of government itself. Sir David Omand, a former Director of GCHQ, perfectly illustrates this when he writes,

> National security today should be defined as a state of trust on the part of the citizen that the risks to everyday life, whether from man-made threats or impersonal hazards, are being adequately managed to the extent that there is confidence that normal life can continue.[33]

The concept of national security can have no specific legal limitations simply because everyone is included in governmental grids of knowledge production. Agencies like GCHQ are institutionalised forms of contemporary modes of knowledge production.

[31] Michel Foucault, *The Birth of Biopolitics*, ed. Arnold I. Davidson, trans. Graham Burchell (Basingstoke; New York: Palgrave Macmillan, 2008), 65.

[32] Ibid., 65–66; Alain Pottage, 'Power as an Art of Contingency: Luhmann, Deleuze, Foucault', *Economy and Society* 27, no. 1 (1998): 1–27.

[33] David Omand, *Securing the State* (London: C Hurst & Co Publishers Ltd, 2012), 9; similarly, the head of the Security Service (MI5), addressing a parliamentary committee following the Snowden disclosures, stated, "The suggestion that what we do is somehow compromising freedom and democracy - of course we believe the opposite to be the case", 'We Defend Freedom - UK Spy Chiefs', *BBC News*, 7 November 2013, sec. UK Politics, http://www.bbc.co.uk/news/uk-politics-24847399.

Surveillance, then, is a general form by which government apprehends and manages risks concerning the subjects that it works on, rather than simply the act of recording or observing individuals against their will. If the fundamental problem for modern society's systems of understanding lies in folding the risks of the future into the operations of the present, then 'surveillance', as such, is ubiquitous.

1.3.1 Control society

Foucault's work shifts attention away from law and the state towards more diffuse notions of power and knowledge. One productive direction of enquiry has focused on the relationship between subjectivities and technology. Building on Foucault's foundation, Deleuze pointed out in 1990 that digital technology and the decline of heavy industry in western societies were transforming the ways that power operated on individuals, and how individuals operated on themselves. The old institutions which were the sites of disciplinary subject-formation – which had provided targets for resistance, like schools, psychiatric hospitals, prisons and factories – have been supplanted or augmented by diffuse, distributed modes of control that lack any single locus. Under such conditions, subjects also lack a single locus. Contemporary subjects distribute their competencies through overlapping networks and relationships, passing through various diffuse control points at which identities are checked and ordered. Labour, for instance, is no longer defined by skills so much as by time. Money and commodities are determined by financial economies that are not determined by the production and exchange of commodities. Institutions are no longer physically bound to buildings, but rather take effect through diffuse channels of communication.[34]

Deleuze's diagram of contemporary power works when thinking about modern surveillance technologies, particularly the deterritorialised, motivational, attention-hungry and ubiquitous systems of mobile information technology. Commercial, governmental, and security agencies use 'big' data to differentiate and regulate subjects, to encourage some behaviours and prohibit others, and encourages a new kind of economic freedom that turns bodies into reservoirs of mobile labour, tapped

[34] Gilles Deleuze, 'Postscript on the Societies of Control', *October* 59 (1992): 3–7.

into as and when required.[35] Theorists who build on the Deleuzian model of 'control society' assume that the panoptic gaze is outmoded now that surveillance is institutionally decentralised and energised by subjects' constant, enthusiastic observation of themselves.

The classic text in this regard delineates the concept of the 'surveillant assemblage', which

> … operates by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' which can be scrutinized and targeted for intervention.[36]

The Snowden archive confirms that much of the surveillance material produced by intercepting or attacking digital networks is essentially parasitic on such sources. The state institutions that produce intelligence from these resources do not own or operate the media that generate data, they use legal instruments to secure access to it. The notion of 'control society' has been deployed in several studies concerned directly or indirectly with surveillance.[37] It has inspired neologisms in the field of surveillance studies, many with minimal conceptual difference, such as 'dataveillance',

[35] Nick Couldry and Alison Powell, 'Big Data from the Bottom Up', *Big Data & Society* 1, no. 2 (2014).

[36] Kevin D. Haggerty and Richard V. Ericson, 'The Surveillant Assemblage', *British Journal of Sociology* 51, no. 4 (2000): 605–22.

[37] Michael Hardt and Antonio Negri, *Empire* (Cambridge, Mass: Harvard University Press, 2000), 197–98, 329–32, 384 For Hardt and Negri, sovereignty is expressed in coding, which distributes *dispositifs* via networks of capital; Deleuze's paper is the departure point for Galloway's thesis on protocols, Alexander R. Galloway, *Protocol: How Control Exists After Decentralization* (Cambridge, Massachusetts: MIT Press, 2006), 4–6; also see David Lyon, 'Everyday Surveillance: Personal Data and Social Classifications', *Information, Communication & Society* 5, no. 2 (January 2002): 254; Louise Amoore deploys the concept in examining how data analytics are used in diverse 'risk' calculations, tracking individuals and ordering interventions, and in no sense enclosed within institutions Louise Amoore, *The Politics of Possibility: Risk and Security Beyond Probability* (Durham: Duke University Press, 2013), 91; Mireille Hildebrandt extracts the concept of 'dividuals' in her account of Deleuzian theory, see Mireille Hildebrandt, 'Profile Transparency by Design?', in *Privacy, Due Process and the Computational Turn*, ed. Mireille Hildebrandt and Katja de Vries (London, New York: Routledge, 2013), 226; for a legal perspective on privacy rights see Julie E. Cohen, *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice* (New Haven: Yale University Press, 2012), chap. 6.

‘sousveillance’, and ‘coveillance’.[38] Academic models for naming various forms of so-called ‘participatory’ surveillance proliferate.

Such approaches run the risk of diminishing the specificity of surveillance practices that they take as their object. Some have the figure of the human lurking behind them, an implicit faith in some ‘lifeworld’ that needs to be recovered and protected.[39] This is not surprising, as the figure of the autonomous individual has long been the central figure in discourses that predate the emergence of the modern state. In relation to law and normativity, the figure of the individual continues to occupy the highest symbolic position. It is an organising principle that is both difficult and undesirable to do away with. But it lacks explanatory power.[40]

Snowden’s call for technical literacy can, however, be taken as a provocation in another direction. It may be productive to materialise ‘surveillance’ by not assuming it in advance. Instead, we return to the specific techniques that produce it in the first place. Rather than drawing increasingly remote connections between subjects and the ‘data’ that is produced about them, we turn to media.

1.3.2 Media theory

In order to read and write, one must learn the techniques required to coordinate paper, pen, eye, and text according to the protocols of text-production. From the perspective

[38] Couldry and Powell, ‘Big Data From the Bottom Up’; Karl Palmås, ‘Inauthentically Intense: Coveillance and Consumer Culture among Speedsurfers’, ***Surveillance & Society*** 13, no. 3/4 (2015): 487–496; Vian Bakir, ***Torture, Intelligence and Sousveillance in the War on Terror: Agenda-Building Struggles*** (Farnham, Surrey: Ashgate Publishing Limited, 2013); Randy Lippert and David Wood, ‘The New Urban Surveillance: Technology, Mobility, and Diversity in 21st Century Cities’, ***Surveillance & Society*** 9, no. 3 (2012): 257–262.

[39] Christian Fuchs criticises the use of abstractions, and at the same time argues for a return to Habermas, Adorno and Marx, which does not necessarily escape the problem, see Christian Fuchs, ‘Surveillance and Critical Theory’, ***Media and Communication*** 3, no. 2 (30 September 2015): 6–9; Christian Fuchs, ***Critical Theory of Communication: New Readings of Lukács, Adorno, Marcuse, Honneth and Habermas in the Age of the Internet*** (London: University of Westminster Press, 2016).

[40] W. T. Murphy, *The Oldest Social Science? Configurations of Law and Modernity*, (Oxford: Clarendon Press, 1997), 213–20.

of this basic observation, any suggestion of 'technical literacy' appears paradoxical, because literacy is already technical. It is a consequence of technical operations.

As Foucault's genealogy of power shows, law has never referred to technical governmental operations directly. Rather, it abstractly describes different practices, outcomes, decision-making procedures, and modes of knowledge in legal terms. Media, however, operate differently. They do not simply operate within culture or context, they generate the possibility of culture and context. Media establish the conditions upon which things can be communicated. Media are not tools of subjective will, but the condition of possibility that enables the idea of subjective will to be applied to different processes and techniques.

The point can be elaborated in Friedrich Kittler's discussion of Foucault's archaeological method. Before his genealogical work on the *dispositifs* of political power, Foucault's work took discrete epochs and explored their epistemic conditions of possibility. The 'archaeology' of knowledge meant situating texts, documents, and other statements within the regime of discourse that made them sayable in a given era. Foucault focused not on the content of texts and the validity of the ideas they presented, but their facticity, treating them as 'monuments' whose very existence was the thing that needed to be explained. Foucault the archaeologist does not interpret meaning, discuss allegorical lessons, identify authorial intentions, desires, or find the 'truth' behind a statement. He does not seek to arrange ideas in a progressive history such that one can appear to lead inexorably to the next.[41] Instead he seeks the material residue of a particular order of discourse that made particular statements possible. This he called an *episteme*, that is, "something like a world-view, a slice of history common to all branches of knowledge".[42]

The description of any given *épistème* is necessarily partial and non-exhaustive. It is not a complete recovery of all the techniques and all the attitudes or limitations that

[41] Michel Foucault, *The Archaeology of Knowledge*, trans. A.M. Sheridan Smith, 2nd edition (London, New York: Routledge, 2002), 155–56.

[42] Ibid., 211.

existed. It does not assess whether or not a particular form of knowledge was true or false, but asks what made it possible to think it was true. And it rejects utterly the suggestion that knowledge or legitimacy were ever originally founded on some transcendental act or substance: everything emerges from processes.[43] Hence one can identify the regularity of linguistically identical or logically equivalent statements over time, and identify moments where functionally comparable statements change across different networks of meaning; networks which Foucault sometimes names *dispositifs*. In short, archaeology is about identifying *how* things became visible, doable, thinkable, but not *why*.

For Kittler, Foucault's 'archives' were primarily libraries. This implicitly "designates a historical a priori of written sentences… [Hence] Foucault's research did not progress much beyond 1850."[44] Foucault overlooked the fact that the networks of information transfer that enabled the discursive knowledge regimes he studied were conditioned by the use of paper media and textual forms of storage. His studies did not account for the transformations in knowledge and power that followed the shift away from textual modes of communication to technical modes, when data replaced sentences and transmission and calculation became automated. Writing is the residue of particular techniques performed in a particular *dispositif,* or, in Kittler's term, *discourse network*,[45] that is, "the network of technologies and institutions that allow a given culture to select, store and process relevant data".[46] This means that shifts in media technologies present epistemological separations between different media-defined epochs.

1.3.3 From text to technics

"Media determine our situation", according to the preface to *Gramophone, Film, Typewriter*, which is to say that media actualise the epistemological horizon against

[43] Ibid., 74–75.

[44] Friedrich A. Kittler, *Discourse Networks 1800/1900* (Stanford: Stanford University Press, 1992), 369.

[45] Geoffrey Winthrop-Young, *Kittler and the Media*, (Cambridge: Polity, 2013), 59.

[46] Kittler, *Discourse Networks 1800/1900*, 369.

which the world is revealed to knowledge.[47] To understand how discourse changed after 1850, one must foreground the medial a priori, the changing technical conditions, switches and relays, circuits, hardware, software, and standard routines that define and activate technical media. Kittler began by re-reading literature and philosophy as a text-based machine that processed information. World history thereby became the history of communication media systems, which made the epistemological assumptions of idealist philosophers redundant in three ways. The three critical differences derive from the abstract technical functions of information systems as described Claude Shannon and Warren Weaver's mathematical theory of information systems: transmission, storage, and processing.[48]

First, the discourse networks of written communication that had relied on pen and paper gave way to new *storage* technologies. Whereas writing required that all information "pass through the bottleneck of the signifier",[49] the electrical, mechanical, and chemical technical media that defined the early twentieth century responded to real physical information and stored it in analogue imprints. Film stored light in a form that permitted cinema to emerge as the imaginary reconstruction of continuously moving optics, changing how perception was perceived; gramophones captured the meaningless noise that is the reality of sound, noise upon which meaning is inscribed as a psychological operation; and typewriters transformed writing from fluid continuous handwritten script connected to the immediacy of voice and the soul into discrete mechanical selections, punched out from a finite order of interchangeable symbols. Second, new technical *transmission* systems were developed that required the translation of information into discrete coded formats, and thereby remade the notion of 'true' knowledge into a calculable physical form called 'information', distinguishable from whatever meaning is assigned to it. Third, the coding required to transfer information ultimately led to the emergence of

[47] The 'revealing' appears in direct reference to Heidegger in Kittler's later works, see Friedrich Kittler, 'Towards an Ontology of Media', *Theory, Culture & Society* 26, no. 2–3 (1 March 2009): 23–31.

[48] Claude E. Shannon, 'A Mathematical Theory of Communication', *The Bell System Technical Journal* 27, no. July (1948): 379–423.

[49] Friedrich A. Kittler, *Gramophone, Film, Typewriter*, trans. Geoffrey Winthrop-Young (Stanford: Stanford University Press, 1999), 4.

programmable computers, which could simulate the operations of all media systems by making it possible to *process* information – and therefore knowledge – as discrete binary digital differences, thereby making it physically possible for digital media to simulate any other medium or network or, indeed, any human. Thus ended the era of "so-called Man".[50]

In order to apply Kittler's method, three steps are required. First, all communication systems are considered as information transfer systems. Information, therefore, is not understood phenomenologically but rather materially. There is a data source, but data has no inherent meaning; as such, it is not observer-dependent. It generates information, which is the physical measure of the capacity for surprise, that is, the mathematical ratio between novelty and redundancy in a transmission. What matters is the reproduction of information at the destination, overcoming any noise generated by interference in the material transmission channel. Communication, then, is simply the physical transmission of commands in an information system.[51]

The second step is to de-anthropomorphise everything. Kittler's universe is ontologically grounded in discrete states of information and entropy. People – 'so-called Man' – have no say. They can act as 'senders' when they act as an interface between data and a channel, such as when a person writes a letter or keys out a Morse code telegram. But this is not a 'human' operation, it is a technique determined by the medium in question. Subjects are materially defined by how they interface with particular technical media and functionally reduced to addressees of the commands of information systems. In other words, the subject's function is to process commands, i.e., to process information. The human mind, for instance, is simply the effect of an organic information processor, nothing more. The only significance of individuals for

[50] Ibid., 243.

[51] Friedrich Kittler, ***Optical Media***, trans. Anthony Enns (Cambridge: Polity, 2010), 46; Bernhard Siegert, 'Media After Media', in ***Media After Kittler***, ed. Eleni Ikoniadou and Scott Wilson (London, New York: Rowman & Littlefield International, 2015), 83–84.

Kittler is that they process information and thereby enable the further transmission and processing of information.[52]

The third step: convert all physical elements into information storage devices. All physical materials are reducible to storage media, viewed as data points in networks of information exchange.

> [As] data give rise to the operation of recording, addresses give rise to the operation of transmission, and commands give rise to the operations of processing, every system of communication that consists of these three operations can be analysed as a system of information.[53]

Kittler's radically de-anthropomorphised framework enables him to read the latent impact of changes in the technical conditions produced by media, captured in engineering terms as *standards*, into the literature, art, and culture of Euro-American modernity.

What are media? Media are anything that perform these three operations.

1.3.4 The end of media

The Snowden revelations may have realised one of Kittler's more apocalyptic prophecies. In 1990, Kittler wrote:

> 0.1 percent of all telecommunications on this planet are absorbed by the NSA's artificial intelligence. What then happens with them, no one knows. As a rule, orders for secrecy are lifted only after thirty years. Perhaps they will no longer be necessary at all three decades from now. The Word that was in the Beginning is vanishing into computer data banks... When all that is said by the inhabitants of the earth has disintegrated into bits, Alan Turing's Universal Discrete Machine will be perfected.[54]

[52] Kittler, *Optical Media*, 43–46.

[53] Siegert, 'Media After Media', 83–84.

[54] Friedrich A. Kittler, 'The Artificial Intelligence of World War: Alan Turing', in *The Truth of the Technological World*, trans. Erik Butler (Stanford: Stanford University Press, 2013), 194.

Computer technology has been subject to state secrecy since it was invented.[55] The cutting edge of computational power has always been reserved for cryptological work. Now that the internet has connected so many subjects – human and non-human – and has exponentially increased the volume of information being processed, the Snowden disclosures of 2013 confirmed what many had already suspected: the default assumption today should be that communication operations are all potentially intercepted, and that as media evolve in complexity, they expand the volume of information they process. Today, digital media are designed to constantly reveal more about users than users know about themselves. In 1990, Kittler knew that the NSA had, by then,

> intercepted telephony, telegraphy, and microwaves… its computers have deciphered messages that are potentially coded, scrambled, and so on, stored the transmissions automatically, and trawled through them (just as automatically) for suspicious keywords.[56]

Today, the NSA and its allied partner agencies are actively and aggressively expanding the scope of their interception, storage, and analysis of world communications, adopting a general strategy of "boundlessness".[57] In combination, the effect is that all users, and therefore all subjects of communication, are potentially enmeshed within the NSA/GCHQ databases that are processing 'real-time' analyses of as much data as can be usefully processed.

Perhaps the thing that makes Kittler's work so compelling, so controversial, and so unrepeatable is his dedication to the implications. For Kittler, the critical step in the evolution of media was the final step, the realisation of the digital computer. It is most frequently discussed in his work by reference to Alan Turing's universal discrete

[55] As exemplified by the challenges faced by Turing's biographer in describing the first computers forty years on, Andrew Hodges, *Alan Turing: The Enigma* (London: Vintage, 1992), x–xi.

[56] Kittler, 'Alan Turing', 193.

[57] SID today (NSA newsletter), 'Chef's Choice: SIGINT and the Question of Governance', *The Intercept*, 5 May 2004, https://theintercept.com/snowden-sidtoday/.

machine, as described hypothetically in a paper written in 1936.[58] Turing proposed a hypothetical machine that could perform a set of discrete read/write/erase operations according to a programmable set of instructions. The machine would be able to cycle through all possible computational operations in order to demonstrate that there are natural numbers that cannot be algorithmically computed. In proposing a solution to an abstract problem in mathematical logic, Turing simultaneously demonstrated a mechanism that could digitally compute everything that can be computed. In turn, this formed the basis for the realisation of programmable computers, beginning with Colossus, which was used to decode German cryptographic systems in the Second World War.

For Kittler, in his more radical texts, Turing's thought experiment put the writing on the wall (so to speak) for media. It demonstrated that data processing bypassed text, bypassed authorship, and bypassed government, existing as "unreadable series of numbers circulating between networked computers."[59] If all media do is offer an interface for the discrete operations of physical data processing, then anything that a physical medium can do can be done by the universal discrete machine. It is the medium that can become all others, and it therefore supersedes them. Its operations make all other media redundant except as simulated interfaces that append humans to their operations.

> Much like impoverished aristocrats who now work as tourist guides on their former estates, media are no longer located at the crucial intersection of physical processes and the human sensory apparatus; they have been moved to the margin of the digital machine in order to allow humans some access to this self-contained numerical universe.[60]

Moreover, if all that defines a 'subject' is the capacity to process information, then computers are subjects just as humans are. The capacity to decide on how to articulate a particular process is what counts.

[58] Alan Mathison Turing, 'On Computable Numbers, with an Application to the *Entscheidungsproblem*', *Journal of Math* 58, no. 345–363 (1936): 5.

[59] Kittler, *Gramophone, Film, Typewriter*, xxxix.

[60] Winthrop-Young, *Kittler and the Media*, 75.

> The consequence for the analysis of power systems—the vast task bequeathed to us by Foucault—is twofold. For one, one should no longer seek to understand power, as conventionally happens, as a function of so-called society; instead, and conversely, one should seek to reconstruct sociology from chip design [*Chiparchitekturen*] up.[61]

Kittler's point is not that media predetermine everything that happens in human society. He is not a techno-determinist. Rather, media predetermine the conditions of human perception, including subjective self-perception. The human-machine interfaces that we interact with each day are imaginary simplifications of real operations that are beyond the limits of human cognitive processing. Human subjectivity is conditioned by media standards, which determine the inputs available to the mind. The only tasks left for humans in the digital age involve processing information into machine-readable form, using coding languages and software that exist only to assist this interface process, and to hide the computational processes behind other human/machine interfaces.[62] Once information processing power is located within silicon media, no one can 'observe' it at all, but must rely on lines of code language, or a graphical user interface that simulates a 'desktop'. The locus of power is contained wholly within the media themselves. And this, inevitably, presents problems for any theory of society.

1.3.5 Cultural techniques

As a methodological framework, Kittler's theory has limitations, not least the distance it takes from any attempt to account for social developments in an empirical manner. Kittler's self-conscious style results in occasionally incorrect or one-dimensional statements concerning history, politics, and gender. These problems seem to stem from his professed disinterest in the role of observation and meaning in relation to 'successful' communication, even though those issues were never eliminated from mathematical information theory quite as completely as Kittler would have us

[61] Friedrich A. Kittler, 'Protected Mode', in *The Truth of the Technological World*, trans. Erik Butler (Stanford: Stanford University Press, 2013), 214.

[62] Kittler, 'Alan Turing', 223.

believe.[63] According to Gumbrecht, Kittler himself eventually found his "cold diagnosis" to be "intolerably burdensome".[64] Most importantly, by declaring society redundant, it threatens to close down precisely what was originally so provocative about the concept of a discourse network. As Geoffrey Winthrop-Young puts it, Kittler's apocalyptic certainty "smacks far less of technologized Foucault than of an updated Hegel; it is a hidden grand narrative."[65]

For Siegert, Kittler's media-ontology that displaces observation amounts to a way of thinking about "operative ontologies". This implies a mode of enquiry which

> asks for the concrete ontic operations and practices that produce first of all ontological distinctions—among many others also those between image and picture or figure and ground or active and passive or message and medium, subject and object, man and animal and so on. These ontic operations are called cultural techniques.[66]

Presented by Siegert in terms borrowed from Actor-Network Theory, cultural techniques address "the objectity of the objects". This way, media can be placed "at the core of entities formerly known as objects and humans and which are now much better addressed as processes of assemblage".[67] As Vismann puts it, cultural techniques "describe what media do, what they produce, and what kinds of actions they prompt."[68]

[63] Winthrop-Young elaborates these critiques, and offers some responses. Winthrop-Young, ***Kittler and the Media***, 121–38; Questions of perception, induction, and evaluation may be taken to imply a more complex evolutionary mode of processing that would re-inscribe the social, or the biological, into the evolutionary processes of information complexity. Of course, these theories are conditioned by digital media, hence Kittler's original thesis still stands, but his prognosis may not, see for a basic primer, James Gleick, ***The Information*** (London: Fourth Estate, 2012), 324–55.

[64] Hans Ulrich Gumbrecht, 'Media History as the Event of Truth: On the Singularity of Friedrich A. Kittler's Works', in ***The Truth of the Technological World***, trans. Erik Butler (Stanford: Stanford University Press, 2013), 319.

[65] Winthrop-Young, ***Kittler and the Media***, 65.

[66] Siegert, 'Media After Media', 87.

[67] Ibid.

[68] Cornelia Vismann, 'Cultural Techniques and Sovereignty', ***Theory, Culture & Society*** 30, no. 6 (1 November 2013): 83.

In one sense, this was Kittler's project all along. *Gramophone, Film, Typewriter* "collects, comments upon, and relays passages and texts that show how the novelty of technological media inscribed itself into the old paper of books."[69] Kittler may have regarded literature as defunct, but his aim was to explain how media had made it so. The point is not to describe what media *are* but to show what they *do*.[70] Kittler's legacy is in placing the singular materiality of technology at the centre of things, as the means of apprehending all that can be apprehended.[71]

Applied to 'interception', it becomes nothing more than the execution of a 'conditional jump', i.e., an IF-THEN logical step. For Kittler, this is the ultimate definition of subjectivity, whether human or machine: a subject is simply that which can respond to conditional commands.[72] The medium processes information by assigning information to channels, but IF there is an interception selector identified, THEN the data concerned is transferred into an interception process, where it is copied and transmitted onwards for further processing. The question then turns to the medium that executes the 'conditional jump'. Kittler, drawing a parallel with Carl Schmitt's observation that in a bureaucracy, sovereign power is hidden in corridors and locked offices – "power amounts to its conditions of access", described the architecture of modern computers as if the computer were a state.[73] As in a bureaucracy, the power to make certain IF-THEN commands is located at sites of privileged access. Computer architecture prevents ordinary users from accessing the protected levels of root command code, hence ordinary users are never sovereign in respect of their machines. If media sovereignty is defined by unconditional access to information processing, then sovereignty must be located at the point where all processing decisions are possible and all information is made visible. Those points, in any medium, are where interception of that medium can occur.

[69] Kittler, *Gramophone, Film, Typewriter*, xl.

[70] The distinction and its relationship to western philosophy is clearly expressed in Kittler, 'Towards an Ontology of Media'.

[71] Gumbrecht, 'Media History as the Event of Truth: On the Singularity of Friedrich A. Kittler's Works', 325–29.

[72] Kittler, *Gramophone, Film, Typewriter*, 258–60.

[73] Kittler, 'Protected Mode', 213.

1.4 Method, structure, and sources

This thesis elucidates the nexus between interception techniques and law. In focusing upon interception, we specifically exclude other surveillance techniques related to the interception of communication, such as hidden microphones, aerial, satellite, and drone reconnaissance, CCTV, telephotography, the use of hidden tracking devices, and so on. Similarly, the purposive uses of intercepted data are mostly excluded and discussed only to the extent that they inform particular technical developments. In practice, military, governmental, and police intelligence services combine information derived from multiple sources, but that is beyond the scope of this investigation.[74] This methodological choice is by no means intended to exhaust the notion of 'surveillance'; rather, it is intended to suspend it.

The history of modern communications surveillance is itself an effect of ascription that covers a wide range of practices. Interception techniques gain their continuity from particular ways of defining certain operations of media. As operations, they operationalise capacities of media to transmit, store, and process information. That they can be repeated and replicated gives them continuity, and this makes possible the historiographical claim that governmental surveillance has 'continued' since the seventeenth century, despite radically different media. From the point of view of techniques, such claims of historical continuity are themselves manifestations of historiographical techniques, which assemble textual media into chronological order and produce a particular grid of temporal intelligibility. They are no more 'real' than other technical approaches to information.

The focus on 'techniques' is not made with reference to human subjects performing interception, but to the ways that media determine the possibility of processing information in transit between two symbolic poles, the sender(s) and receiver(s). Interception techniques are independent of individual actors, and this independence is precisely what makes them reproducible across time and space. As Vismann has it,

[74] Guides to understanding analytical techniques used in state intelligence agencies include Michael Herman, *Intelligence Power in Peace and War* (Cambridge University Press, 1996); and Omand, *Securing the State*.

focusing on media and the cultural techniques rather than on human subjects and wilful agency means:

> One must therefore draw a distinction between persons, who *de jure* act autonomously, and cultural techniques, which *de facto* determine the entire course of action. To inquire about cultural techniques is not to ask about feasibility, success, chances and risks of certain innovations and inventions in the domain of the subject. Instead, it is to ask about the self-management or auto-praxis [*Eigenpraxis*] of media and things, which determines the scope of the subject's field of action.[75]

This vision of the self-management of communication media claims that media arrange and condition the basic tasks of ordering time, space, and information that, in combination, are described as the interception of communication. For instance, in the postal age the delay between communication being transmitted and intelligence being produced was an order of days, in digital environments it is a matter of seconds. In both scenarios, however, interception occurs in the time defined by operations of transmission and operations of delivery. Media function to establish different "notions of duration, assign origins, and secure the future".[76] Humans and non-humans are equally capable of performing media-technical operations, the point is that they do so only according to the conditions of the medium.

As an operationally secret practice, interception has always been deliberately subjected to obscurantism and censorship. The law itself has been involved in this process. Because of this, this research work is constrained in large part by the contingent archival traces, secondary sources, and contemporary materials that are available. This necessarily entails a forensic approach, assembling heterodox materials in order to produce a genealogy of a *dispositif* of interfaced systems and the ways they have interfaced: interception and law.

[75] Vismann, 'Cultural Techniques and Sovereignty', 84.

[76] Ibid., 10.

1.4.1 The question

The thesis takes Snowden's statement as its point of departure: can technical literacy produce laws that control interception? The thesis is arranged as follows:

1.4.2 Chapter two: Letter interception in the postal epoch

We begin with the emergence of personalised letter-writing as the medial precondition for the discourse networks that mark out an epochal shift between the medieval and modern. The form of medieval letter production is contrasted with the forms that emerged in the early modern period. To master the techniques of letter production was to enter into written discourse, transforming subjects into senders and receivers of correspondence, and attributing to them a new dimension of epistolary subjectivity. Postal networks can be read as manifestations of political power structures, and in this respect the formation of the Post Office can be linked to the shift from a medieval society defined by overarching sovereign unity, to a society centred on the modern political subject, whose discourse must be disciplined and made subject to inspection under new regimes of disciplinary power.

Foucault's broadly-defined genealogy of power as it evolved from disciplinary institutions to biopolitical governmentality is used as a methodological infrastructure.[77] Interception first takes on organised forms under conditions of civil war, gaining information on plotters at home and enemies abroad. It was performed by a small group of men who derived their resources from the labour performed by postal workers, who themselves were placed under constant disciplinary supervision in order to perform the sorting operations required to produce and maintain an ordered flow of letters through the office. This way the Post Office generated connections between all senders and all receivers, providing an observable media-technical infrastructure for the development of discourse networks.

In the eighteenth century, the Post Office expanded the scope and intensity of its operations. Interception practices became professionally organised within the Post

[77] Foucault, 'Governmentality'.

Office, but the surveillance of senders and receivers extended also into the duties of ordinary postal workers. Interception was an integral part of the larger machinery of governmental knowledge-production, which was in general ordered and channelled by the Post Office.

In the nineteenth century, interception became less of an organisationally secret activity and more of a formally secret policy. The Post Office was reorganised in a manner that converted it from a corrupt and economically dysfunctional extension of political power into a self-regulating machine that responded only to its own logical procedures, which were most clearly manifested through reconfigurations of postage and addressing systems. Once postal operations were differentiated from the explicit exercise of political power, interception could no longer be considered an inherent reason for the Post Office's existence. New normative justifications and procedures were required for the practice to continue, manifesting the calculus of 'liberty' and 'security' that Foucault identified with 'biopower' in the nineteenth century. A secret parliamentary report prepared in 1844 offers the earliest history of letter interception in England, provides details of its administrative context, and at the same time stands as a monument to the changing governmental practices of the period. Only then did it become important to discuss how records were assessed and stored, and how recorded procedural practices had to be indexed to normative ends.

We end with a brief account of interception in the twentieth century, with a focus on the techniques that emerged during conditions of war. Of the few available accounts of professionalised letter interception, they tend to highlight the detection – or attempted detection – of non-discursive media hidden within letters, rather than straightforward text-based letters themselves. Interceptors were required to seek out technical storage media designed to disguise themselves as ordinary letters, anticipating and evading interception. The letter itself was a ruse, a simulation of a discursive form, designed as camouflage for technical media that could carry both discursive and non-discursive forms of information to their addressees.

In each of these eras, interception remained centred upon reconfigurations of the same privileged location: the sorting-room.

In addition to Foucault's genealogy of power, this chapter is theoretically indebted to Bernhard Siegert's media genealogy of postal systems.[78] In terms of empirical resources, the chapter draws primarily from secondary historiographical sources. As the thesis demonstrates, there are relatively few documents associated with interception practices that have survived today. The vast majority were apparently destroyed, partially because archiving did not emerge as an organised governmental practice until the nineteenth century, and partly in order to eliminate traces of events and practices that were inherently secret. The Royal Mail Archive, which holds meticulously catalogued records demonstrating the financial and administrative history of the Post Office, contains no information whatsoever on the interception of communication. However, there are a number of historical works on the history of the Post Office, the history of state intelligence in Britain, the history of the Civil War, the Interregnum and Restoration governments, and the history of the offices of the British state that have made it possible to present outlines both of interception practices and of the procedures through which they were directed. These have been invaluable, especially as the author does not have the specialised skills required to discern the handwritten scripts used by letter writers of the seventeenth and early eighteenth centuries. The historical works relied on here turned the records that survive into objects in the service of historical ends; here, those works are turned back towards the media that they implicitly revolved around.[79]

1.4.3 Chapter three: Interception and technical media

This chapter identifies how 'interception' was articulated in different media environments, and how media in turn were developed as a result of escalations caused by the problem of 'interception'. The first medium considered is the domestic

[78] Bernhard Siegert, ***Relays: Literature as an Epoch of the Postal System***, trans. Kevin Repp (Stanford, California: Stanford University Press, 1999).

[79] A methodological inflection used by Cornelia Vismann, ***Files: Law and Media Technology***, trans. Geoffrey Winthrop-Young (Stanford: Stanford University Press, 2008).

telegraphic network and the form of the telegram. The Imperial deep-sea international cable network, by contrast, was designed and operated to ensure security against interception. While both modes of cable transmission were valued for their transmission speeds, practices of 'interception' did not focus on the means of transmission – with at least one notable exception – so much as on the telegrams that were produced in order to store information as it was transferred between paper and technical media.

Telephonic interception, commonly known as 'tapping', is similar to telegraphic interception in that it did not begin in earnest until the advent of reliable recording systems in the late 1930s. One might 'tap' the line, but the critical device required to derive useful data from telephonic interception was a tape recorder.

'Wireless' technology, or radio, was understood initially in terms of its differences to cable technology. The capacity to 'broadcast' was adopted for other purposes – entertainment – only once it was clear that there was no way to control the reception of transmissions. At that point, 'interception' was defined abstractly within a set of protocols developed in order to enable international co-operation on the 'airwaves'. Attempts to limit reception, however, led to the realisation of new techniques of interception based around identifying the location and source of transmissions, rather than the content of messages. From that point on, the territorial understanding of the earth's surface was transformed by radio direction finding. Many air and sea confrontations of the Second World War revolved around this principle. Radio direction finding guided night bombers to their targets and, conversely, intercepted transmissions risked betraying the positions of ships and submarines.

The inability to determine who received radio transmissions prompted escalations in cryptographic techniques. For centuries, cryptography was done on paper. In the 1930s, new mechanical machines were devised that transformed discrete letters into code values based on the variable arrangement of a set of mechanical wheels. The famous Enigma machine had 159 quintillion possible combinatory settings, and the settings were changed each day. Under Alan Turing's guidance, the first electronic computer was built in order to process possible cryptographic key settings, and crack the code anew each day.

Computer cryptographic research dominated the post-war period, when the problem of intercepting communication became less focused on securing the medium itself and more about the capacity of processing media. Computers were devised to decrypt and process vast amounts of intercepted material. In order to link supercomputers with field computers, the NSA implemented a digital packet-switching network using the TCP/IP protocol, prefiguring the internet and putting it to work on processing intercepted data almost from its inception.

In each instance, the position of sender, receiver, and interceptor depends on the operations of the medium. Interceptors occupy the privileged position where they can survey and determine the whole operation of the medium. The power to determine who occupies that position is, in turn, the function of the symbolic governmental authority to intercept communication.

For this chapter, secondary sources regarding intelligence agencies, cryptographic techniques, and histories of technical communication systems have been consulted. Kittler's own work discusses the interception of communication at several points, which has been instructive. This chapter also draws on a large amount of unpublished archival material, much of which does not appear to have been referenced in publication prior to this research. In this respect, the National Archives hold a number of recently declassified Home Office and Security Service files dealing with the interception of communication, either directly or obliquely, particularly during the nineteenth century and the first half of the twentieth century. They are relatively few in number, but rich in detail. Much of the material presented in chapters three, four, and five is drawn from those sources.

Technical details about communication systems and the security concerns they generated were found in the British Telecom Archive, conveniently located on the site of the original Holborn telephone exchange, just yards from the London School of

Economics. BT inherited all archival materials pertaining to electrical and technical communication media from the Royal Mail Archive when British Telecom was separated from the Post Office and sold off. A former engineer working as an archivist was particularly generous in explaining the techniques that *may* have been used to implement telephone line interception. The BT Archive, surprisingly, contains a file with details of an interception operation carried out in 1870 against striking telegraphers by tapping the telegraph lines themselves. This incident appears in no history of interception or the Post Office that has been consulted for this project.

In terms of computer technology, the NSA has recently declassified selected articles from the NSA Technical Journal and published them online. The articles help to explain the development of computers, their application to interception practices, and the implementation of Platform, the first NSA packet-switched network. Finally, the materials that have been published from the cache of material provided by Edward Snowden, referred to in this thesis as the 'Snowden archive', helped set the scene.

1.4.4 Chapter four: Issuing warrants

The second half of the thesis presents a genealogy of the legal and administrative techniques through which interception is made into a governmental capacity. Interception is independent of the law in its operations and effects, because it is determined by media operations, not legal rules. Yet media are indifferent to the *meaning* of their operations. 'Interception' and 'delivery' of information are, technically speaking, identical outcomes of different selections made during information sorting procedures. What makes 'interception' nameable as such, and thus symbolically differentiates it from delivery, depends upon the processing operations of warrants, which operationalise different media in a different register.

The brief historical legal account is as follows: since at least 1710, Secretaries of State have been understood to have the power to order the interception of communication according to warrants. The warrant symbolises a valid decision, made according to law. It thereby acts as an instrument for the will of the Secretary, who symbolically represents the agencies formally under her command. However, the legal-historical perspective does not account for the function of warrants *within* the administrative apparatus of government. What remains to be explained is how such a history can be told in the first place.

As Murphy explains, the figure of the autonomous willing subject has long been enthroned at the heart of epistemological conceptions of the social world.[80] Nowhere is this more forcefully inscribed than in the law, which can lay claim to being 'the oldest social science'.[81] Nonetheless, law functions by ordering information. It is an effect of media-technical operations. The law itself is media-based and must be analysed as such. In order to ask whether or not the law can 'regulate' digital media, one must first understand the law's own information processing operations. To do so is antithetical to the law's self-description, which is why law's media – files, documents, warrants, and writs – are unable to directly enter into legal consideration, except as evidence. As Vismann puts it,

> In the eyes of the law, the relation of mediation becomes a question of attribution… The category of personal subjecthood is the object of an act of assignation, and that act, in its turn, is itself a technique, one that occupies a central place in our legally defined culture.[82]

Therefore, we suspend the effects that warrants supposedly had in terms of expressing political will or regulating the application of interception power, and instead look at the media-technical conditions that indicate what exactly warrants *do*, how they have been *made*, and the protocological networks in which they are deemed to be effective. The genealogical excavation of the interception warrant ends at the moment that they enter into consideration of the legal system itself, which occurred in 1979.

The empirical resources for this chapter are drawing primarily from the National Archives. Other material is drawn from historical studies of the history of medieval administration in Britain, the function of medieval seals and documents, and

[80] The notion of the 'juridical soul', Murphy, *The Oldest Social Science?*, 11.

[81] Murphy, *The Oldest Social Science?*

[82] Vismann, 'Cultural Techniques and Sovereignty', 88.

historiographical accounts of bureaucracies of the British state. The theoretical matrix is indebted to theoretical studies made of legal and administrative systems by Tim Murphy, Markus Krajewski, and Cornelia Vismann.

1.4.5 Chapter five: Secrecy, publicity, and legislation

If the warrant is produced by a logic that is administrative, rather than legally performative, then what of law? This chapter picks up where chapter four ends, with a warrant coming before a court, demanding an account of itself. The process by which the interception warrant was explained illustrates the difference between administrative and legal reasoning. Law works with documents and files in order to assign things to categories and to transfer rights and obligations. Interception occupies a particularly unusual place in the legal history of the UK, however, because for around three hundred years it was practiced secretly, deliberately avoiding any adjudication by the law.

This chapter begins with an account of how the law processed the question of interception when it was finally required to do so in 1979. It develops an account of secrecy and law, via Niklas Luhmann's theoretical treatment of the mass media. There are theoretical rules prescribed by Luhmann's epistemological framework which do not perfectly align with a theory of cultural techniques and media.[83] However, there are enough affinities to enable a productive conversation to emerge; particularly when one considers the media-technical making of systems theory itself.[84]

The chapter shows that the shift to legislation that followed the disclosure of a warrant before the law was not a 'progressive' victory for the 'rule of law', nor was it based on the finding in the European Court of Human Rights that the UK was in violation of the Article 8 right to privacy. The problem was in how to produce a set of protocols for the legal processing of warrants that would achieve other ends: first, the

[83] Geoffrey Winthrop-Young, 'Silicon Sociology, Or, Two Kings on Hegel's Throne? Kittler, Luhmann, and the Posthuman Merger of German Media Theory', *The Yale Journal of Criticism* 13, no. 2 (2000): 391–420; Siegert, 'Media After Media'.

[84] Markus Krajewski, 'Paper as Passion: Niklas Luhmann and His Card Index', in *'Raw Data' is an Oxymoron*, ed. Lisa Gitelman, trans. Charles Macrum II (Cambridge: MIT Press, 2013), 103–20.

imperative to preserve the secrecy of the administration of interception operations in the future; second, to design procedures to ensure that all future legal questions regarding warrants are foreclosed in advance. Legislation was required in order to give a second-order account that secret files are kept in good order, and to thereby prevent any unauthorised transfers of information into the public domain. Legislation is thus indexed to the dissemination of information, as performed by the mass media, which has been translated into legal standards of 'foreseeability' where the question of secrecy is concerned.

We then review recent legal developments in the Investigatory Powers Tribunal – the semi-secret Tribunal that deals with interception powers – and the formulation of the Investigatory Powers Act 2016, drawing on the insights developed in relation to law, secrecy, and publicity.

1.4.6 Chapter six: Silicon Sovereignty

The thesis concludes not with a recapitulation of points made throughout, but rather with a return to Snowden's archive, specifically to an analysis of the operational interface used by GCHQ to organise and direct the interception of communication in the online environment. Material drawn from the Snowden archive shows how the protocological recipes of legislation are enacted through the form of the digital interface, which determines in advance the legality of all permissible operations.

2. Letter Interception in the Postal Epoch

2.1 Introduction: power relays

The historian of media, Harold Innis, demonstrated that empires can be described through the media and structures of their communication systems. On this account, an empire is an imaginary unity based on shared symbolic references to a hierarchical power structure that are disseminated across a given territorial space. The experience of empire is not the same for all of its subjects. Acceptance, rejection, the degree of confusion, or of cohesion experienced by subjects across imperial spaces are stratified, and entirely contingent. What they all share in common is some mode of distributing imperial messages, which shapes the medial substrate of the empire as it imposes one culture over others, and which constitutes the archaeological residue that fallen empires leave behind. Any history of imperial media is necessarily reflexive, since the objects of analysis are also the condition of the possibility of analysis: "the means of appraisal are influenced by the media, and indeed the fact of appraisal seems to be peculiar to certain types of media."[85] Hence the surviving archives and archaeological traces of empires are always the material remains of imperial delivery systems that defined imperial territorial space, and which constituted the empire by permitting commands to traverse that space.

What is missing from the archive, then, is all the communication that went undelivered, either because delivery failed or because it was impossible to send, and all that was destroyed on reading, which remains historically unknowable. The positivity of an archive is constituted by the preserved deposits of completed communication, and thus presupposes the circulation of messages that the postal historian wishes to examine. Descriptions of postal operations are always secondary accounts, which in themselves had to be delivered. In short, one can never observe the failure of communication, or its conditions, but only the residue of its success. With

[85] Harold Adams Innis, ***Empire and Communications***, 2nd ed. (Toronto: University of Toronto Press, 1972), 9.

these preconditions in mind, Innis nonetheless demonstrates the structural affinity between forms of imperial power and the forms of postal systems.[86]

Writing a history of interception, which involves manipulating missives while they are in the process of delivery is, in this sense, a history of a practice without traces. Interception – the 'taking-between'[87] – is only possible in the intermediate phase between sending and delivering. For the reader and writer of correspondence, it occurs within the excluded middle, the medium that facilitates correspondence in the first place. Interceptors, if they do the job well, must facilitate a smooth delivery, which is the best way to guarantee the ongoing success and security of their practice. But, as it is with Serres's figure of the parasite,[88] the transmission medium both determines and feeds upon the relationship that it appears merely to enable. Interceptors left records, stored copies of ciphers and letters, and provided some account of their activities, which have been picked up by historians interested in postal systems, bureaucrats, and intelligence services. Their work is a function of the delivery system itself, which preceded and determined the configuration of the 'sender' and 'receiver'.

This chapter tries to reconstruct letter interception techniques as they were practiced in Britain, or more precisely, England, across four centuries. The postal systems of Europe were initially established to maintain the transmission of sovereign correspondence and to raise profits from the inexorably growing traffic in mail during the early modern age. The growth in postal traffic not only delivered letters; it delivered addressability, which is the precondition of entering into postal correspondence. The possibility of entering into correspondence created new networks of knowledge extending beyond the horizon of one's locality, presenting a radically new horizon of possibility for communicating across space and time. In this

[86] Albeit largely Occidental in focus. Postal communication also developed in India, China, and elsewhere, see Gagan D. S. Sood, "The Informational Fabric of Eighteenth-Century India and the Middle East: Couriers, Intermediaries and Postal Communication," *Modern Asian Studies* 43, no. 5 (2009): 1085–1116.

[87] 'Interception, N.', *OED Online* (Oxford University Press), accessed 22 June 2017, http://www.oed.com/view/Entry/97583.

[88] Michel Serres, *The Parasite* (Minneapolis: University of Minnesota Press, 2007).

sense, it was the condition of entering modern history, which was written by reference to collections of letters.

2.1.1 The meaning of letters

A typical letter of the seventeenth century was composed on one side of a sheet of paper using ink and a stylus. Paper was expensive, so writers tended to fill up the available surface as best as possible, using script of different sizes and writing in different directions in order to fill up the margins and corners of pages with text. However, the way that one formed the writing on the page depended on the status of one's interlocutor and the purpose of the letter. Form could communicate as much as content, and the nobility, for whom the cost of paper was no object, arranged their text more elegantly. To historians, scripts and layouts indicate class, skill, and the intended impression the letter was to make. Content was stilted and "filled with compliments". One had to enter into the epistolary conventions of the letter, which in the seventeenth century was a heavily inflected version of the *ars dictaminis*, in order to learn to become a letter-writer. Each decision of what to write and how to write it required reflection upon what it would be taken to mean.[89] Learning to write letters was to learn to become an author, and required reflexively assessing one's authorship.[90]

Once the writer had finished the letter he added date, location and his signature. The letter was sprinkled with sand mixed with gum to prevent the ink spreading. The writer was required to make folds in the paper to bring the edges towards one another. To seal up a letter, it was folded so as to hide its content and thus make it private. The addressee's name and address (a name and a town, or a name and a government office), were written on the blank space on the back, then the folded letter was sealed with melted wax and impressed with the sender's personal seal, which confirmed authorship. The 'social moment', as Whyman puts it, occurred when the writer gave

[89] Susan E. Whyman, ***The Pen and the People: English Letter Writers 1660-1800*** (Oxford: Oxford University Press, 2009), 21.

[90] Here one can connect epistolary technique to second-order observation, see Hans Ulrich Gumbrecht, 'Second Order Observation Historicized - An Epistemological Frame Narrative' (Design of the In/Human, Stuttgart: Akademie Schloss Solitude, 2010), http://www.design-in-human.de/lectures/gumbrecht.html.

the letter to a postman. This comprised the basic procedures of letter writing during the late seventeenth and early eighteenth centuries.[91]

To master the techniques of letter production was, and is, to enter into written discourse, which transformed subjects otherwise lost to historical record into senders and receivers of correspondence, who left traces of themselves. Even today, to encounter a seventeenth-century letter in an archive is to attribute to its writer a sense of a shared internal dimension. This symbolic effect is generated by the reading and writing techniques that together define epistolary subjectivity. Friedrich Kittler's essay *Authorship and Love* illustrates the role these techniques of reading and writing played in transforming understandings of subjectivity. The essay compares two accounts of the nexus between love and text, one from the High Middle Ages, the other from the eighteenth century.[92]

In Dante's *Divina Commedia* (1321), in the second circle of the Inferno reserved for "the bodies of the lustful",[93] we meet Francesca and Paolo, who were condemned when they read aloud together the Lancelot romance, kissing one another at the moment that Lancelot kisses Arthur's wife. For Kittler, the act of reading aloud manifested the power that the medieval book had over bodies. Reading was a compelled action produced by the text. Its compulsion pushed the two together in lust, and condemned them to death.

Against Dante, Kittler juxtaposes Goethe's *Sorrows of Young Werther* (1774). This epistolary novel takes the form of an exchange of letters between Werther and his love, Lotte. In their letters, they write of souls and of words and glances exchanged. Their bodies never meet. Their desire is neither forbidden or punishable; in Foucault's terms, the clerical law that condemned the bodies of Francesca and Paolo was replaced by the norm, which indexed desire to a managed economy of sexuality. What unites Werther and Lotte is a shared love for the texts of the poet Kloppstock, which they

[91] Whyman, *Pen and the People*, 22–23.

[92] Friedrich Kittler, 'Authorship and Love', *Theory, Culture & Society* 32, no. 3 (2015): 15–47.

[93] Ibid., 17.

interpret for one another in their letters. Together they seek to understand what the "Creator-like creator meant with them".[94] But Kloppstock's meaning is inaccessible, just as their bodies and true intentions are to one another. This is the condition of engaging in epistolary correspondence:

> Werther and Lotte's eyes do the same thing while reading as while exchanging gazes: they are always-already beyond the corporeality of the letter and the corporeality of the Other, searching for a soul, a meaning, an idea... The silently-read and internally comprehended books, those which no longer inscribe bodies or provoke desire, instead make writers or authors out of the readers themselves.[95]

Desire is aimed beyond the letter at the authorial intention behind it, but this intention is always a projection of the reader's own desire. Kittler concludes that authorship emerges only when "the two discursive practices of reading and writing were fully coupled to one another". Authorship is "founded upon the deception inherent in reading one's own writing and writing one's own reading."[96]

As the poet John Donne (d. 1631) put it, "this writing of letters, when it is with any seriousness, is a kind of ecstasy, and a departure and secession and suspension of the souls, which doth communicate itself to two bodies".[97] The minds of writer and reader can never connect, but one can self-actualise in relation to another through techniques of reading and writing. Unlike medieval scribes, who simply copied texts that carried their own authority in a chain of unbroken substitutions, the modern letter writer is always already a reader of their own texts, and writing that is to be read by another is always also a form of self-observation. One anticipates the other reading what one is

[94] Ibid., 23.

[95] Ibid., 24.

[96] Ibid., 25.

[97] Quoted by Cecile M. Jagodzinski, ***Privacy and Print: Reading and Writing in Seventeenth-Century England*** (Charlottesville: University of Virginia Press, 1999), 74.

about to write, and in that moment, one considers how it might be written or understood otherwise.[98]

Letters were not only inter-personal in a romantic sense. The distinction between public and private communication became a settled axiom of social contractarian theories of government, an axiom that letters materialised. According to Michel de Servan, a French lawyer and essayist of the 'Republic of Letters', letters constituted private property belonging to both the sender and receiver. Private letters require writers to feel free in their thoughts. Correspondence is only valuable when free-flowing thought and tentative, half-formed ideas can be suggested and developed securely. The medium of the letter fixes fleeting thoughts, even if the author immediately abandons them, thus letters tie authors to a persona created by certain ideas. As they are then delivered out of the author's control, they are potentially risky objects. But the meaning of a letter is always co-constituted and therefore belongs neither to sender or receiver. Both must be bound to keep it private, hence correspondence should be legally recognised as property.[99] Servan also published an open letter to the *cabinet noir*, where letters were intercepted. Acknowledging it publicly, let along criticising it, was dangerous. Servan argued that all sealed letters were inviolate. Interception is ultimately good for nothing, he argued; not even the state, because it diminishes the confidence that the public can place in their rulers and the freedom of thought they can exercise in letters.[100] By the end of the eighteenth century, correspondence had become so central to social operations that the content ascribed by readers to letters was articulated as an object of intellectual property.

We begin by briefly tracing the pre-history of the modern letter and the pre-history of the modern postal system, in order to clearly delineate the connection between modern postal systems and the possibility of interception.

[98] This alludes towards the theory of second-order observation, see Gumbrecht, 'Second Order Observation Historicized'.

[99] Dena Goodman, 'Epistolary Property: Michel de Servan and the Plight of Letters on the Eve of the French Revolution', in *Early Modern Conceptions of Property*, ed. John Brewer and Susan Staves (London, New York: Routledge, 1995), 350.

[100] Ibid., 356.

2.1.2 Medieval letters

According to M.T. Clanchy, the idea that the medieval age was marked by blanket illiteracy and ignorance until the dawn of the humanist Renaissance in Italy is a myth, propaganda promoted by humanists taking advantage of their economic success to create a self-aggrandizing hegemonic history of literacy. Literacy, in the sense of the ability to read text, was far more widespread than humanist propaganda suggested. The humanist account dominated, however, because reading was far more widely practiced than writing, and thus left few traces. Reading was not confined only to educated segments of society: children often learned to read with their mothers, primarily in order to recite prayers aloud. Reading compelled the body into practices that were realised in common with others, rather than a solitary, silent practice.[101] Yet the *way* that texts were actualised, and the meaning that they generated, were radically different to the techniques and forms that define the modern reading-and-writing subject. Crucially, readers were not writers, and the texts they read were not supposed to represent the interior experiences of others.

Most medieval documents were generated by scribes, who were institutionalised in chanceries, universities, and monasteries. Their documents were not intended to be transmitted but rather to form records. In this sense, they were addressed to posterity. Records of the first formal missives – primarily writs issued by Chancery – appear in England from around the thirteenth century. Typically, they were brief modes of command.[102]

Scribes composed documents in the classical 'dictaminal' form, which rose to prominence in England as the *ars dictaminis* in the twelfth century.[103] Such compositions were in no sense personal or confidential. 'Authority', or *auctores*, was

[101] M. T. Clanchy, *From Memory to Written Record: England 1066-1307*, 2nd Edition (Oxford: Blackwell, 1993), 13.

[102] Ibid., 90.

[103] Mary J Carruthers, *The Book of Memory: A Study of Memory in Medieval Culture* (Cambridge: Cambridge University Press, 1993), 191–92; John O. Ward, 'Rhetorical Theory and the Rise and Decline of Dictamen in the Middle Ages and Early Renaissance', *Rhetorica: A Journal of the History of Rhetoric* 19, no. 2 (2001): 175–223.

attributed to text itself rather than any to individual compositor. No conscious will was supposed to lie behind it. As no extra-textual authority was ascribed to the text, there was no 'true' interpretation to discern. An author, or *auctore*, was "simply one whose writings are full of 'authorities'",[104] and a well-trained 'author' was a skilled reader who could speak fluently from memory, because he knew the authorities so well that it was as if he had "transformed the many nectars of the reading-flowers in one's memorial store-house into a single honey."[105] Such 'authors' did not physically write their texts. They dictated aloud to scribes, who recorded what they said. Scribes often lacked the ability to read in any authoritative manner. They were "no more than a medium between the speaker or hearer and the document."[106] Writing was not a mechanism for producing novelty, difference, or originality, but rather for ensuring successful repetition of a fixed and unitary set of laws. For Carruthers, this engendered a particular relationship with time. Medieval scholarship, in contrast to modern, is marked by "an utter indifference to the pastness of the past, to its uniqueness and integrity".[107] Medieval omnitemporality arose through the literate techniques of *memoria,* "by means of which texts of past authors are constantly related in and through present minds".[108]

One precondition for the emergence of personalised and informal writing was the development of European papermaking. It prompted a commercial revolution that enabled written communication to find new purposes outside the formal spaces of rhetorical repetition. The first European paper mill, at Fabriano, began producing paper around 1268. From there, paper and its production techniques spread into the towns and cities of Europe. Compared to the animal skins used for vellum or the reeds used for papyrus, paper was cheaper and easier to manufacture, and the product was lighter, versatile, and it could be folded. It allowed more people to send and receive more messages. Its cheapness engendered disposability, which enabled transience;

[104] Carruthers, *Book of Memory*, 190.

[105] Ibid., 273.

[106] Clanchy, *From Memory to Written Record*, 271.

[107] Carruthers, *Book of Memory*, 193.

[108] Ibid., 193–94.

messages could either be stored or destroyed on reading and thus enfolded secrets. Add wax, and suddenly information could be committed to writing with a sense of security.

After paper, universities displaced rural monasteries as centres of learning and their monopoly over knowledge diminished, as did the symbolic importance of expensive parchment.[109] Commercial bills were exchanged, accounting books were drawn up; paper set the conditions for an expansion of credit. Local vernaculars and languages were used to index writing to speech, freeing writing from ecclesiastical Latin. Printing meant that books were no longer the preserve of those who could afford scribal copies and, of course, new translations of the bible were illicitly circulated.[110] The meeting of movable type with paper produced a copying machine that turned books into mass-produced storage media.

Yet when uneducated people wrote letters during the late medieval period, they did not seek to relate events to one another, or discuss their internal thoughts. Surviving examples are almost exclusively devoted to noting the circulation of money and commodities. There was no commonly-shared vernacular form of writing generally available for self-expression. Non-clerical letter-writers in the fifteenth and sixteenth centuries would often copy the format and content of their letters directly from royal missives, which emanated from the Chancery and thus bore the ossified remnants of the *dictamen* format. Such letters were short, concerned one topic and one topic only, and were either injunctive (you must do this…) or supplicatory (I beseech you…).[111] More flexible than the strict scribal copyists of the monasteries, they were nonetheless extremely constrained in what they communicated because they afforded no opportunity for exposition:

[109] Innis, *Empire and Communications*, 129.

[110] Ibid., 130–40.

[111] Malcolm Richardson, 'The Fading Influence of the Medieval Ars Dictaminis in England After 1400', ***Rhetorica: A Journal of the History of Rhetoric*** 19, no. 2 (2001): 230–31, doi:10.1525/rh.2001.19.2.225.

> The "narrative" turns into a grotesquely drawn out "whereas" clause of the normal royal missive, except that no "therefore" clause resolves it. Rhetorically, it is just one long preamble, a head without a torso.[112]

Latin, the medieval language of written discourse, was simply too formal for a mode self-expression that mirrored individual discourse. Eventually, writers

> realized without being told that the *ars dictaminis* was misaligned with both their social and professional needs, and they hence allowed it to trail off quietly into a byway of public administration.[113]

Around the fifteenth century, modern English replaced Latin and French as the language used in Chancery documents. At this point, scholars note a marked diminution of the use of *ars dictaminis* for royal missives.[114] As lawyers, judges, and Secretaries of State increasingly replaced the administrative functions of Chancery, the royal missive format itself began to drop away during the sixteenth century. Transmitted documents required replies, and had to be stored in files, which required filing techniques and gave rise to the administrative foundation of the state.[115] Through letters and their replies, the possibilities of writing expanded in scope and form.[116] Yet away from the narrow and inherently political realm of kings, emperors, ambassadors, and courtiers, personalised correspondence did not motivate people to write letters. It appears that for around a century the English lacked any vernacular form in which to exchange private letters.[117] Instead, they sent each other bills.

2.1.3 Medieval networks

Modern postal systems emerged alongside modern authorship. In medieval Europe, the constitution of messenger services reflected feudal society's segmented and overlapping sources of authority. Charlemagne (d.814) established three main postal

[112] Ibid., 231.

[113] Ibid., 226.

[114] Richardson, 'The Fading Influence of the Medieval Ars Dictaminis in England After 1400'.

[115] Vismann, *Files*, 79–82.

[116] Clanchy, *From Memory to Written Record*, 91.

[117] Richardson, 'The Fading Influence of the Medieval Ars Dictaminis in England After 1400', 237.

routes in the Holy Roman Empire, through Italy, Germany and Spain,[118] but during the three centuries that followed no organised imperial postal system existed in Europe, reflecting the absence of any one centralised source of political authority. Only the church employed couriers, and paid them well.[119] Relatively few people travelled. Those who did, such as merchants, troubadours, pilgrims and friars, could be haphazardly entrusted with carrying messages, giving rise to the etymological root of 'mail', after 'male', a laced-up leather travelling bag. But any kind of long-distance delivery mission was a dangerous assignment.

When organised communication networks re-emerged in Europe, they worked on segmented lines. Networks can be distinguished by the specific type of communication they carried. Religious orders communicated with houses of the same order via a corps of *nuntii*, often making their way across the entire territory of Europe.[120] Merchant guilds established their own commercial communication services, such as the Hansa merchants, and the Butchers of southern Germany (later confirmed as a state postal organisation by a patent granted in 1597).[121] University postal systems began in Bologna around 1158; soon they were replicated in Naples, Salamanca, and Bourges.[122] The universities recruited trusted *nuncio volantes* primarily in order to ensure that student's fees were paid and the money carried securely back from their families. The messengers enjoyed all the privileges of members of the University and were treated as *clerici* when they travelled, meaning they enjoyed the same freedoms and protections that guaranteed ecclesiastical safe conduct and exempted them from feudal tolls. The *petits messagers* system of Paris came to be used for other purposes until it was suppressed during the French Revolution.[123]

[118] E. J. B. Allen, *Post and Courier Service in the Diplomacy of Early Modern Europe* (The Hague: Martinus Nijhoff, 1972), 2.

[119] H. C. Barnard, 'The Messageries of the University of Paris', *British Journal of Educational Studies* 4, no. 1 (1955): 49–56.

[120] Ibid., 49.

[121] J. Kerry Grant, *A Companion to The Crying of Lot 49* (Athens: University of Georgia Press, 1994), 11.

[122] Allen, *Post and Courier Service in the Diplomacy of Early Modern Europe*, 2.

[123] Barnard, 'The Messageries of the University of Paris' The University's postal service survived the rise the French territorial state, and only folded when the University itself was suppressed on 15 September 1793.

Modern postal networks in Europe originated in the messenger services of medieval kings. In England, the Anglo-Saxon and Norman *curia regis* comprised the King's Court, the Exchequer, and the Chancery. Until around the end of the fifteenth century, the Chancery was the secretariat, the source of authentic documents in the nascent bureaucracy of England.[124] Chancery clerks were educated in rhetorical forms of writing in monasteries and universities, often elsewhere in Europe.[125] There was no question of privacy or confidentiality in what they produced.[126] The security of royal documents depended upon the King's Messengers. They were members of the royal household, paid from the Exchequer, and bound to their role by oaths.[127] Known as *nuncii et cursores*, they were "intimately connected with the person of the sovereign".[128] The King's Messengers carried letters abroad to other courts, called together local assemblies in the shires, carried proclamations of new laws about the kingdom, summoned the nobility to appear before the monarch, distributed papal decrees, and carried out other administrative tasks, but their main occupation was tethering the Chancery and Exchequer to the Court as it moved around the country.[129]

2.1.4 Establishing posts

The first set of permanent postal relays in England was established in 1482 to facilitate war against Scotland. Each relay was positioned twenty miles apart on the road north. This made Edward IV the first English King to direct a war away from the battlefield.[130] As princes increasingly came to rely on postal relays for the transmission

[124] John H. Fisher, 'Chancery and the Emergence of Standard Written English in the Fifteenth Century', *Speculum* 52, no. 4 (1977): 870–99; the Chancery's work is discussed in greater detail in section 4.2.

[125] Ibid.

[126] Richardson, 'The Fading Influence of the Medieval Ars Dictaminis in England After 1400', 229.

[127] Mary Paget, *The King's Messengers, 1199-1377: A Contribution to the History of the Royal Household* (London: Arnold, 1961); Siegert, *Relays*, 30.

[128] *Report from the Secret Committee on the Post-Office, Together with the Appendix: Ordered, by the House of Commons, to Be Printed, 5 August 1844*, 1844, 21, available at http://www.gbps.org.uk/information/downloads/files/official-documents/Report%20from%20the%20Secret%20Committee%20on%20the%20Post-Office%20(1844).pdf.

[129] P. O. Beale, *A History of the Post in England from the Romans to the Stuarts* (Brookfield, VT: Ashgate, 1998), 27.

[130] Frank Staff, *The Penny Post, 1680-1918.* (London: Lutterworth Press, 1964), 20.

of secret information in order to secure the interior of the territorial kingdom, they also found that foreign networks had to be disrupted in their attempts to infiltrate the territory.[131] The emergence of the territorial state coincided with the settling of regular posts.

Elizabeth I declared a legal monopoly over letter carrying in 1590. The proclamation called on "all Mayors, Bailiffs, etc. … to make diligent search for all Mails, etc. … coming into or going out of the Realm with packets of Letters."[132] Merchant postal guilds, known as the Stranger's Posts and the Company of Merchant Adventurers,[133] were expelled from London in 1591 as the Crown sought to consolidate control.[134] The Master of the Posts began to take an administrative interest in issuing orders to postmasters across the realm.[135] In 1633, Thomas Witherings was appointed as the first holder of a new office; that of Postmaster General. He was tasked with turned the Messengers from an expense to a source of revenue.[136] In 1635, the Letter Office was formally opened for public use by royal proclamation.

2.2 Seventeenth century: the birth of interception

Becoming an author of letters requires technical skill. As Luhmann puts it, "individuality = self-reference".[137] To succeed, self-reference depends on recognition. An author cannot autonomously decide on what a letter is, as the form must pre-exist the writer to be recognised as self-referential. Only by developing one's media-technical skill can one learn to add personal inflections within the form. At that point, letters transform subjects into senders and receivers, granting to each confirmation of their will and ideas.

[131] Allen, *Post and Courier Service in the Diplomacy of Early Modern Europe*, 3–12.

[132] *Report from the Secret Committee on the Post-Office, Together with the Appendix*, 4.

[133] J. A. J. Housden, 'The Merchant Strangers' Post in the Sixteenth Century', *The English Historical Review* 21, no. 84 (1906): 739–742.

[134] *Report from the Secret Committee on the Post-Office, Together with the Appendix*, 5.

[135] J. C. Hemmeon, *History of the British Post Office* (Cambridge, Mass: Harvard University, 1912), 9–10.

[136] William Lewins, *Her Majesty's Mails: A History of the Post Office and an Industrial Account of Its Present Condition.* (London: S. Low, son, and Marston, 1864), 32–34.

[137] Niklas Luhmann, *Theory of Society*, trans. Rhodes Barrett, vol. 1 (Stanford: Stanford University Press, 2012), 297.

The political changes associated with the rise of individual opinions, and the emergence of publicly mediated debates about politics, science, law, religion, art, and so on, depended first and foremost on the adoption of the techniques required to enter epistolary communication. In England, the consequences manifested in the Civil War (1642-51), which in turn led to the English Revolution, the execution of King Charles I, and a period of would-be republican rule under Oliver Cromwell during the so-called Interregnum (1649-1660).[138] As Foucault puts it, what was at stake was not so much the ideas that people defended in their writing as a deeper conflict; a conflict over conduct itself. The reasons why things should be as they were and the means through which things could be apprehended took on different orientations.[139]

During the Civil War, letters were frequently captured and published as evidence of whatever position the publishers wished to attribute to them. In 1644, James Howell, in an open letter that was published anonymously, bemoaned the "barbarism" of the "interception" and opening of letters. It had, he wrote,

> quite bereft all ingenious Spirits of that correspondency and sweet communication of fancy, which hath been always esteemed the best fuel of affection, and the very marrow of friendship.[140]

He was not addressing himself to state interception as such, but to a generalised condition of the times. Under conditions of civil war the risk of interception of letters was generalised, to the extent that it was extremely risky to indulge in the pleasures of correspondence. One's private thoughts were at risk.

Controlling letters was a political objective. By 1641, the year before the Civil War began, there were two Postmasters General; one for the Royalists and one for the

[138] Christopher Hill, *Intellectual Origins of the English Revolution Revisited* (Oxford: Oxford University Press, 1997).

[139] Michel Foucault, *Security, Territory, Population*, ed. Arnold I. Davidson, trans. Graham Burchell (Basingstoke; New York: Palgrave Macmillan, 2007), 197.

[140] Cited in Lois Potter, *Secret Rites and Secret Writing: Royalist Literature 1641-1660* (Cambridge: Cambridge University Press, 1989), 39.

Parliamentarians. Each nominally controlled the posts in their faction's territory.[141] In practice, this meant most local postmasters were dismissed and the system, such as it was, disintegrated. Anyone stopped on the roads was searched for letters. Those letters that were discovered by Parliamentary forces were sent to a Committee of the Lords in London for inspection. Intercepted Royalist letters were frequently read aloud in Parliament, sometimes for their intelligence value, other times merely to confirm their existence so that Parliament would vote to approve reward payments to the soldiers who had found them.[142]

Captured letters were frequently published as propaganda, transforming them into matters for public consumption.[143] Yet even over enemy correspondence, moral distinctions were made as to what should remain private. On capturing a packet of Royalist correspondence in 1642, for instance, one writer's letter to his parents was forwarded to them unopened. Letters addressed to women were, generally, forwarded intact. The privacy of intercepted letters addressed to Charles's wife, Queen Henrietta Maria, was respected at first, until one letter was found addressed to her from Lord George Digby, Charles's Secretary of State. The Commons elected to open it, the House of Lords abstained.[144]

The King himself became perhaps the most dramatic example of the nexus between secrecy, interception, and publication. On 14th June 1645, the Royalist army was defeated at the battle of Naseby. Charles escaped, but his 'cabinet' of personal papers was captured. Charles, like most letter writers of his class during the period, used codes and ciphers to try to protect the meaning of his letters in case they were intercepted or captured. But his cabinet contained all his cipher keys, the plain text

[141] Hemmeon, *History of the British Post Office*, 13–18; *Report from the Secret Committee on the Post-Office, Together with the Appendix*, 8–9.

[142] See for instance, 'Intercepted Letters', in *Journal of the House of Commons: Volume 2, 1640-1643*, vol. 2 (London: His Majesty's Stationery Office, 1642), 883–84, http://www.british-history.ac.uk/commons-jrnl/vol2/pp883-884.

[143] Jason Peacey, *Politicians and Pamphleteers: Propaganda During the English Civil Wars and Interregnum* (Aldershot: Ashgate, 2004).

[144] Potter, *Secret Rites and Secret Writing*, 39–40.

drafts of letters previously sent, and deciphered versions of all the letters he had received and kept. Parliament put the letters on display at Westminster to prove their authenticity, then translated and transcribed them for publication as *The King's Cabinet Opened*. The introductory gloss pointed to the 'cabbalistical' ciphers, mobilising the general aura of mysticism ascribed to coded writing.[145] The book was intended to symbolise the exposure and overthrow of mythical *arcana imperii*.[146]

2.2.1 Monopolising a mode of visibility

Establishing a post-revolutionary monopoly over the transmission of letters, packets, and newsletters required violently seizing and suppressing other channels of correspondence. In 1649, the new Postmaster General for the Commonwealth government, Edmund Prideaux, found himself in competition with the Common Council of London, which had established a cheaper postal system during the Civil War. Prideaux slashed his prices and sent his men to attack the London messengers. They killed at least one man, raided the Council's offices, and stole their letters.[147] Private initiatives were similarly suppressed in Bury, Dover, Norwich, and Thetford. The state's monopoly was deeply unpopular amongst merchants, evidenced by records of printed pamphlets demanding the freedom to carry letters, for reasons of efficiency and principle.[148]

In 1654, Cromwell issued an Ordinance to legally establish the General Post Office and set postage prices. In 1657 Parliament confirmed the Ordinance in legislation.[149] The preamble to the 1657 Act for 'Settling the Post' states that it is commercially necessary, but also

[145] Ibid., 39.

[146] Ibid., 60.

[147] Hemmeon, *History of the British Post Office*, 193–94.

[148] Lewins, *Her Majesty's Mails*, 33–34.

[149] Cromwell's Interregnum government saw legislation as a mechanism for remaking the state, see, Stephen Sedley, *Lions Under the Throne: Essays on the History of English Public Law* (Cambridge: Cambridge University Press, 2015), 83–106.

> to discover and prevent many wicked designs, which have been and are daily contrived against the peace and welfare of the Commonwealth, the intelligence whereof cannot well be communicated except by letters of escript.[150]

According to Vismann, legislative preambles "tell a story that law does not and cannot contain".[151] They separate rules from their legislative history to establish a simple story about the state of the world into which the law must intervene. The general intelligence circulating in correspondence was held to contain traces of plots and conspiracies. The function of the General Post Office was to manage the flow of discourse. Letters were to be secured, protected, and taxed, and at the same time placed under surveillance.

Late in life, Samuel Morland, the polymath, inventor and the first master-technician of letter interception, wrote a short essay entitled *Of Intelligence*, in which he said,

> A skilful Prince ought to make watch towers of his General Post Office of all his kingdoms and there to place such careful Sentinels as that, by their gaze and diligence, he may have a constant view of all of any moment throughout the universe: but more especially of the various tempers of his own subjects, and of the first ferments of all factions, without which it is morally impossible for him long to sit on his throne...[152]

On this view, interception in the late seventeenth century was a necessity, required in order to anticipate and therefore control the plans of treacherous rebels at home and enemy princes abroad. Morland was known to exaggerate his skills and accomplishments, but on this topic, he wrote from experience.[153] He spent years opening letters, identifying and thwarting rebellious plans, subverting trust amongst

[150] 'The National Archive of the UK POST 114/1' (1657), British Postal Museum and Archive: The Royal Mail Archive.

[151] Vismann, *Files*, 22.

[152] Samuel Morland, 'A Brief Discourse Concerning the Nature and Reason of Intelligence' (Egmont Papers. Vol. CCXIV (ff. ii+276)., 1695), Add MS 47133, British Library, Western Manuscripts.

[153] Alan Marshall, 'Sir Samuel Morland and Stuart Espionage', in *King Charles Lecture* (Bath Spa University College, 2003), http://www.academia.edu/1557372/Sir_Samuel_Morland_and_Stuart_espionage.

enemies by interfering in their correspondence, and enhancing his reputation in the process.

What is most interesting about this text is the description of the Post Office as a window into the private thoughts of subjects, offering the capacity to map out the factional groups and political connections they form. During the Civil War, intercepted enemy letters were used for propaganda purposes,[154] but Morland is describing a practice that in itself must remain secret and undetected. The unique visibility he attributed to the Post Office presupposes a certain type of information latent within it, ready to be unveiled within the flow of letters: the thoughts of their writers. This order of visibility had to be monopolised, both to control access to the power it produced, and to deny that power to others.

That letter interception became a set of organised procedures demonstrates the power attributed to the knowledge that they promised to reveal. Interception was born as a response to a new form of political subjectivity generated not individually, but in correspondence with others. Letters materialised the discourse they had effected and made it visible. As Murphy explains, subjects of the feudal order were conceived of in terms provided by the common law's particular construction of subjectivity. Murphy calls this the "juridical soul", a concept based on an analogical relationship between interiority and exteriority: "God is to the world so the king is to his kingdom so the soul is to the man".[155] Government, such as it was, worked on the assumption that an oath taken publicly and before God could provide the "measure of a man", presupposing "at one and the same time 'whole-hearted' commitment, self-subjection, and the threat of punishment by the higher power".[156] This marks out the counter-factual model through which society apprehended itself as a unity, bonded together by oaths and loyalty.

[154] Potter, *Secret Rites and Secret Writing*, 39.

[155] Murphy, *The Oldest Social Science?* 11, 31.

[156] Ibid., 108; see also J. G. Bellamy, *The Law of Treason in England in the Later Middle Ages* (Cambridge: Cambridge University Press, 1970), http://ebooks.cambridge.org/ref/id/CBO9780511522369.

Under the Post Office, by contrast, letters are marked by their capacity to differentiate individuals within society; to access representations of the inner life of the individual; to understand his alliances and friends; and, in particular, to anticipate his plans. This made him governable according to the broader dynamics of the moment by assigning to him categories of political opinion, intentions, beliefs and states of mind; in short, understanding him through a set of tactics and strategies that were not determined by the law. Letters gave access to the private domain that they constituted. The authorship-effect letters engendered made them worth intercepting. The ascription of authorship to a text is always a functional categorisation process, and a statement only has salience within a particular regime of discourse, "separating one from the other, defining their form, and characterizing their mode of existence".[157] A letter could only be intercepted if it was selected, and as such, something interesting had to be anticipated. Through interception, the author's words were extracted from a network of private correspondence that assigned to them one meaning, and were animated instead within a regime of suspicion, anticipation, inspection, and investigation, indexed to the distinctions that shaped the political *épistème* of the period.

2.2.2 Interception techniques

During the 'Interregnum' period of Commonwealth rule which followed the Civil War in England, between the execution of Charles I and the coronation of his son Charles II (1649-1660), Samuel Morland and Isaac Dorislaus intercepted letters at the Post Office and reported their findings to John Thurloe, Cromwell's Secretary of State.[158] An account of their activities was later provided by John Wildman, a fellow republican who attempted to enter the service of the monarchy after the Restoration (1660), and towards that end wrote an account of Thurloe's intelligence system. He claimed that each post night, at about eleven o'clock, Dorislaus had

> the letters brought and laid before him, to open any as he should see good, and close them up again, and there he remained in that room, usually till about three or four in the morning, which was the usual time of shutting up the mail.

[157] Michel Foucault, 'What Is an Author?', in *The Art of Art History*, ed. Donald Preziosi (Oxford: Oxford University Press, 1998), 305.

[158] Marshall, 'Sir Samuel Morland and Stuart Espionage'.

> And in process of time the said Dorislaus had got such knowledge of all hands and seals, that scarcely could a letter be brought him but he knew the hand that wrote it.[159]

Samuel Morland joined him after midnight if "a rising was near".[160] They were primarily concerned with overseas diplomatic correspondence and inland letters addressed to ministers and known plotters. Sometimes certain routes were selected to search through; for instance, one account explained that he "looked over the Paris bag for the state letters."[161] But on the whole, Wildman recounted, Dorislaus operated from a written list of named targets supplied by Thurloe. The list, as Vismann emphasises, is a form of purely functional writing and the departure point for all written administrative culture.[162]

> Lists do not communicate, they control transfer operations… Lists sort and engender circulations.[163]

That the primal technique of list-making appears on the scene at the beginning of organised interception practices is mundane, but in a sense, that is an effect of the efficiency of administrative techniques. They fade into the background.

Lists demand execution. In executing the list, Dorislaus lacked dexterity. He is said to have melted sealing wax with a heated knife in order to open and close the letter while trying to keep intact the original stamped seal.[164] This crude method left visible traces. Morland, on the other hand, was an adept. Not for him a heated knife. He took impressions of seals, probably with plaster, made forgeries with which to replace them, then simply removed the original wax. He had a talent for remembering and reproducing the handwriting of others, and was able to recognise on sight the handwriting and seals of regular targets. As most letters were simply addressed to a

[159] C. H. Firth, 'Thurloe and the Post Office', *English Historical Review* 13 (1 January 1898): 531.

[160] Peter Fraser, *The Intelligence of the Secretaries of State and Their Monopoly of Licensed News, 1660-1688* (Cambridge: Cambridge University Press, 1956), 24.

[161] Ibid., 25.

[162] Vismann, *Files*, 5.

[163] Ibid., 6.

[164] Marshall, 'Sir Samuel Morland and Stuart Espionage'.

name in a post town, and names alone can easily be disguised, his knowledge of scripts was vital. Under the Restoration government he built copying machines that wet the ink on a letter and took an impression of the text without leaving a trace.[165]

The number of targeted correspondents was relatively small, as was the overall volume of correspondence. Many targets were famous men in society, such as the Royalist noblemen of the Sealed Knot conspiracy during the Interregnum. Morland uncovered the plot, observed their plans and paranoia, and then inserted forged correspondence that insinuated that they had all betrayed one another.[166] Correspondence was to him a medium that could manipulate minds, given patience and observation.

Interception of seventeenth century letters was a highly personalised affair. The individual produced by the addressing of letters served as the reference point for both interception and the tactical interventions that it afforded. Yet it was not a great secret. The practice was so intensely applied that knowledge of it circulated widely, which Wildman felt served "to discourage conspirators from using such a reliable means of transmission of communication, for fear of the regime gaining the insight".[167] Accordingly, foreign ambassadors took steps to avoid the Post Office, or delayed submitting letters until the last possible moment to minimise interception time.[168] In the city of London, illegal postal networks sprang up between opponents of the regime. Secret agents were recruited to ingratiate themselves with plotting sects and then volunteer for the dangerous job of carrying their letters. The agent would secretly open and mark any letters of interest, then allow himself to be seized by a King's Messenger, who took away the letters.

[165] Ibid.

[166] See David Underdown, ***Royalist Conspiracy in England, 1649-1660.*** (New Haven: Yale University Press, 1960), 248, 289; letters subsequent to Morland's intervention asked, 'Where shall we expect to find faith?', 'How shall we trust each other?'

[167] Alan Marshall, ***Intelligence and Espionage in the Reign of Charles II, 1660-1685*** (Cambridge: Cambridge University Press, 2003), 85; Underdown, ***Royalist Conspiracy in England, 1649-1660.***, 61.

[168] Marshall, ***Intelligence and Espionage in the Reign of Charles II, 1660-1685***, 85.

Thurloe's papers, preserved in the British Library, contain many examples of intercepted letters and deciphered copies, including an intercepted letter from Charles II, sent from France while in exile, the red seal broken.[169] Apocryphally, Thurloe survived the Restoration, when many republicans were executed, on account of a 'black book' full of the secret treasonous thoughts he had collected from the letters of supposedly loyal subjects of the King. The mere possibility of its existence was enough to guarantee his safety.[170]

The Restoration government also spied on and bribed opponents to ensure access to conspirators' letters.[171] Morland, untroubled by any political conviction, continued to conduct interception in the Post Office. The Restoration government made the most of his services. Meanwhile, the Post Office began printing intelligence reports, which it distributed in exchange for information. Domestic and foreign informers whose intelligence flowed into the Post Office reported on local unrest, foreign shipping news, trade movements, and military developments abroad. In exchange, informants received selections of intelligence in the government's official newsletter, *The London Gazette*, that they could put to their own uses. A discourse network emerged based on an economy of shared secret information too valuable to disseminate – except in exchange for more secret information.

2.2.3 Cryptographia

Given the generally risky conditions of entrusting correspondence to the roads, 'secret writing' was popular amongst seventeenth century letter writers. The Post Office was widely known throughout the seventeenth century to function as an instrument for spying on correspondence. Plays and prose of the time describe posted letters as a "disguised tightly folded form of communication", and society itself as being "thick with informers … skilled in creating crafty letters, and unpicking and inventing

[169] John Thurloe, 'Thurloe Papers, First Series. Collection of State Letters and Papers Relating to Events at Home and Abroad Chiefly in the Time of the Commonwealth - Add MS 4155-4159' 1692, Western Manuscripts, British Library.

[170] Marshall, *Intelligence and Espionage in the Reign of Charles II, 1660-1685*, 20–27.

[171] Whyman, *Pen and the People*, 49.

codes".[172] Popular treatises on devising and using cipher systems were published as early as the sixteenth century.[173] The Reverend Dr John Wallis, professor of geometry at Oxford and co-founder of the Royal Society, wrote of *cryptographia*, a term he coined in 1641,[174] that, "there is scarce a Person of Quality, but is more or less acquainted with it".[175] He was employed as the principal codebreaker for both the Interregnum and the Restoration governments, eventually becoming chaplain to Charles II.[176]

There are three sets of techniques that can disguise the meaning of text without mechanical or computational methods. Technical steganography conceals the presence of the secret message by physically disguising it within other media. Such media include 'invisible' ink (milk with onion juice is an ancient formula), or writing within folds of paper, or caching letters in hidden compartments of other objects. The second technique, linguistic steganography, hides the text of a message by embedding it sequentially within a larger text. The intended reader extracts the distributed letters of the hidden message from the larger text by applying the algorithm according to which it is embedded, for instance, read the third letter of the fourth word of every fourth line.[177] Alternatively, significant code words or phrases might signify certain pre-agreed meanings.[178] The third alternative is encryption. If steganography aims at avoiding recognition, encryption expects it and attempts to defy it.[179] Coded or ciphered text is overtly recognisable as such; an *ars occulte scribendi* intended to be comprehensible only to one who holds the encryption 'key'.[180] The security of cryptographic key systems is a paramount secret; conversely, so too are the cryptanalytic methods used to attack them.

[172] Ibid. fn 32.

[173] David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, 2nd ed. (New York: Scribner, 1996), chap. 4: On the Origin of a Species.

[174] Friedrich L. Bauer, *Decrypted Secrets: Methods and Maxims of Cryptology*, Third (Berlin: Springer, 2002), 8.

[175] Cited by Potter, *Secret Rites and Secret Writing*, 39.

[176] Kahn, *Codebreakers*, 167.

[177] Bauer, *Decrypted Secrets*, 12–18.

[178] Ibid., 18–24.

[179] Ibid., 24.

[180] Ibid., 8.

The codes that Wallis solved for both the Interregnum and Restoration governments were mostly nomenclator codebook systems and monalphabetic transformation systems.[181] A nomenclator codebook is simply a list of words with a list of corresponding codewords or numbers listed next to it. The code elements should ideally be disarrayed so as not to correspond in any way to the alphabetic order of the plaintext. Frequently they were arranged according to the alphabetic order of the words they encoded, so that one correctly-guessed codeword can help unravel the others, placing them all in alphabetical order in relation to the first guess. Eventually irregular tables were introduced, and some that contained nulls, which are decoy code terms inserted into a text, having no corresponding meaning.[182]

A monalphabetic transformation system, also known as a 'Vigenère system', translates the common alphabet into an alternative alphabet via a key of random letters, usually based on an easily remembered phrase from a poem, song, or prayer. Each letter in the code alphabet corresponds directly to a letter in the plain alphabet and the original message is transcribed accordingly.[183] Letter frequencies provide grounds for educated guesses as to the signified letters used in monalphabetic transformation systems.

The cultural techniques of encrypting information in paper and ink based media could be defeated by inverting the techniques using the same media. Storing and processing semantic forms of writing into other written forms was solved by storing and processing samples, until the possible transformation algorithms had been narrowed to a small range of possible solutions, within which a guess led to the plain text. Codebreakers therefore built archives of intercepted letters. Wallis's papers contain meticulously ordered transformation keys describing the codes and nomenclator systems that he solved, accompanied by annotated examples of deciphered letters. Yet many Royalist writers whose letters were intercepted did not believe that cryptology

[181] Kahn, *Codebreakers*, 168.

[182] Ibid., 161.

[183] Potter, *Secret Rites and Secret Writing*, 40.

– the study and breaking of codes – was possible. When a packet of letters was seized on the road in 1658, they thought themselves safe on account of their codes.[184]

2.2.4 Settling the posts

The Post Office overlaid its operations on existing mail roads, and the maintenance of a post by a Postmaster was often a secondary function of another business, such as an innkeeper. What mattered was a place on the road where correspondence could be reliably sent or collected to or from elsewhere for a fee. The governmental problem was bringing these regional operations into the formal accounts of the General Post Office. It was conceived of as a primarily financial problem. The aim was to make sure that the profit made from organising the carriage of mails went to the Post Office itself rather than the postmasters.[185] The monopoly, such as it was, was conceived of not as the physical transmission of letters, but in terms of who received the money letters generated.

After the Restoration, the Secretary of State, Lord Arlington, and his deputy, Sir Joseph Williamson, set about intensifying the operations of the Post Office to ensure mail was channelled through the Office, and thereby made available for inspection and taxation.[186] Some sense of the tactics and strategies used to give effect to the monopoly are captured in a 1682 report by the Master of Ordinances, Thomas Gardiner. Gardiner provided a detailed account of the postal routines of the day. The Post Office had been re-established in Lombard Street after the original site and its staff were displaced, first by the plague in 1665, and then by the Great Fire of London in 1666.[187]

Gardiner's account gives a sense of the "political anatomy of detail", in Foucault's formulation, by which the Post Office generated, expanded, and refined its

[184] Ibid.

[185] Hemmeon, *History of the British Post Office*, 14.

[186] Whyman, *Pen and the People*, 49.

[187] Thomas Gardiner, '*A General Survey of the Post Office - Add MS 62091*' 1682, Western Manuscripts, British Library: modern spellings have been substituted in for ease of reading.

competencies.[188] At bottom, the Post Office worked through techniques that attributed personae (as addressees) to things (their letters), and at the same time attributed monetary value to its own operations (as postage). In order to discipline discourse, to observe the thoughts of the population, to achieve a monopoly over the flow of correspondence throughout the territory, and to secure postage as revenue, the Post Office first had to discipline the bodies and minds of its staff.

This account is important because it reveals the operations by which the Post Office produced and sustained an organised flow of traffic in mail. It accounts for the development and consolidation of the techniques of transmission upon which the development of interception depended for its basic resources.

2.2.5 In the office

The function of an office, at a minimum, is to process information. In this sense, an office instantiates a set of procedures that can be realised anywhere that information "is received, recorded, arranged and given out."[189] In order to convert individual letters into a flow of discourse, the Post Office of the late seventeenth century operated in an enclosed, segmented, and disciplined space. Bodies, furniture, scales, pre-printed dockets, and accounting books were used to ensure that paper and postage circulated along fixed circuits, converting the unsorted bags of material and money that came into the office into an ordered outward flow of taxed letters and postage revenue. Everything that mattered was counted, inspected, and put into order via pre-printed forms and ledgers, ready to record and compile postal statistics.

Early on Mondays, Wednesdays and Fridays, inbound letters arrived in the Inland Office early in the morning from each of the six mail roads. The roads were named according to either their termination point or cardinal direction: Chester, West, Bristol, North, Yarmouth, and Kent. All six roads terminated at ports. Work in the Post Office

[188] In particular, see Foucault, ***Discipline and Punish***, 139–62: this section details the themes of disciplinary techniques that produce and supervise 'docile bodies' in different enclosed spaces of nascent institutions - schools, prisons, barracks, and so on.

[189] Alan Delgado, ***The Enormous File: A Social History of the Office*** (London: John Murray Publishers Ltd, 1979), 11.

was divided according to functional needs. There were clerks, responsible for processing the post (eight in total); window men, who received letters at a counter from the London public and placed them into one of six large drawing boxes, one for each road; sorters, who arranged letters into bags for delivery; letter carriers, who took letters out to be delivered in town; a stamper of letters; porters for carrying bags of mail and parcels; and return men for dealing with dead letters, i.e. undelivered letters. Other than the clerks, these were functional roles rather than fixed positions: individual workers could do several different jobs in a weekly cycle. Bodies were individualised not according to the needs of the order of work.[190] The professional roles in the Office, however, were fixed: the accountant, treasurer, and comptroller (who symbolised "the authority and Person of the Chief Governors") organised and supervised operations in order "to influence the whole body through all circumstances of their duty".

Everything was arranged to ensure that workers could not collaborate with each other or with postmasters in the countryside to defraud the Office of revenue. Clerks were randomly assigned incoming mail bags to process, and the prices, numbers, and weights of the tallies they arrived at were checked by the accountant against paper bills supplied to him from each postmaster to ensure they matched. Sorters rearranged letters into delivery bags according to their onward destination. Until the nineteenth century, most letters were paid for on delivery. That was so as to guarantee that letters did not simply go missing after payment. Postage was calculated on each item separately, according to the total distance it had travelled along the post roads. All unpaid letters in a bag were stamped with the date on the sealed side and the cost was converted into a charge against the letter carriers, to be recouped as they made deliveries, or against the postmaster of the destination post town, to be recouped as letters were collected and paid for. Porters guarded the sorting rooms so no one could enter or leave until the work was done. Colloquially known as 'bellmen' because of the bells they rang to attract attention on their walks, letter carriers followed the same routes each day, "in a constant manner, still beginning and ending in the same place",

[190] Foucault, *Discipline and Punish: The Birth of the Prison*, 146.

then settling their bills “without more trouble to the Office”. Return men disciplined the letter carriers by making checks on any letters they returned undelivered to the Office.

Outbound post was processed overnight on Tuesdays, Thursdays, and Saturdays. Receivers brought in bags from fixed walks through the suburbs of Westminster, Charing Cross, Pall Mall, Covent Garden, and from the Inns of Court. They too separated their letters according to whether they were paid or unpaid, calculated the anticipated postage charges for the unpaid letters, and ensured the correct sums of cash were handed over for prepaid letters. Each had a unique personal stamp to mark each letter he handed in. At midnight, the Office gates were closed to prevent any further letters being handed in. The timed order of the day was rigidly enforced in order “to keep the Clerks in continual action”. Occasionally, “little offices abroad… bring a glut of Letters at that unreasonable time, most prejudicial to us”. The priority was to ensure the efficient and orderly processing of outbound mail.

Clerks were again randomly assigned a different road on each night shift to prevent secret arrangements with postmasters. The sorting desks had pigeonholes for each of the towns of the roads in sequential order, this way, the territory of the postal network was represented in the furnishing and fittings of the office. A bill to each town’s postmaster on a pre-printed form was attached to their bag. Post boys took the bags out on horseback to the first posts on the roads.

The precise connection between mail sorting and interception at the time is unclear; it is not mentioned in Gardiner’s report. While diplomatic post would have been sent in identifiable packets for each particular embassy and, therefore, would have been easily spotted, it seems likely that a list of names was copied and distributed to each of the clerks, who were the only members of staff to inspect each letter individually as they sorted the mail.

What matters is that interception was an inflection on sorting operations. Sorting was the moment that converted unsorted data into clear transmission channels. This necessarily required inspection of each letter. To function within the Post Office delivery system all that was required of a letter was a name and an address, usually based on a London neighbourhood or on the nearest postmaster's location outside the city. But the sorting process was an opportunity to observe more, to make other selections according to seal, signature, handwriting, or other material differences that might mark a letter out for selection and interception. Hence the sorting space was a secret space, guarded at all times during operations, symbolically separating the material operations of the postal system from the outside world.

2.2.6 Stamp and deliver

Postmasters were effectively innkeepers who agreed to make horses and food available for the relay riders of the Royal Mail.[191] What mattered here were the techniques for recording the presence of a letter in the system. Only when a letter had entered the mailbag and had been recorded in the postmaster's pre-printed accounting book could it be counted as taxable by the Post Office, and only when it physically reached London was it formally processed, by reference to the recorded lists of letters received. Postmasters could therefore secretly profit from 'bye-letters', which reached their destinations somewhere along the road and thus never passed through the central Inland Office in London. It was easy, they simply didn't enter bye-letters in their accounting books. All that was required, presumably, was a different bag, a different notebook, or perhaps no book at all. What was not recorded for the Post Office was invisible to the Post Office. In this sense, the Post Office was primarily experienced as a form of taxation on a system that could just as well get along without the need for central organisation. To underline the point, Gardiner, in his 1682 report, suggested that 'riding surveyors' could perhaps police this by travelling the roads making unannounced inspections. There was nothing useful about this suggestion beyond the extraction of tax.

In Gardiner's report of 1682, postal problems were presented in financial terms, but they represented implicitly the inaccessible flow of discourse that could not be sorted, inspected, taxed, or intercepted. Gardiner's solutions to postal revenue problems offer

[191] Hemmeon, *History of the British Post Office*, 9.

an indication of the logic of the Office at the time. He proposed surveillance tactics be applied, not only within the Office but across the territory generally. Yet other tactics emerged instead. Postmasters were on the whole underpaid and frequently incurred losses, which did not encourage them to send any profits they made onward to London. One successful tactic was to send them copies of the government's newsletter, the *London Gazette,* which they could sell for a penny in their towns. The newspaper soon became so successful that some postmasters were eventually paid only in *Gazettes.* Clerks, in turn, were awarded franking privileges over newspapers – that is, they were granted the right to send newspapers through the post free of charge. Clerks soon came to supplement their low salaries by buying newspapers in bulk from publishers in London and selling them on to postmasters at a profit, who in turn sold them to their customers and to local taverns and coffeehouses in their towns. Newspapers became intractably coupled to the economy of the postal communication network. Demand for news effectively subsidised the efficient transmission of mail.

Within London, a different model emerged to challenge the Post Office's aim of monopolising discourse. The 'penny post' was a decentralised network based in the City of London, established in 1679 by William Dockwra and backed by the Whigs, the opposition parliamentary party who opposed absolute monarchical rule. Letters were sent and received in around one hundred and eighty different shops and coffeehouses in the City via several small sorting offices. In exchange for a penny, the letter was stamped on sending (using the world's first stamps) and delivered. There were no unpaid letters, so no need to register sent letters in a book or calculate prices on delivery. Anonymity went hand-in-hand with efficiency. Dockwra's network very quickly turned a large profit, while the General Post Office incurred losses.[192]

The penny post disseminated an unregistered flow of information, news, and political agitation throughout London.[193] It was subversive not because of what it transmitted, but because it could not be inspected. The Duke of York, who held the postal monopoly, brought an action for infringement of the royal prerogative and the

[192] Staff, *The Penny Post, 1680-1918.*, 35–37.

[193] Fraser, *Intelligence of the Secretaries of State 1660-1688*, 128–32.

network's admirable profits were incorporated into the General Post Office in 1692.[194] The operations, however, continued as before, assisting the cheap circulation of a disorderly flow of information through eighteenth-century London.

2.3 Eighteenth century: the function of interception

The Post Office grew unevenly in terms of revenue in the eighteenth century, but in terms of complexity and efficiency it rapidly transformed into a large bureaucracy overseeing a postal monopoly. It became an apparatus through which a new set of relationships between the territory, the state, and the population were articulated. In public discourse, the institution came to be regarded as a "private necessity and public right", as Whyman puts it, rather than the distrusted instrument of political surveillance it had been. Postal services effectively served as the informational infrastructure for the emergent notion of the 'public sphere'.[195] But the General Post Office, as it came to be known, was also wrapped up with the technics of population, economy, and security through which power operated. If in the eighteenth century the "finality of government resides in the things it manages and in the pursuit of the perfection and intensification of the processes it directs", then the postal system is an archetypal case study for the emergence of governmentality, which operates not though law but through the development of mutable tactics.[196]

2.3.1 The postal dispositif

When the financial administration of the Post Office was placed under Treasury control in 1685, postage became an instrument of taxation, payable on a permanent basis to the institutions of a fixed and established form of state rather than to the temporary holder of a monopoly. Although it continued to lose money, the losses did not constrain postal growth in a number of dimensions. First, postal work became professionalised. In 1703, a Post Office solicitor was appointed to manage the growing need for legal decisions; managers were appointed to conduct uniform weekly audits;

[194] Hemmeon, *History of the British Post Office*, 30.

[195] Whyman, *Pen and the People*, 71.

[196] Foucault, 'Governmentality', 211.

an architect was permanently appointed, as were two bag-makers.[197] Boys were sent to the Post Office to train as clerks; a "good Post Office education" included learning postal geography and different postage rates by heart.[198]

Second, postal institutions became fixed and permanent across the territory. The General Post Office redefined conceptions of territory as it became the first reliable and regular system for transmitting communication anywhere across the space it connected. By the middle of the eighteenth century most market towns and manufacturing regions had daily delivery and collection services at official locations. Regional postal sorting offices were established to increase circulation speed and lower the postage costs of mail within local areas, and London ceased to be the radial hub of the network. As the speed and coverage of the mail increased, competing networks were swallowed up. Roads, canals, and turnpikes supplied not only economic growth to communities, but postal services. The first armoured mail coaches appeared in the 1780s, increasing the speed and security of all long-distance deliveries.[199] Overseas deliveries and postage rates became standardised.

Third, the postal system generated more work for itself by bringing more people into view as postal subjects. Its increasing reach and efficiency delivered the opportunity to invent oneself: to become an author of letters. Through "reading, copying, adapting, and composing narratives about their lives",[200] postal subjects attained the capacity to produce themselves in writing for the express purpose of communication with others,[201] and in the process generated new circuits of economic, financial, news, and legal transactions that accompanied changes in labour mobility.[202] These postal discourse networks recursively amplified their own operations. Contemporary letter

[197] Kenneth Ellis, *The Post Office in the Eighteenth Century: A Study in Administrative History.* (Oxford: Oxford University Press, 1958), 6–8.

[198] Ellis, *Post Office in the Eighteenth Century*, 21.

[199] Susan E. Whyman, *The Pen and the People: English Letter Writers 1660-1800* (Oxford: Oxford University Press, 2009), 47–58.

[200] Whyman, *Pen and the People*, 77.

[201] Ibid., 128–29.

[202] Ibid., 106.

writers came to view the institutionalised General Post Office not as object of suspicion, but as a necessary public service, from which users demanded constant improvements in speed, reliability, and cost.[203] It was the ambition of any good postal worker to meet those demands.

The postal service had become a governmental *dispositif*. It continually lost money for the Treasury, but that was beside the point. Postal operations generated their own reasons for expansion that were not economically determinable. As Siegert puts it,

> it no longer would be the role of postage to achieve maximum utility from an established and unquestionable circulation of discourses, but instead to produce those discourses in the first place: 'And henceforth the theory of production must always precede that of circulation.'[204]

The postal *dispositif* attained the capacity to measure and adapt its own operations. Postal statistics were collected as the institution took account of its operations, which were used to refine management practices. When in 1682, Gardiner had considered the problem of bye-letters, those letters which were sent and delivered at towns on the same road and so could not be accounted for within the Post Office, he suggested appointing riding surveyors to apply postal discipline; to inspect and enforce the law against postmasters. Postal governmentality, however, solved the problem with statistics. By introducing pre-printed post bills upon which each postmaster had to account specifically for the number of bye-letters they collected, average figures were used to calculate a projected number of bye-letters that statistically ought to pass between any two given towns, based on their relative size and commercial importance.[205] Postmasters whose figures notably deviated from their anticipated average flow were placed under suspicion. The problem of bye-letters vanished. Such letters were brought into the official postal economy by the application of a norm, derived from the very statistics that postmasters were required to gather in the course

[203] Whyman, *Pen and the People*, 56–57.

[204] Siegert, *Relays*, 57, the citation is from Foucault's discussion of the economic theories of Smith and Ricardo, see; Michel Foucault, *The Order of Things: An Archaeology of the Human Sciences* (London: Tavistock, 1970), 250–63.

[205] Hemmeon, *History of the British Post Office*, 37.

of their own operations. They effectively disciplined themselves by observing and recording their own work, in a media-technical process that was actualised through changes made to their pre-printed notebooks. Postal power operated technically, and at a remove.

Nonetheless, all such operations occurred within a highly-stratified hierarchical society. This is perhaps most clearly visible in the issue of franking, derived from *franc*, meaning 'free'. Franking rights were granted to ministers, MPs, and members of the nobility as privileges of their office. To 'frank' a letter, the privileged person simply endorsed it with their signature.[206] Franked letters were sent and received free of charge, and people with franking privileges would allow others to use them in exchange for favours. Franking created a bifurcation in the postal economy. Between 1711 and 1761 the number of franked letters grew by seven hundred per cent, while paid-for letters grew by only fifty per cent. In short, many more letters were sent than were paid for. When letters were paid for, postage was considered excessively high, as the Treasury tried to extract the maximum possible postage to cover losses. Those dependent on the mail, particularly bourgeois merchants with money but without privilege, frequently wrote to the Post Office to complain that postal methods were out-dated, and postage over-priced.[207]

Although understood to be an exemplary symbol of class privilege, franking was a blunt instrument that produced unanticipated effects. In 1764, a statute aimed at restricting the abuse of franking privileges created a loophole that allowed MPs to have others sign their franks on their behalf. Almost immediately, printers, booksellers, and newspaper publishers flooded the Post Office with printed matter, signed on behalf of their patrons. Between 1764 and 1796, the number of newspapers franked by postal clerks in London rose from one million to over eight million.[208] Newspapers circulated free of charge throughout the country, carrying news, criticism, gossip, and providing platforms for anyone who wished to write in response

[206] Delgado, *The Enormous File*, 66.

[207] Whyman, *Pen and the People*, 56–57.

[208] Ibid., 67.

to have their own thoughts circulate back to them. The relatively rapid expansion in critical discourse and news reporting were destabilising to the existing monarchical order, which ultimately paid for the costs of its transmission via the losses franking incurred. As a side-effect, it ensured that writers and journalists were added to the long lists of interception targets.[209]

2.3.2 Postal intelligence

Broadly speaking, the eighteenth-century postal *dispositif* created, collected, and transmitted 'intelligence' on the population as a whole, which it brought into consideration through its operations.[210] All postal workers knew that part of the job was to record and relay back any "remarkable occurrences" in local areas by writing and sending reports through the post.[211] Postal surveyors reported on crime, disorder, economic conditions, and local elections; postmasters and secretaries in Ireland, Scotland, and the overseas colonies reported privately on civil and military issues there. Port officers provided news of enemy ship movements and copied passenger lists, and foreign spies continued to avail of the network to supply Britain with intelligence. One Rotterdam merchant, Richard Wolters, operated an intelligence ring that posted information back to London concerning every foreign naval base from Ostend to Toulon.[212] The Post Office was the interface between government and 'society' at large. These tactics served a broader strategy associated with governmentality, which is the bringing to light of the 'population' as a kind of 'thickness', a mobile set of diverse groups and categories that are irreducible to individual members and that follow a set of natural processes associated with factional or group 'interests'.[213] The Office conducted surveys and collected statistics

[209] Ibid.

[210] Ellis, *Post Office in the Eighteenth Century*, 60.

[211] There are extensive and unordered collections of intelligence reports, letters, printed pamphlets, posters, and other evidence of 'unrest' generated by the Post Office stored in disparate boxes in the National Archives, see the series beginning 'Home Office: Post Office Correspondence 1787-1816 HO 33/1' 1816, National Archives.

[212] Ellis, *Post Office in the Eighteenth Century*, 62.

[213] Foucault, *Security, Territory, Population*, 350–53.

but it was also the channel through which surveys and statistics were delivered to the reforming institutions of government in London.

The Post Office had a specific policing function at times of unrest, as demonstrated in *Hensey's case* of 1758. A Catholic, Doctor Hensey, was prosecuted for treason during the Seven Years War with France. At trial, a postman from the City of London appeared as a prosecution witness. He said he regularly collected letters from Hensey when he rang the post bell on collection nights on Arundel Street, London. He became suspicious:

> —I observed that the letters I received of Dr. Hensey were generally directed abroad and to foreigners; and knowing the doctor to be a Roman Catholic, and as I imagined in the interest of the Pretender, I advised the 'xamining clerk at the office to inspect his letters, telling him that I had some suspicion that the writer of those letters was a spy.
>
> —Did you open any one of these letters yourself?
>
> —No; but I happened to challenge the letter about the Secret Expedition; and when it was opened at the post-office and found to be what it is, after that I received directions to bring every letter I received from the doctor…

The next witness was a clerk of the Post Office, who explained,

> when war is declared against any nation, immediate orders are given out by the Postmaster General to stop all suspected letters, in order to prevent intelligence being given the enemy of our transactions at home.[214]

Here are the two sides of the Post Office as a specific organ of intelligence: the suspicious postman monitoring his customers in the streets, and the internal use of a general warrant to supervise entire channels of communication.

[214] *Some Account of the Trial, &c. of Dr. Florence Hensey*, Kimber, Edward (ed.) *London magazine, or, Gentleman's monthly intelligencer*, 1747-1783; London 27 (Jun 1758): 304-305.

2.3.3 Professional interception

Warrants were prescribed as the only lawful means of authorising the opening or delaying of a postal letter or packet by section 40 of the Post Office (Revenues) Act 1710. Under section 41, all postal workers were required to swear an oath, bringing interception and non-interception into a tight relationship with the overall priorities of the institution. Warrants symbolically disciplined postal workers, and calibrated the seriousness of the interventions they could make into the mail they carried:

> I do swear, That I will not wittingly, willingly, or knowingly open, detain, or delay, or cause, procure, permit, or suffer to be opened, detained, or delayed any letter or letters, packet or packets, which shall come into my hands, power, or custody, by reason of my employment in or relating to the post office; except by the consent of the person or persons to whom the same is or shall be directed, or by an express warrant in writing under the hand of one of the principal Secretaries of State for that purpose …[215]

Interception work was functionally differentiated in the eighteenth century. If a Secretary of State's warrant for the opening of letters concerned matters connected with a criminal investigation in a particular area, they were intercepted in the sorting rooms of that area. Such letters were not carefully opened. It did not matter that such interception was known to have occurred. Letters intercepted for political reasons, however, were forwarded unopened to the Private Office within the Post Office in London, where skilled interceptors opened them undetected.[216] The cultural techniques of letter interception could extract more information from a given letter than the sender or receiver intended or expected, and everything significant was thus recorded as a future resource for selecting and copying further correspondence. The Private Office was the operational centre of a distributed domestic interception network. It received letters intercepted under warrants from local sorting rooms in

[215] 'An Act for Establishing a General Post Office for All Her Majesty's Dominions, and for Settling a Weekly Sum out of the Revenues Thereof, for the Service of the War, and Other Her Majesty's Occasions.', (9 Ann.) C A P. X. (11) § (1710).

[216] Ellis, *Post Office in the Eighteenth Century*, 64.

regional offices and the Post Office sorting room in London, processed them, returned them, and distributed the intelligence onwards as directed.

The most specialised techniques, however, were applied in the Secret Office, also known as the Secret Room. There, diplomatic mailbags were processed as they passed through the Post Office. It comprised three rooms within the Post Office headquarters. In the Secret Office, candles constantly illuminated the workroom and enabled the melting of sealed wax, while a fire was kept alight for comfort and for the disposal of executed warrants. Two other rooms served as lodgings – the interceptors lived and slept where they worked. They came and went via a private entrance located on Abchurch Lane to avoid observation. Admission was strictly controlled, restricted to the staff and the Postmaster General only. Only the head of the department, known as the Foreign Secretary, was officially listed in the Post Office accounts as a public official, and he only from 1723, when the then-Foreign Secretary gave evidence in the House of Lords during a trial for treason.[217] Otherwise, the very existence of the department and the names of the staff were kept secret, with salaries paid anonymously from a general pot of secret service money allocated to the Post Office by Parliament.[218]

Interception was performed by teams of professional technicians. Anthony Todd, a Secretary of the Post Office, was a farmer's son who began his postal career in the Secret Office. He wrote that a working day would typically begin at 8am or 10pm on post days and nights. In order to give the appearance that diplomatic mail was not interfered with, the Post Office prioritised the rapid delivery of diplomatic post to foreign embassies in London.[219] As this compressed the time available to work on intercepting it, the clerk's first duty was to quickly check all the diplomatic bags to

[217] Bishop Atterbury was involved in a 'popish plot', condemned for treason and exiled; his intercepted letters were later published. See A. Lang, 'The Bishop's Plot.', ed. William III Blackwood, *Blackwood's Edinburgh Magazine* 161, no. 975 (January 1897): 90–99 The role of Foreign Secretary was internal to the Post Office. The contemporary office of British Foreign Secretary refers to the head of the Foreign Office, which was not created until later.

[218] Ellis, *Post Office in the Eighteenth Century*, 65.

[219] Ibid., 79.

select target letters and packets of letters, open them, quickly scan the letter, noting in a registry ledger the names of sender and receiver, the address, date, and the general thrust of the content. He then indicated particular passages and passed the material to the copying clerks. Todd's role included noting the "connexion of hand, address, and seal" revealed in each letter so as to aid future identification of targets.[220]

Where the use of invisible ink was suspected, special liquors for detecting it were applied. Inks and waxes were procured from across Europe to disguise the work. Translators were on hand to translate letters penned in other European languages. Once the clerks had finished with a letter, the precise colour and type of wax used on the original letter was selected, melted, applied, and stamped with a precise forgery of the original seal. All letters had to be returned to their original packets intact and in the original order. Where a seal had changed or a new target was selected, a forger immediately set about carefully engraving a new duplicate. Interception, was no longer the work of one or two men, but an organised workflow.[221]

As in the seventeenth century, the operations required to intercept letters depended on selection criteria, applied in the course of the processing and sorting of mail in transit. The scale and scope of interception had altered but the essence of the technique remained. By the eighteenth century, the interception warrant had become the only established means of legally delivering a list of targets, inserting selection criteria into sorting operations and demanding their execution.

2.3.4 The deciphering branch

The same secret fund that covered the Secret Office and Private Office also paid the mathematicians of the Deciphering Branch, which was composed of several decipherers sworn to secrecy. They worked mainly from home rather than in the Post Office, receiving their work via special messengers. The Deciphering Branch built upon the deciphering techniques and archive of codes bequeathed by the seventeenth

[220] Ibid., 81–83.

[221] Ibid., 75.

century decipherer, John Wallis.[222] Secrecy was essential, as demonstrated at the treason trial of Bishop Atterbury in 1723 before the House of Lords. Two decipherers were called to give evidence. They testified that they had deciphered the intercepted letters shown as evidence of the Bishop's treason. The defence challenged them to demonstrate how they had done it, to prove the connection between the code and the deciphered text. However, the Lords ruled that they should not explain their methods, nor say anything that might reveal "the Art or Mystery of deciphering".[223]

The decipherers used many of the same techniques and principles as Wallis had a century before. But they were assisted by the development of enciphering techniques amongst the professional letter interceptors. Clerks of the Secret Office were specially trained to recognise information in intercepted letters that could be useful to the decipherers, by looking for cribs. A 'crib' is any piece of information that gives a contextual clue as to what words have been substituted or enciphered. The clerks noted down details written in plain alphabetic text that might indicate the meaning of enciphered text.[224] Cribs could precede or follow the coded text that they refer to; therefore, everything that a target sends or receives by post is a potential crib. A common source of cribs came from diplomatic staff of foreign embassies encoding the contents of documents that their ambassador had obtained from the British government. As the decipherers always had access to the original, it was easy to see how certain words were encoded. Another frequent mistake was to refer in code to events discussed in plain text in previous correspondence. Provided the interceptors arranged their registry of intercepted letters carefully to note who wrote to whom and when, they could simply look up possible solutions to coded terms in plain text, accessing stored records of older elements in an ongoing chain of correspondence.

[222] John Wallis, 'Letter-Book of John Wallis 1651-1701 - Add MS 32499' 1701, Western Manuscripts, British Library.

[223] Kahn, *Codebreakers*, 170–71.

[224] Ibid., 157–163 for examples.

Although better encryption techniques had been devised in theory, some of them practically unsolvable by hand, diplomatic clerks generally did not use them.[225] In practice, they were slow to prepare and complicated to use, and because they typically required at least two sets of transformations, mistakes in encoding or decoding could easily render the whole letter meaningless. Yet it was known that the codes in use were relatively simple to break, and each major European government knew that others operated so-called 'black chambers'. Encoding letters, it seems, was primarily a cultural technique that identified the particular skills expected of diplomatic clerks, rather than a means of actually securing messages. It was also expensive, costing around £150 for a new nomenclature system in the late eighteenth century. Governments were reluctant to pay and so carried on using some codes for over a decade, rendering them useless; more ritualistic than rational.

2.4 Nineteenth century: normative closure

If, for the purposes of this chapter, the seventeenth century was a time of violent suppression, and the eighteenth century a time of intensification of political control and corruption, then the nineteenth century completes the genealogy by marking the differentiation of postal operations from other social distinctions. This was accompanied by a transformation in the way interception was observed, and the purposes that it was put to.

2.4.1 Postal reconfigurations

The dysfunctional economics of the postal service were well-known to complainants writing in the 1790s; by the 1830s perennially high postage and the abuse of the postal system were widely viewed as counter-productive to social progress. A parliamentary committee convened in 1837 heard the following complaints:

> A multitude of business transactions were not carried on at all, or were carried on clandestinely, or were hampered by the high postage rates. Bills for small amounts were not drawn, commercial travellers did not write until several orders could be sent on one sheet of paper, samples were not sent by post, communication between banks and branches was restricted, statistical

[225] Ibid., 77.

> information was denied, social correspondence restricted especially among the poor, working men were ignorant of the rates of wages in other parts of the country, and the high postage was a bad means of raising revenue.[226]

In order to become truly productive and to finally pay for its own operations through postage, the postal system had to be 'liberalised'.

According to Foucault, the 'biopolitical' mode of power emergent in the nineteenth century aimed at measuring the intensity of applied methods and tactics, striking 'balances', making adjustments, checking results and optimising techniques so that they function collectively. All aspects of life became objects of power, developing reflexive forms of governmentality. Decisively, biopolitical power is cognitive of the risks of governing and takes actions accordingly. The ultimate aim is the improvement and growth of society through processes of 'normalisation' – bringing things into line with mobile norms, while simultaneously assessing and altering norms. This means taking a second-order attitude to government itself; politics is then a matter of the correct application of "action upon actions".[227]

2.4.2 Systemic closure

Reform of the Post Office commenced in 1840 under Rowland Hill, a utilitarian schoolmaster who had proposed radical changes in a series of published letters, and who had no prior experience of the postal system until he was made Postmaster General.[228] His idea was simple. A letter could be posted anywhere in Britain for a penny. The postage charged was the same for each item (classified by weight), regardless of how far it travelled between sender and receiver. Distance was therefore disconnected from postage. Postage pricing became indifferent to space and all deliveries were made spatially equivalent.

The entire domestic territory was reconfigured as a single penny post network. Hill correctly foresaw, through studying postal statistics, that the higher cost of letters

[226] Hemmeon, *History of the British Post Office*, 61.

[227] Pottage, 'Power as an Art of Contingency'.

[228] M.J. Daunton, *Royal Mail: The Post Office Since 1840* (London: The Athlone Press, 1985).

carried over long distances would be covered by the efficiencies gained in local deliveries, and he correctly predicted that introducing a universal penny post would spur a rapid rise in use of the mail and induce an end to various abuses. Circulation rates and overall revenue would rise. Postal work was simplified greatly, because clerks, postmasters, and delivery carriers no longer had to calculate the price of postage on each item. All franking privileges were abolished, further simplifying the processing of mail. Every item had to be paid for, and as such postage became indifferent to the social rank and personal favour that had dominated in the eighteenth century.

As Siegert points out in terms drawn from systems theory, Hill's successful reforms implemented the 'operational closure' of the postal system. From that point on, postal logic formed a closed system that followed its own internal programming when processing the mail. Postage would be indicated by prepaid stamps, manufactured for the first time to coincide with the new system. Provided a valid stamp was in place, no additional input from the environment was required to validate the delivery of a letter to its address, wherever it may be. With postage stamps, another differentiation occurred: the money economy was separated from postal operations. There was no exchange of cash when sending a letter or receiving it. Rather, stamps separated monetary and postal operations in time and space. The strict uniform postage rate meant that individuals and companies could know the total amount of money required for any given number of future deliveries in advance. By purchasing stamps, they could pay for deliveries long before composing, let alone sending, a letter or parcel. With a stamp, the customer purchases an *opportunity* to send a letter anywhere in the network at some undefined point in the future.

The reforms also compressed the time required for delivery. Letter carriers and postmasters no longer had to take time to give out bills and collect cash with each delivery, meaning they could move between addressees rapidly and in order, dropping off letters that had been paid for the moment their stamps were cancelled in the sorting room. So immediately successful was this plan that the supply of adhesive stamps, introduced on 6th May 1840, could scarcely keep pace with demand.[229]

Circulation speeds increased in line with the explosion in the number of letters sent and received. Postal reform not only differentiated its operations from space, and from the money economy, it also divorced itself from individuals, with whom postal workers no longer had to interact. This was confirmed when, within a few short years of the reforms, secure collection boxes for safely posting letters appeared across the country in cities, towns and villages, while letter boxes appeared on front doors.[230] By abstracting postal operations from the personalities, politics, and local differences of the institution, the new system functioned by reference to the technical requirements of circulation.

2.4.3 Addressing the nation

The other side of the closure of the postal system was standardisation of all communication sent via the Post Office. Once postal operations ceased responding to the differences of particular users, users had to adapt their communication to the standards of the postal system. Stamps and delivery boxes demonstrate this, but not as clearly as the addressing system.

In 1856, the Post Office began the process of affixing street names and street numbers to all addressable sites in the country. There was considerable resistance, particularly in wealthier areas where streets were often named for ancestors. By 1871 there were around one hundred thousand officially numbered houses and almost five thousand renamed 'areas'. Within London, ten postal districts were established, each with a local sorting office. The public were asked to add the districts' initials to addresses – EC, WC, N, SE, SW, and so on. Codes and street names were slowly introduced in other large towns and cities.[231] Postal addresses operate according to the following

[229] Siegert, *Relays*, 100–107.

[230] Daunton, *Royal Mail*, 40–43.

[231] 'Postcodes', *The Postal Museum*, accessed 28 August 2017, https://www.postalmuseum.org/discover/explore-online/postal-history/postcodes/.

presumptions and requirements. First, that every dwelling or building is a potential addressee, regardless of who lives there; second, that all buildings and dwellings are serially arranged on streets or roads and can be numbered as such; third, that all streets and roads have, or can be given, names that are unique within a defined locality; fourth, that localities have names that are unique to a defined region; fifth, that regions are uniquely named within the country.[232] On these principles, the Post Office rationalised cartographic geography, ultimately indexing all delivery points addressable according to a single master index, a coding of space, indifferent to the particular people located there.[233] From then on, letter writers had to adjust their mode of address to match the one applied by the Post Office. Letter writers were addressable by the terms and codes assigned to them. This had always been so, but here it was made explicit.

The unified postal address system transformed unmapped urban spaces into a panoptical territory by fixing in place both "souls and houses".[234] Without such an index of addresses, there is only an indistinct "*sea* of houses",[235] which required local knowledge to navigate. Just as imposing an address ties deliveries to standardised and coded locations, it frees postal workers from local knowledge, and means they too could go anywhere in the territory. Everyone who wished to use the postal system to send mail had to address themselves according to its index, and everyone who wished to receive mail in return had to submit themselves to an address.

> We exist in the eyes of the law as long as only one mail slot is to be found at the address recorded by power… Thus, there is indeed "no destination before the arrival." Only at the moment of the letter's delivery is there a destination, an address, our existence. The letter therefore is not delivered to the address, but

[232] Paul A. Longley et al., *Geographic Information Systems and Science*, 4th Edition (Hoboken, NJ: John Wiley & Sons, 2015), 113.

[233] 'Draft Report by the Metropolitan Board of Works, Including Post Office Proposals for New Street Names in Central London POST 17/120' 1856, Royal Mail Archive.

[234] A description issued by the mayor's office and Council of Vienna, 1771, cited in Markus Krajewski, *Paper Machines: About Cards & Catalogs, 1548-1929*, trans. Peter Krapp (Cambridge, Mass.: MIT Press, 2011), 27.

[235] Ibid., 28.

> the address is delivered by the letter; there is no place before its arrival, no identity before the address.[236]

Hill's reforms meant individuals were liberated from the close attention of postal employees. Rather than the Post Office learning about differences between individuals, individuals adapted themselves to the names and numbers generated by the Post Office. This way they became individuated according to nationwide standards, and addresses became an index for confirming identities across different information retrieval systems, such as those used by banks, the police, the revenue, and so on. Addresses enabled the interception of mail to be targeted with unprecedented precision, but also enabled any number of categorisations to be applied once each individual became identifiable by more than just their name and locality.

A postal address remains a precondition of access to other services. Surveillance, as Foucault demonstrated, is simply a prerequisite of inclusion in modern society. Indeed, the implementation of the address system occurred concurrently to the 'liberalisation' of labour in the mid-nineteenth century, when workers began to be encouraged to save money and enjoy leisure time in addition to labour time, thus all of a subject's time was entered into calculations of economy and political power that increasingly channelled subjects into the operations of banks, advertisements, and the general expansion of consumption.[237]

Man, as Rowland Hill put it, "is made of the Post Office, and not the Post Office for man."[238] It was always the postal system that dispatched addresses, never people. In doing so, the Post Office nonetheless produced the conditions for an anthropocentric theory of modern society, i.e. for the appearance of the 'man of letters'. Provided the postage was affordable, "the materiality of the postal service could remain beneath

[236] Siegert, *Relays*, 115–16.

[237] Michel Foucault, 'Truth and Juridical Forms', in *Power*, by James D. Faubion, trans. Robert Hurley & Ors., vol. 3, Essential Works of Foucault 1954 - 1984 (London: Penguin, 2002), 80–81.

[238] Patrick Joyce, *The State of Freedom: A Social History of the British State since 1800* (Cambridge: Cambridge University Press, 2013), 53.

the threshold of consciousness".[239] Yet the postal *dispositif* determined the conditions under which this authority could refer to itself and transfer itself across space and time. Postal communication autopoietically generated more postal communication, once the blockages caused by humans, and their local differences, had been ironed out of the system. Authors or lovers, businessmen or labourers; the postal system only succeeded once it became utterly indifferent to the meaning and status of what was sent and delivered.

2.4.4 Interception as infrastructural capacity

Letter interception had been a secret practice for as long as there had been organised postal services, but it suddenly became a topic of public discourse in England in the summer of 1844. A prominent Italian nationalist living in exile in London, Giuseppe Mazzini, discovered his letters were being intercepted by experimenting with the materiality of the network. One account claims he posted letters to himself containing poppy seeds, which were missing when the letter was returned.[240] Another claims he sent two letters to his own address on the same day, one with his name on it and another with a different name, and observed that 'his' letter arrived later than the other one.[241] Either way, Mazzini responded by recruiting Chartist politician Thomas Duncombe, who was in opposition to the government of the time, to put the matter to Parliament and to inform the press. Mazzini aimed to publicise the cause of Italian nationalism, rather than to promote English privacy.[242]

When the Mazzini scandal broke in the English press, an editorial in *The Times* of 17th June 1844 declared:

> The Home Secretary contented himself with declaring, in general terms, that there were reasons for his conduct. But the [House of Commons] was not satisfied with this, nor will the country be so. We want facts and circumstances. We want such evidence as would satisfy any reasonable man or any set of men

[239] Siegert, *Relays*, 76.

[240] According to David Vincent, *The Culture of Secrecy: Britain 1832-1998* (Oxford: Oxford University Press, 1999), 1–10.

[241] Denis Mack Smith, *Mazzini* (New Haven: Yale University Press, 1996), 41.

[242] Ibid., 42.

> that the Home Secretary was morally justified in the course which he pursued. The whole question is one of constitutional rights, and nothing else. Mr Mazzini's character and habits and society are nothing to the point, unless connected with some certain or probable evidence of evil intentions or treasonable plots. We know nothing, and care nothing about him. He may be the most worthless and the most vicious creature in the world. But this is no reason of itself why his letters should be detained and opened.[243]

The Times editorial could not be clearer about the irrelevance of the personality of the target. What was explicitly required was some normative justification for interference in the flow of letters. *The Times* and its readers never received the express public declaration of reasons that it demanded. We shall return to the Mazzini incident, but for now suffice to note that in the Report of the Secret Committee presented to Parliament in the aftermath of the scandal,[244] which was the first attempt to review both the history of the Post Office and of letter interception, an evaluation of the utility and justifications of postal interception was required.

Apparently, no records were kept of warrants earlier than 1712, and that the few which had survived the eighteenth century were vague in detail. Some, however, were clearly an abuse of patronage, used to spy on family members within the nobility. The report implicitly suggests that by nineteenth century standards, such incidents were taken as mere symptoms of a corrupt and bygone political culture. In one example that the Committee selected, in 1741 on the request of Mr 'A', his eldest son was granted a warrant to open and inspect any letters which A's youngest son should write to two named women, "one of whom that youngest son had imprudently married".[245] This warrant was selected as an exemplar by the Secret Committee

[243] This is a cutting from the Times retained by the Post Office in a special entry book composed of cuttings about the Mazzini scandal. We shall return to this in chapter 6. 'Newspaper Cuttings Relating to Letter Opening, 1844/1845 POST 23/7' (Newspaper cuttings relating to the Secretary of State's abolition of the board established at Post Office Headquarters to consider the policy on the opening of letters from persons suspected of treason against the UK and foreign governments, 4 April 1845), British Postal Museum and Archive: The Royal Mail Archive.

[244] *Report from the Secret Committee on the Post-Office, Together with the Appendix*.

[245] "Secret Committee", 12.

precisely because it indicated triviality, showing how freely warrants could be granted in the corrupt age of grace and favour, when match-making within the nobility was a critical element of political power. Yet the report only briefly mentions much more significant interventions, such as the occasions on which general warrants that arrested entire categories of mail had been used. It simply states that no general postal warrants had been made since the turn of the nineteenth century.

Contemporary interception was divided in the report into two classes: 'criminal' cases and 'political' cases, the latter of which were almost all concerned, at the time, with Irish nationalism.[246] In August 1842 a clerk was sent to "the manufacturing and mining districts… in the week of the greatest anxiety" with a warrant to open letters of named persons. Most of the targets were subsequently convicted before a special commission. Two clerks were also sent to other towns with warrants, but found no letters to open and returned to "ordinary business" soon after.[247] This would seem to suggest they were clerks seconded from the Post Office's Investigation Department, which was publicly described as a department that dispatched clerks to investigate criminal matters involving abuses of the postal system. Their investigations were publicly said to only concern offences against the revenues of the Post Office itself, not general criminal investigation, so this cannot be confirmed.[248]

Tabulated statistics on the use of interception warrants in the report seem to demonstrate the decline in the number of interception events. Moreover, the tables serve to represent interception as a well-organised, carefully controlled practice.[249] Subjecting the question of interception to a utilitarian moral calculus, the Committee calculated the mean number of annual warrants: eight per year since the start of the nineteenth century. Each warrant had an average of two names per warrant – thus the report finds that it affects an insignificant number of letters within the overall volume

[246] Ibid., 7–11.

[247] 'Secret Committee', 14.

[248] For a brief overview, see 'POST 120 Series: Post Office Investigation Department 1836-1999', Royal Mail Archive, accessed 21 September 2017, http://catalogue.postalmuseum.org/index.php?

[249] Ibid., 10–11.

of traffic. The Committee concludes that selective interception actually minimises intrusions into the "liberty" of correspondents because it produces useful intelligence leading to measured responses, thereby avoiding intrusive over-reactions which could lead to violent popular reactions. On the population level, then, privacy and freedom in the post were found by the Secret Committee to have *increased* since the eighteenth century, and this was in part down to the selective use of interception.[250]

Having started as a determinative reason for the monopolisation of discourse, interception had thus become an exceptional and controversial practice. The 'public mind', which had come to observe itself through the news and letter media disseminated by the Post Office itself, re-entered the operations of the postal system. When interception was no longer the *raison d'être* of the Post Office, no longer a necessary condition of state survival, it was possible to imagine that interception should not take place at all, that it was normatively unacceptable that anyone should invade the privacy of communication. Letter interception thus demanded a normative justification extrinsic to the security and operations of the postal system itself.[251] As Foucault observes, the

> subject of interest overflows the subject of right. He is therefore irreducible to the subject of right… and is the permanent condition of him functioning.[252]

Liberalism, in other words, meant maintaining and developing existing techniques of observation of the population but, at the same time, promoting and producing 'freedom' meant allowing for risk. The moral calculus of interception was a security issue, in the sense that the discursive distaste for interception practices did not derive from, nor refer to, any moral philosophy concerning privacy or subjective integrity, but rather to a utilitarian calculus, comparable to what Foucault has identified as a "principle of calculation… the problem of security is the protection of the collective interest against individual interests."[253]

[250] 'Secret Committee', 18–19.

[251] Ibid. The relationship between interception and the 'public mind' is revisited in chapter five, see 5.4.3.

[252] Foucault, *Birth of Biopolitics*, 274.

[253] Ibid., 65.

In the aftermath of the Mazzini scandal, the government quietly closed down the diplomatic interception of the Secret Office, pensioned off the decipherers, and ceased all interception of foreign mail. Yet such foreign letter interception was nowhere mentioned in the secret report, which mentioned only domestic interception.

Domestic interception continued as before, and indeed soon found new purposes in the moral health of the population. Postage reform in 1870 introduced a new halfpenny rate that was specifically designed to allow advertising circulars to be distributed to all addressees in general. The 1870 reforms, in essence, opened up the addressable population to the discourse network of the advertising industry. But commercial circulars contain both legal and illegal offers, and this particular adaptation of the postal service soon allowed illegal lottery competitions to emerge, which, alongside the rising circulation of pornographic material from overseas, were regarded as an immoral abuse of the medium that had to be intercepted, blocked, and eliminated from the network.[254]

2.5 Twentieth century: media in media

The latent potential of total interception inherent in the Post Office monopoly over mail was realised with the implementation of general interception and, later, mass censorship.

In anticipation of war with Germany, in September 1911 the Home Secretary, Winston Churchill, secretly signed a general warrant granting the newly formed domestic Counter-Espionage Bureau, MO5,[255] wide scope to direct postal interception. The first task was to identify 'postmen', a nickname for messengers who received letters from German intelligence and forwarded them to German spies.[256] A "carefully compiled, cross-referenced index of the intercepted letters" was created, gathering 1,189 discrete

[254] 'Detection of Lottery Correspondence in the Post; Secretary of State's Warrant of 19 April 1920 HO 45/25958' 1934, National Archives.

[255] Christopher Andrew, ***The Defence of the Realm: The Authorized History of MI5*** (London: Penguin, 2010), 29.

[256] 'Investigation of Espionage 1914-1919: Incomplete, Draft Summary KV 1/48' 1919, National Archives.

entries between 1911 and 1914, when war officially began.[257] Rather than intercepting individual letters, the pre-war foreign interception task sought to identify networks operating through the postal system.[258]

At the trial of Karl Gustav Ernst, the fact that interception had occurred was acknowledged.[259] Interceptors Richard Alfred Evans, Frederick Bosworth Booth, John Duncan, and John Barr Featherstone provided sworn statements and testimony. They described themselves as "clerks in the Secretary's Office of the General Post Office" and said they all understood German. Around 160 different intercepted items were exhibited in evidence. Not only did the intercepted letters make it possible to identify Ernst's role in a network of German secret agents, but each agent's own persona and role in the network was established with a depth of detail sufficient to mount a successful prosecution of Ernst under the Official Secrets Act. While the German nationals were rounded up and deported, Ernst was a British citizen and therefore had to be prosecuted. Later, during the war, anyone in the same position could have simply been executed. It seems that Ernst's case may have been the last deliberate use of intercepted material as evidence in a British civilian court.[260]

War began in July 1914. By the end of the year, there were 170 postal censors in place, checking items of mail to and from enemy territories. By the 1918 armistice there were 4,861 censors opening all letters and packets.[261] By 1917, the following steganographic techniques had been detected:

> … handkerchiefs embroidered in Morse Code; imitations of Raphael Tuck's postcards;[262] religious books; newspapers sent in batches, the number of newspapers indicating the number of troops; the colour of the ink of the

[257] Andrew, *The Defence of the Realm*, 37. Indexes and registries are discussed in detail at 4.4.3.

[258] 'Special Duties: General Post Office Investigation Branch MEPO 2/1500' 1919, National Archives.

[259] One of the very rare occasions that intercepted letters were used as prosecution evidence, see 'KV 1/48', 18. See also 5.3, 5.4.4 on law, secrecy, and courts.

[260] Ibid., 48; 'Central Criminal Court Deposition, Defendant: ERNST, Karl Gustav. Charge: Offences against the Official Secrets Act. Session: November 1914, CRIM 1/151/2' 1914, National Archives.

[261] Andrew, *The Defence of the Realm*, 65, 71.

[262] Raphael Tuck & Sons produced popular designed postcards for sale

> address indicating the arm of the service; phonographic records and printed advertisements. Importation and exportation of phonographic records was prohibited and all advertisements had to have a police visa before publication.[263]

Different media formats were mobilised in an attempt to evade censors and infiltrate the postal system. External technical assistance was required to detect them.[264] Artificial invisible inks, known to the British as 'F' and 'P' ink, were infused into scarves and socks in order to be utilised by spies. All such items were dipped in water when discovered in parcels in order to release any chemicals stored within. An escalating series of ever-more sophisticated invisible inks and developing reagents unfolded.[265]

The microdot is perhaps the best illustration of how the interception of letters ceased to target discourse and instead targeted storage media. To make a microdot, a message is typed on paper, photographed, and developed. The image is optically reduced in size and printed at around 0.05 square inches. The miniaturised image is lifted using a hypodermic needle and cemented onto an ordinary letter with glue. It must be placed somewhere it can be disguised – over a full stop, beneath a stamp, or inside the lips of the envelope were frequently used locations.[266] To read a microdot, one requires the aid of a 200-power microscope. To the naked eye it is just a dot. Without some forewarning, an ordinary letter censor had little chance of noticing that a paper medium carried a celluloid medium on its surface.[267]

In the 1950s, according to former MI5 agent Peter Wright, Post Office Investigators worked as interceptors under the direction of the Security Service (MI5, formerly

[263] 'KV 1/48', 163, it should be noted that British attempts to infiltrate information past German censors do not feature in this report.

[264] Andrew, *The Defence of the Realm*, 71.

[265] Kahn, *Codebreakers*, 353, 524; Peter Wright, *Spycatcher* (New York: Viking, 1987), 119.

[266] Kahn, *Codebreakers*, 525–26.

[267] Nigel West, *British Security Coordination: The Secret History of British Intelligence in the Americas 1940-1945* (London: Little Brown, 1998), 353–54, 362.

MO5). Wearing rubber gloves, they worked side-by-side at a long table. Each investigator was equipped with a lamp, a Photostat machine or pedal-operated camera, and an electric kettle for steaming open envelopes. The work was repetitive and, apparently, quite mechanical. They did not stop to read the letters they worked on, but simply photographed them for others to inspect later and returned them to the flow of sorted letters. Letter interception no longer required any discursive or linguistic skills. It was essentially a repetitive set of technical procedures.[268]

By collating data from multiple interceptions, targeted correspondence networks could be outlined on paper. A 'letter check' request from MI5 simply required the interceptors to note down everything on an envelope: its origin, its destination, details about the stamp. It did not involve opening the envelope and, therefore, on the Post Office's reading of the law, it required no warrant.[269] Around 155,000 postal items were selected and opened in 1961, growing to 221,000 by 1969.[270] Interceptors were stationed securely out of sight within Post Office sorting rooms, selecting items to inspect according to a rolling list of targets, copying the content, and sending on the item for delivery as normal.[271] Yet the techniques employed in accessing, copying and processing the contents of letters had changed entirely.

2.6 Conclusion

The technical operations of postal interceptors vary, but all depend on two preconditions: access to the sorting room, which converts disorderly noise into regulated, observable discourse available for inspection, and sufficient time. The interceptors occupied a physically segregated space into which only authorised personnel could enter. Symbolically speaking, it was the space reserved for sovereign operations of postal sorting, which was, after all, the materialisation of the monopoly. But it also reserved a secret, separated space in which commands issued by secret

[268] Wright, *Spycatcher*, 45. Wright's book was controversial for political reasons – he claimed there was a Soviet spy in the senior ranks of MI5 – but his descriptions of technical practices have never been questioned or denied.

[269] Ibid., 46.

[270] Andrew, *The Defence of the Realm*, 334, 549.

[271] Duncan Campbell, 'Big Buzby Is Watching You', *New Statesman*, 1 February 1980, 160.

warrants from the Secretary of State, the symbolic user of intelligence, could be safely executed.

Time was a variable that conditioned operations. Interception was constrained by the number of disciplined bodies that could be effectively deployed at once. Mass interception was possible given hundreds or thousands of hands, but only at the cost of severe postal delays and, therefore, widespread knowledge of the practice. The 'liberal balance' in respect of mail interception is not between personal privacy on one hand and state security on the other. It is a balance between optimal inspection time and optimal delivery time. Delayed deliveries risk other, second-order consequences, as Mazzini showed when he (perhaps fictitiously) posted two letters to his home and timed the delay between their delivery.

Given the preconditions of access to sorting operations and time, interception is a conditional selection operation that can be performed on any posted letter. The function of interceptors, then, lies in executing the selection commands they receive. Interception techniques were applied, or not applied, to letters according to a conditional decision implicitly taken over all sorted mail that entered the apparatus of the Post Office. Everything not selected – the vast majority of postal correspondence – is positively sorted and paid for, and thus delivery is always dependent on a system that permits an item to proceed as 'normal'. This positivity eventually became the norm, and thus it is largely invisible. Nonetheless, one should insist on regarding the delivery of an untouched letter as a consequence of its positive non-interception. This implies understanding delivery, and thus interception, not as cognitive experiences but as media-technical operations. From the perspective of the Post Office, viewed as a non-discursive medium that sorts and orders other discursive media, it requires a processing decision applied in each and every sorting operation, even if the human sorter does not perceive it as such. In terms drawn from systems theory, non-interception is the 'unmarked side' of all interception decisions.

Respect for the 'privacy' of a letter is therefore a second-order effect of non-selection against a horizon of possibilities that include, at the extreme end, the potential for total interception. The First World War illustrated this. One day, only some traffic was selected for interception, and the majority passed undisturbed. The next day, all postal traffic was halted and checked, with very little allowed to pass undisturbed. Tactically, total interception could not coincide with operational secrecy; the time demands and organisational commitments to secrecy made that impossible. The point is that the potential is always latent in the network.

While the postal monopoly provided the technical precondition for the application of techniques that selected and processed intercepted letters, the symbolic meaning of those letters, that is, the 'intelligence' generated from interception, is conditioned by the discourse networks in which the political, moral, economic, or legal meaning of things unfolds. Interception commands are always issued in anticipation of something, but such anticipations are secondary to the techniques that select a letter for interception.

Recalling Harold Innis, we could argue that the modern postal empire is one in which everyone is free to communicate by post, under the condition that the post is free to observe everyone's communications. This is nothing more than a consequence of 'good government'.

> The danger emanating from the noise of the people was dispelled as soon as it was intercepted by a network that controlled, redirected, sorted, and calculated it, thus ensuring that its waves were not emitted at unanticipated speeds or in unanticipated directions.[272]

The postal system, which takes letters very seriously, is indifferent to whether or not an item is intercepted on the way, provided that it is eventually delivered or its non-delivery is accounted for. What makes the difference between interception and non-interception are selection criteria that enter the postal system from outside, via the medium of the interception warrant.

[272] Siegert, *Relays*, 105.

3. Interception and Technical Media

3.1 Introduction: the processor in the cage

By 1898, the year that Henry James wrote *In the Cage*, the telegraph was already the most mundane and commonplace of the so-called 'new' media developed in the nineteenth century.[273] The story turns on the observation of communication in transit, illustrating the relationship between electrical telegraphy and interception. In the first generation of telegraphic systems, interception was, at its most basic, simply a possible mode of observation inherent in the technical role that human bodies played in transforming alphabetic messages into informative electrical patterns, and back again.

The central character is a young unnamed telegrapher, who sits alone in a glass dome within a wire telegraph cage at the back of a grocery shop. There she receives and sends telegrams, exchanging messages for money. The drama arises when, in a break with the normal operating protocols of her role, she appears to become the intermediary in a love affair that she believes is unfolding between a rich man and woman. The affair, it seems, is being conducted entirely via the telegram messages that the telegrapher sends and receives between them each day. The latent ambiguity in every thirty-four-word telegram, full of abbreviations and devoid of exposition, leaves ample room for imaginative interpretation. The drama is entirely contained within our protagonist's own construction of events; in how she imagines the lives of these two characters, their pasts and their future plans, their mutual desire, all based upon the enigmatic correspondence that accumulates with each transmission.

All the while, the telegrapher herself remains essentially invisible to the couple that she thinks she knows intimately. She is wired to the cage; a moving part in a bigger machine. Formally, she should be attuned only to the task of silently writing out text messages translated from the coded bursts of noise produced by the electric sounder, or passively reading the pencilled characters the customers jot out on the pre-printed

[273] Henry James, 'In the Cage', in ***In the Cage and Other Stories*** (London: Penguin, 1972).

telegram forms provided as she 'keys' them out with the electric circuit-breaker. She processes telegrams endlessly; there is no end to what the machine must communicate. But as soon as she assigns meaning to the text that she discretely encodes and decodes, she implicitly differentiates herself from the medium and instead observes the results of her work, now as a second-order observer. She is no longer only transmitting; she is processing transmitted data for herself.

In cybernetic terms, the young woman's actions add to the trivial medium of the telegraph a non-trivial component. The telegraphic *dispositif* is 'trivial' in that it simply transforms text into coded pulses and back again. The 'non-trivial' element arises when she receives the throughput of the telegraph as an input for a different operation: meaningful composition. Messages continue to pass through the telegraph, unchanged and forgotten thanks to her training in Morse code, but when this particular couple's messages arrive, she selects and copies them to her consciousness mind, and thus generates a story. Each message transforms the meaning of those that came before, adding a new dimension to the unfolding pattern that she recognises (incorrectly, as it transpires) to be a love affair. It is a secret observation that leaves the messages unchanged, a consequence of the fact that her technical capacity is essential to the operation of the telegraph, which could not transmit without her capacity to read, write, and follow commands in two languages, text and Morse code.

For Henry James, this makes his unnamed telegrapher complicit in the process of authorship itself, composing stories from the raw data flowing in serial bursts through the wires and into her head.[274] Hence, although she is wired to her cage, she occupies a privileged position, one that enables her alone to determine the meaning of the symbols she processes.

3.1.1 Interception technology

This chapter traces the relationship between successive generations of technical communication systems and interception techniques, with a particular empirical focus

[274] A point developed by Richard Menke, 'Telegraphic Realism: Henry James's In the Cage' 115, no. 5 (October 2000): 975–90.

on the practices and priorities of UK governmental agencies. It draws specifically from the distinctions that Friedrich Kittler's theory of *Medienwissenschaft* derived from information theory: that all communication media can be assessed in terms of their *storage*, *transmission*, and *processing* capacities, and that these operations determine the possible understandings and symbolic assignations available to knowledge. All the elements required for the interception of communication are identifiable in the operations of every technical communication system, and these factors determine the spatial and temporal dimensions of the interception of communication, as well as the epistemic possibility of naming an operation as 'interception' in the first place.

Transmission connects two points, perfectly reproducing information at both ends of the wire, but if observed otherwise, it also situates potential targets, spatially defined according to the addressing system of the network, and transparent to whomsoever can access the visibilities afforded by the transmission medium. *Storage* connects two moments in time, reproducing data for observation at a time chosen by whomsoever can access the memory facility. *Processing* involves the basic operations required to make it possible to interface between human senses and technical media, like the telegrapher in her cage who switches between Morse and alphabetic coding. But for interception there is something more: rather than simply translating data between two forms, it requires the capacity to respond to the data in a non-trivial manner, taking decisions on the basis of whatever coded symbolic values are observed in transmission or storage media. The techniques of 'interception' involve processing, i.e. performing a pre-configured selection program upon communication, in order to select certain messages for copying and further processing elsewhere. These parameters become clearer as they are applied across four distinct media domains: cables and telegrams, telephones, radio, and digital media.

3.2 Cables and telegrams

3.2.1 Monopolising telegraphy

Electrical telegraphy began on the railroads, allowing 'signalmen' down the line to know a train was coming before it arrived.[275] The first telegraphic commercial messaging service in England began operating on 1st January 1848. Competing for business with the uniform penny post, the telegram was marketed as a command system for the instant delivery of urgent information and "a collecting service for economic and financial news."[276] It was deliberately portrayed in advertisements as a 'masculine' medium, with a curt efficiency and lack of soul that rhetorically differentiated telegrams from the inherently 'feminine' form of letter writing, which was to be relegated to dealing with inefficient matters, like love and gossip and human emotion.[277]

By the 1860s, telegraphy's potential to transform communication had made it a long-standing object of governmental attention. At the end of the decade legislation was used to compel the sale of all private telegraphic communications services, which each operated their own networks, to the government. Beforehand, the Electric Telegraph Company ran an unsuccessful campaign against the proposed legislation. According to one pamphlet printed in 1868:

> What is a telegram? Practically it is an *open letter*, the contents of which is known to and is capable of being used by everyone through whose hands it passes. Is it desirable that the most important part of correspondence of the country should pass through the hands and be subject to the surveillance of government officials?[278]

[275] The sense of pre-emption compelled Dickens to write a ghost story, Charles Dickens, *The Signalman: A Ghost Story* (London: Profile Books, 2015).

[276] Simone Fari, *Victorian Telegraphy Before Nationalization* (Basingstoke: Palgrave Macmillan, 2015), 34.

[277] Ibid.

[278] Electric and International Telegraph Company., *Government and the Telegraphs: Statement of the Case of the Electric and International Telegraph Company against the Government Bill for Acquiring the Telegraphs.* (London: E. Wilson, 1868), 78–79, https//catalog.hathitrust.org/Record/006847104 (emphasis original); quoted in Fari, *Victorian Telegraphy Before Nationalization*, 176.

A good description, and a good question. It did not make a difference to the outcome. Private ownership constrained the connective potential of telegraphy. Different networks delivered telegrams only to points located within their own circuits. Submitting telegrams to government surveillance was a precondition of universalising the network.

3.2.2 Tapping the line

Contra Marshall McLuhan, the telegraph did not 'extend' human consciousness into the wires,[279] rather, it incorporated the bodies and minds of telegraphers into its apparatus, and disseminated material symbols, not consciousness. It enabled the emergence of new discourse networks where it interfaced with other media systems: trains, canals, ports, banks, offices, and so on. Time was no longer indexed to the speed of postal riders.[280]

Operations were determined spatially: at the cost of mental exhaustion and repetitive strain injury to arms and wrists, known as 'telegraphic paralysis', the telegraph enabled the instantaneous copying of data from one point in space to another. The elision of distance from communication depended on material connections between all points of the network. In telegraphic systems, electrical current 'carries' a message, but no singular 'thing' is transported, as in the postal system. The physical medium is the 'connection' itself. For customers and telegraphers, the wire, the electromagnetic switching 'key', and the printers and the sounders that it interconnected were mere instruments. From the perspective of media, the position of telegraphers and customers were assigned by the spatial dimensions described by the line itself, which determined the operations required to copy information from one point to another, using patterns made from the two possible states (on/off) of the electrical circuit.[281]

[279] Marshall McLuhan, *Understanding Media: The Extensions of Man* (London, New York: Routledge, 2001), 269.

[280] Markus Krajewski, *World Projects: Global Information Before World War I*, trans. Charles Marcrum II (Minneapolis: University of Minnesota Press, 2014), 1–32.

[281] Vismann, 'Cultural Techniques and Sovereignty', 91.

What later became known as 'line-tapping' (in respect of telephones) first occurred in England very soon after the nationalisation of commercial telegraphy in 1870. Once it was placed under control of the General Post Office (GPO), an extensive expansion of telegraph lines and stations took place, bringing lines to areas remote from the train lines and stations where the telegraph originated. Discontent arose amongst telegraphers in relation to their new working hours, conditions of employment, and long-term remuneration.[282] In 1871, they sought to organise a strike. As they had no union at that time, the strike had to be secretly organised. The telegraphers used the network itself to plan a collective walkout at multiple sites across the network, creating a sudden and uncontrollable nationwide disruption to communication. But GPO managers learned of the plan.

In an internal report to the Postmaster General, Frank Ives Scudamore (in a file now stored in the British Telecom (BT) archives)[283] it was explained that the strike's leaders were suspected to be based in the Liverpool and Bristol offices, but that they could not be precisely identified. Apparently, the organisers were careful to check the identity of the operator on the other end of the line before signalling any sensitive information. A memo on file states,

> A combination of telegraphy clerks in different parts of the country is more easy (*sic*) than a combination of Post Office Clerks or Letter Carriers in different parts of the country, because the Telegraph Clerks can communicate with each other so freely on a wire, no matter what its length may be, as if they were sitting face to face in the same room.[284]

During daytime working hours the lines were too busy, and managerial supervision too intense, for conspiring on the lines. It was therefore at night that the management's spies went to work somewhere on the lines. Where and with what apparatus they tapped the line was not relayed to the Postmaster General, who was informed only that "they can be watched in a manner which I will not here specify at intermediate

[282] Fari, *Victorian Telegraphy Before Nationalization*, 195.

[283] 'Strike of Telegraphists 1872, POST 30/215' 1871, BT Archives.

[284] Minute to PMG, 28 November 1871, in ibid.

points." Handwritten notes taken contemporaneously at the interception site recorded the circuits targeted, the dates and times, and brief summaries of intercepted exchanges. A subsequent letter to the Postmaster General confirmed that the leaders had been identified and dismissed. With full details of the planned strike on hand, contingency plans were put in place, with army telegraphers ready to step in and operate the Post Office system should the strike go ahead.

In December 1971, the strike went ahead despite the dismissal of its leaders, and the army was ready for it. In order to ensure that army operators in position before the striking operators could react, Scudamore ordered that all press telegrams were to be delayed for several hours on the day the strike began. This delay in the reporting of the news caused a media outcry: it was taken as evidence of abuse of the new monopoly, a sinister form of press censorship resulting from governmental seizure of the means of telegraphic communication. In press reports of the strike that eventually were published, all recorded in the same file in the BT Archives, the secret tapping of the lines is not mentioned, but the delay in press telegrams is. The entire episode, apparently the first governmental line tap in Britain, appears in few historical accounts of the development of the postal system or telegraphy.[285]

The security of a telegraphic transmission system was thus primarily conceived as a physical problem concerning the material network. Landlocked countries learned early on to assume that all messages sent and received via international telegraph lines were vulnerable to electrical interception by means of simple line extensions, which could be installed unobserved at any point beyond the geographical border of the territorial state. But effective line-tapping required synchronisation, or rather, a solution to the temporal problem of the asynchronous information relationship between the sender and the interceptor. Without some additional information

[285] It is briefly mentioned by Charles R. Perry, 'Frank Ives Scudamore and the Post Office Telegraphs', *Albion: A Quarterly Journal Concerned with British Studies* 12, no. 4 (1980): 350–67; There is no mention in any of the major histories of the Post Office, such as Daunton, *Royal Mail*; A. M. Ogilvie, 'A New History of the Post Office', *The Economic Journal* 23, no. 89 (1913): 137–141; Hemmeon, *History of the British Post Office*; Duncan Campbell-Smith, *Masters of the Post: The Authorized History of the Royal Mail* (London: Penguin, 2012); Fari, *Victorian Telegraphy Before Nationalization*.

provided in advance that would allow one to correctly anticipate messages when manning a line-tap, an interceptor cannot anticipate when a discrete message will begin or end. Technical solutions to synchronisation problems emerged with the invention of automatic teleprinters in the 1920s, discussed below, but until then, 'interception' had to be conducted elsewhere.

3.2.3 Networked memory

As Henry James showed, the notion of personal authorship linked to epistolary literacy was challenged by the enigmatic structures of telegrams, which standardised the value of all words as it mechanised their transmission. Whereas letters had been charged according to distance travelled until 1840, and by standard stamps thereafter, telegrams, transmitted serially on electrical circuits, were charged according to the number of words they contained, which approximated the transmission time each message took up on the line. At that point, says Kittler,

> minimum signs release maximum energy. Hermeneutic theories, with their notion of context, are inadequate to such a calculus… Once there are telegrams and postcards, style is no longer the man, but an economy of signs.[286]

The individuality previously attributed to letter writers was absorbed by the technical standards of the medium, producing telegrams as a new form of depersonalised writing.[287]

The standardised telegram, however, allowed for smooth integration with the standardised operations of the post-1840 postal service, particularly given the recently-imposed address system used for postal deliveries from 1856 onwards. As standardised forms, telegrams could be handled as if they were posted messages. The physical isomorphism of telegrams and postcards is no accident, the latter were based on the former.[288] Both offered standardised textual message formats, calibrated for short and inexpensive communication.

[286] Kittler, *Discourse Networks 1800/1900*, 191–92.

[287] Siegert, *Relays*, 185.

[288] Ibid., 184.

The telegram was a versatile interface that could spatially extend the range of telegraphic communication beyond the physical parameters of wires and offices. As if it were a postcard, one could post a telegram message with an appropriate prepaid stamp at any street corner pillar-box. It would be collected, sorted with the rest of the mail, and sent to the sorting office's telegraphy station for transmission to another Post Office telegraphy station. There, a copy of the telegram would be delivered to its final destination as part of the normal mail delivery routine. Alternatively, one could have an urgent telegram hand-delivered by a Post Office messenger boy anywhere in the country, sometimes within minutes of sending it. Customers could simultaneously send multiple copies of a single message to several receivers, simply by listing them and their local offices on the form and affixing the correct number of stamps.[289] In short, telegrams, packets, letters, and postcards were treated as if they were the same thing: a message.

To correspond via telegraphy, one had to enter information into the prescribe form of the telegram. At a telegraph office, customers wrote messages onto printed pro-forma telegrams, and received replies on the same forms, written, and later typed, by the operator. The paper telegram forms allowed operators to queue up messages for serial transmission, and this in turn enabled the functional division of labour and time in telegraph offices. Facing the public were those who received and gave out both messages and money, in the back were those who translated and transmitted them on the lines. The telegram form contained a grid of boxes, one for each word, allowing customers and clerks to keep track of the charge and emphasising the discontinuity inherent in a medium that translated words into money. The telegram form established the parameters for textual communication to conform to the requirements of wire and electricity, and functioned as a means of storing up and processing time.

Telegrams also provided the telegraph system with an error checking function. Given that messages were charged per word, many people, particularly commercial users, relied on code books. They were most commonly used for economic efficiency rather

[289] These features influenced the decision to nationalise telegraphy, see '"A Report to the Postmaster General, July 1866" HIC 0197/005/033' 1866, BT Archives.

than secrecy. Some standardised codes were commercially published, others were specialised. They varied in length and complexity.[290] Governments developed codebooks in order to communicate with ambassadors overseas.[291] But because telegraphers were then using two codes – first, receiving text from customers written in nonsensical coded alphabetic text, then sending that as a Morse message, and perhaps receiving an equally nonsensical reply in Morse by return – they recommended repeating all coded messages back to the sender, in order to check for errors.[292] This doubled the cost of transmission, but it ensured accuracy. Provided the code had decreased the overall word count by more than half, it remained cost-effective. In order to conduct this error-checking, the paper forms and a ready supply of pencils were essential.

In this way, paper messages provided the entire telegraph network with a non-human memory system distributed throughout the network. All transacted telegram messages, the sediment of past transmissions, were filed and stored in at least two locations, the telegraph office that had sent them, and the one that ultimately received them. In media-technical terms, the telegraph's transmission protocols functioned by duplicating information. 'Sender' and 'receiver' exist where the information was processed into text and recorded on paper. Telegrams were stored in telegraph offices for a period of three months. Every day, new telegrams were filed and three-month old telegrams were destroyed.

The memory system took on another function. The three-month archive provided the customer with insurance; it meant undetected errors could be checked and corrected later, and that stored messages could be retransmitted or copied to other addresses in the network. But at the same time, it served a police function, providing a window of time for the reconstruction of events and the tracing of links made by past interactions. To enter telegraphic communication was to be constituted as an entry in the storage

[290] Gleick, *The Information*, 158.

[291] Christopher Andrew and Keith Neilson, 'Tsarist Codebreakers and British Codes', in *Codebreaking and Signals Intelligence*, ed. Christopher Andrew (London: Frank Cass, 1986), 6–12.

[292] Gleick, *The Information*, 158.

system of the GPO's memory, configured according to the parameters of the telegram form, and this particular temporality of telegrams altered the possibilities of 'interception'. Postal interception techniques were performed in the sorting operations required between sending and delivery of all letters, and the line-tapping techniques deployed against the striking telegraphers in 1871 placed a parasitic 'third' listener on the line, but depended on perfect synchronicity and knowledge of which line to target. Telegrams, by contrast, afforded interception after the fact.

In 1886, the Home Office obtained a legal officer's opinion on the legality of interception of letters and telegrams. In approving the power, subject to the provision of an interception warrant from the Secretary of State, the legal officer observed that telegrams:

> do not merely multiply communications but remain for some time as a record in the Post Office which, if necessary can be collected during that time without the person whose telegrams are examined finding it out and taking alarm, as is the case where letters are detained or appear to have been opened. Again, telegrams can be identified more easily than letters – a certain man is known to have gone to a certain post office, it will be easy to find out the telegram he has read without disturbing other telegrams or even delaying the delivery of the message. It is obvious therefore that these telegrams in the Post Office constitute an immense resource for police investigation only if it is proper they should be used for this purpose.[293]

In contemporary terms, the Post Office afford the Home Office a 'back door' into a storage facility, containing hundreds of thousands of discrete indexed units of already-processed 'data at rest'. There was nothing to learn from the materiality of a telegram, in the way that one could study the unconscious signs visible in the materiality ascribed to letters, like the paper, the seal, the spread of ink, the signature and the handwriting. Nor was there anything personal about the messages themselves. All telegrams were designed to be identical, except in the spaces where

[293] 'Telegraphs: Interception of Letters in Criminal Case. L.O.O.797 as to Exercise of Power by Secretary of State HO 144/164/A42354' 1886, 1, National Archives.

the 'customer' was differentiated by whatever variables they entered. An example of a telegram interception warrant found in the Home Office records in the National Archives, this one prepared on 12th January 1888, reads:

> Sir, I hereby decrie and authorize you to forward to this office copies of any telegrams which may during the last three months have been sent by Major Teufler to a person of the name of Lane, or to a person of the name of Edward, at Birmingham, London, or old Charlton; or to any person at Birmingham from the following telegraph offices.
>
> New Brompton, Kent
>
> Old Brompton, Kent
>
> Brompton Barracks, Chatham,
>
> Chatham,
>
> Rainham.[294]

The delivery possibilities afforded by the telegraph system were directly transposed into new options for intercepting communication. Selection criteria referred to the addressing options used by the telegraph network: names, dates, addresses, and local telegraph offices. Warrants simply listed targeted names and listed the local telegraph offices where stored telegrams were to be checked for matches.

A specially-assigned clerk at GPO headquarters received all such warrants from the Home Office and arranged for any relevant telegrams to be forwarded on to him (whether by courier, post, or re-transmission is unclear). The clerk signed his name on a cover letter, added the date of the relevant warrant, and sent the telegram on to the Home Office. Telegrams were copied at the Home Office onto standard pre-printed Post Office Telegram forms by hand,[295] then returned to the Post Office and filed

[294] 'Out Letters to the General Post Office Regarding the Interception of Telegrams and Letters (1887-1899) HO 151/7', The National Archives, Kew.

[295] 'Disturbances: Warrant Issued for Production of Telegram Addressed to Anarchist Prisoner at Stafford from the "United Anarchist Groups, London" HO 144/242/A53582B' 1892, National Archives.

alongside the warrant.[296] (see figures 6 & 7) Warrants no longer only directed time-pressured operations in postal sorting rooms, which were locked and secure spaces. Now, they were the condition under which telegrams could be accessed in the GPO's memory. The time allowed for each message to be intercepted was of an order of months, rather than minutes. The symbolic positions of sender, receiver, and interceptor were confirmed in legislation. By section 20 of the Telegraph Act 1868, the privacy of telegrams was given protection in law analogous to the existing status of letters. Section 20 prohibited the disclosure of a telegram to anyone but the named sender or receiver, except where in the course of a postal worker's 'duty', meaning under instructions from above.[297]

3.2.4 Empire cables

The first undersea cable was laid between France and England in 1851 and the first functional transatlantic cable was completed in 1866, eight years after the first unsuccessful attempt. The British led the way in submarine cable technology thanks to their monopoly over gutta percha, then the only available waterproof insulator, which they took from the jungles of their colonies in Sumatra, Malaya, and Borneo.[298] Gutta percha transformed the ocean from a technical problem into a vital asset that prevented line-tapping. From the 1870s, the British government invested heavily in international telegraph companies and regulated their operations via licensing conditions. Britain soon displacing Belgium as the hegemonic state in the International Telegraph Union.[299] The global cable network was inseparable from British colonialism. State investment was driven by the desire to secure and connect up communication between sites of colonial rule and the metropolitan centre in London.[300] Cable stations and cable routes were selected to achieve a balance between the social and the geographic with regards to "existing populations and infrastructure

[296] 'Telegraphs: Mode of Transmitting Letters Intercepted under Warrant of Secretary of State HO 144/203/A47869' 1887, National Archives.

[297] See section 4.5 on the form of the telegram warrant.

[298] Nicole Starosielski, *The Undersea Network* (Durham: Duke University Press Books, 2015), 32–33; Arthur C. Clarke, *How the World Was One: Beyond the Global Village* (London: Gollancz, 1992), 103.

[299] Fari, *Victorian Telegraphy Before Nationalization*, 207.

[300] Starosielski, *The Undersea Network*, 34.

and the affordances of an area's natural and social topography".[301] The 'Empire Cables' became

> the cerebrospinal axis of our political system … through which would freely pass the sensory impressions and the motor impulses of the British people.[302]

Cables were defended on several fronts. The Committee on Telegraphic Communication with India in 1891 contemplated the risk that a syndicate of foreign state powers could, under cover of commercial aliases, buy the shares of the Eastern Telegraph Company and thereby "alienate" it from the Empire.[303] In response to this phantom financial threat, an 'all-red line' was devised an implemented, a submarine telegraph network controlled by the Empire and divorced from the market, which would land only on safe British shores.[304] Its realisation became a "virtual fetish" for the Colonial Defence Committee.[305]

Physical threats to undersea cables came from underwater topography, sea animals, earthquakes, ships' anchors, and deliberate dragging and dredging by enemy vessels. Yet the positions that humans operated within the apparatus remained the critical point of maximum risk and, therefore, maximum security. Human-operated relays and junctions were necessary for the network to function. They had to be distributed around the network to operate relays, the locations of which was determined by the maximum distance possible to send a clear signal before the electrical resistance of the cable made the signals sent by artificial current indistinguishable from the electrical noise caused by the earth's magnetic field. As such, human relay operators had to be produced according to the Empire's standards. Cablemen were typically drawn from the metropolitan British middle classes. They trained at a specialised school in

[301] Ibid., 31.

[302] Sandford Fleming, quoted by Simon James Potter, ***News and the British World: The Emergence of an Imperial Press System, 1876-1922*** (Oxford: Clarendon, 2003), 65–66.

[303] Paul M. Kennedy, 'Imperial Cable Communications and Strategy, 1870-1914', ***The English Historical Review*** 86, no. 341 (1971): 728–752.

[304] Hugh Barty-King, ***Girdle Round the Earth: The Story of Cable and Wireless and Its Predecessors to Mark the Group's Jubilee, 1929-1979*** (London: Heinemann, 1979), 148.

[305] Kennedy, 'Imperial Cable Communications and Strategy, 1870-1914', 731–33.

Porthcurno, Cornwall, which now, in the age of fibre optics and digital processors, serves as a museum to the telegraphic age. Cornish locals provided the telegraphers with servants.

Cable work was a form of imperial duty. Cablemen lived apart from local towns (assuming any were nearby), and typically reported feeling more connected "to a distant homeland and other cablemen instead of to local residents", according to Starosielski. They inhabited:

> …a social structure that kept the men from becoming attached to specific locations; stabilized flows within the network; and prevented information, expertise, or resources from diffusing to individuals outside the cable colony.[306]

They were discouraged from marriage, drinking met with disapproval, and any "improper language" or "quarrelling on the instrument" was strictly forbidden. Magazines and newsletters circulated to produce an "imagined cable community", which also disciplined their work. Through the apparatus itself, individual errors in transmission were remotely tracked and recorded in order to evaluate their reliability as they passed 'cablegram' messages from station to station, servicing different circuits.[307]

The physical protection of remote relay stations, some on uninhabited islands, entered naval and military planning. Cable routes and Royal Navy patrols were aligned. Redundancies were added to the network by linking stations in triangular fashion, so that the loss of no single station could disrupt the global network. Licencing conditions ensured that private cable operators complied with the requirements set by the Cables (Landing Rights) Committee of the Board of Trade. Cable huts were situated so as to be invisible from the sea, ideally in sheltered harbours, otherwise, "where there is a possibility for guns or rifles alone to make it defensible".[308] For the first generation of cable landing stations, geographical isolation was threatening,

[306] Starosielski, *The Undersea Network*, 100.

[307] Ibid., 106; David Souden, *Voices Over the Horizon: Tales from Cable and Wireless* (Cambridge: Granta Editions, 1999), 88–112.

[308] 'Defence Requirements for Cable Landing Sites' 1910, BT Archives.

because the station would be sited far from local garrisons and sources of food and water in case of attack or blockade.[309]

As Starosielski shows, securing submarine cables from breaches, interception, and noise required a complex set of governmental strategies.[310] The imaginary evaporation of space in the global communication systems of Empire resulted from the intense application of local colonial control, and the close scrutiny of all human interfaces with the undersea cables. The cables – critical elements in the production of globalised society – in turn produced globalised threats. According to the logic of liberal security, all such threats had to be anticipated and foreclosed. Transoceanic communication involved imperial property, at least until the development of wireless media. The entire network was therefore physically designed to restrict access to the machinery to those imperial subjects deemed worthy and reliable enough to enter its operations.

3.2.5 International cable interception

Mass interception of telegrams, known as 'cable censorship', began along with postal censorship on 2nd August 1914, days before the formal outbreak of the First World War. The primary aim in the beginning was to ban enemy diplomatic traffic altogether rather than to selectively intercept it. Censors were installed at London cable offices and in Porthcurno, Cornwall, which had by then become a relay hub for the world's international submarine cables. The submarine network, according to an internal report prepared after the war, constituted "a single field which offers facilities for the use of circuitous routes apparently remote from the sphere of action."[311]

As with the postal system, censorship demonstrated the inherent interception capability of the network, and the labour required to do it. All telegrams processed at state or commercial telegram receiving stations and relay hubs around the world were checked according to the censorship protocols, with potentially useful telegrams

[309] Later, after decolonisation, the inverse logic applied. Local populations became part of the threat and isolation came to be considered a source of security, see Starosielski, *The Undersea Network*, 110–15.

[310] Ibid., 95–111; Kennedy, 'Imperial Cable Communications and Strategy, 1870-1914'.

[311] *Report on Cable Censorship during the Great War (1914-1919)* (London: General Staff, War Office, 1920), 9–10.

selected and passed on to naval intelligence for closer inspection. The initial rules for censors were: all languages other than English and French were banned, all diplomatic and private codes were banned (except those used in communication between allied or neutral governments and their diplomats abroad), all commercial codes were banned (they were gradually reintroduced, provided the codes were first registered and approved and thus transparent to government), and all commercial traffic was automatically delayed by up to forty-eight hours so as to diminish the utility of any secret messages smuggled through.[312] To apply these protocols every message had to be checked and categorised.

Censorship led to one of the most politically charged diplomatic incidents of the war. When war was formally declared (by telegram), a cable ship conducted Britain's first offensive action. On the night of 5th August 1914, German submarine cables to the Azores, North America, Vigo, Tenerife, and Brest were dredged up and cut in the North Sea. Russia cut German overland cables to the east. By 1915, Germany was wholly dependent on longwave radio transmission for long-range international communication. Knowing the risks of radio interception, Germany used the ostensibly neutral Swedish embassy to smuggle encrypted messages via cable to its embassies in the Americas. The United States, still formally neutral, secretly agreed to bend its own rules against enciphered diplomatic traffic to allow Germany to send encrypted traffic via American channels. Britain controlled the relays from Europe to America, but the ruse worked. Swedish diplomatic traffic sent by cable was not checked by British censors as it was relayed through British cable stations. But when it emerged that the Netherlands, formally neutral, were providing Germany with imported materials to relieve the British naval blockade of German ports, the British began closely checking *all* cable traffic. The aim was to pressure neutral European countries into ceasing trade with Germany,[313] but as an unexpected consequence, known German codes were spotted amongst what was supposedly Swedish diplomatic traffic. Initially, the British complained to the Swedish ambassador about

[312] Daniel R. Headrick, *The Invisible Weapon: Telecommunications and International Politics, 1851-1945* (Oxford: Oxford University Press, 1991), 141.

[313] Ibid., 147.

facilitating German communications, but then decided to treat it as a source of intelligence. On 16th January 1917, the 'Zimmerman telegram' was intercepted. Addressed to the Mexican government, it promised that if the Mexicans were to attack the United States in response to a US declaration of war against Germany, Mexico would eventually be rewarded with Texas, Arizona, and New Mexico. The telegram helped persuade President Wilson to declare war on Germany.[314]

Commercially speaking, censorship was extremely profitable for the cable companies who had to enforced the rules. The general ban on private codes meant that the average number of words per message increased from twelve to twenty-one, and government communications via telegraph increased 327 per cent. To accommodate this, cable bandwidth was effectively requisitioned during the war, which further drove up prices for other users of what was effectively a monopoly. The backlog was such that to send a private telegram from London to Calcutta took around seventeen days in 1918,[315] which ultimately incentivised telegraph companies to invest more seriously in radio technology as an alternative to cable routes for commercial traffic.[316] Additionally, it meant that governmental had to develop an intense and permanent interest not only in the security of the physical infrastructure of the network, but also in the economics of transmission.

In a sense, cable censorship never ended but merely shifted in intensity and tactical aims. The Admiralty's intelligence team known as 'Room 40' in the war was renamed Government Code & Cypher School (GC&CS). Control over the new organisation was transferred from the Navy to the Foreign Office. Publicly described as a new department for securing British governmental communications and codes, it was in fact tasked with five main functions. First, organising, developing, and coordinating the wireless interception and analysis of foreign communications from various

[314] Ibid., 168–69; David Paull Nickels, *Under the Wire: How the Telegraph Changed Diplomacy* (Cambridge, Mass.: Harvard University Press, 2003), 148–52; Barbara W. Tuchman, *The Zimmerman Telegram* (London: Constable, 1959).

[315] Barty-King, *Girdle Round the Earth*, 175.

[316] Ibid., 180–85.

governmental sources across the Empire, which fed back information to the office in London via a dedicated network of secure telegraphic and, later, teleprinter links.[317] Second, receiving and processing radio and cable intercepts of international diplomatic correspondence passing between foreign countries. Third, processing and examining radio signals picked up from foreign armies and navies at a growing number of British radio receiving stations around the world. Fourth, helping develop and coordinate technical methods for detecting radio broadcasts from clandestine agents broadcasting from within the UK.[318] Fifth, analysing intercepted commercial cable traffic.

To this end, all commercial cable companies operating in Britain were required to continue handing over copies of all telegrams to Naval Intelligence each day for 'vetting'. On 16th December 1920, the President of Western Union, Newcomb Carlton, informed a US Senate subcommittee of the practice. Carlton said he had been told that the content of messages was not deciphered, and that the government simply wanted "to keep general track of who was cabling" in order to gain "an inkling of pending disorders", connected with "Irish unrest" and "Bolshevik propaganda".[319] In response, the Official Secrets Act 1911 was quickly replaced by the Official Secrets Act 1920. The Home Secretary immediately issued warrants under section 4 of the Act, which required telegraphic companies to continue providing their daily traffic, and to maintain official secrecy.

In 1944, the first head of GC&CS, Alastair Denniston, wrote a brief, secret history of the organisation, first published is 1986. It is worth quoting at length:

> Throughout the twenty years (1919-39) it was our aim to make this procedure work smoothly with the companies (British and foreign). It was undoubtedly a nuisance for them to have to send all their traffic in sacks to an outside

[317] A. G. Denniston, 'The Government Code and Cypher School Between the Wars', in ***Codebreaking and Signals Intelligence***, ed. Christopher Andrew (London: Frank Cass, 1986), 48–49.

[318] Ibid., 54–61.

[319] James Bamford, ***The Puzzle Palace: A Report on America's Most Secret Agency*** (New York: Penguin, 1983), 415–16.

> department, and I have always considered that the credit for smooth working and no questioning should go to Maine [H.C.S. Maine – his deputy]. To carry out the work of sorting and copying we took over a comparatively small body of GPO lower grade staff that were accustomed to this work. Our aim was to inconvenience the companies as little as possible, and throughout we tried to let them have their traffic back within twenty-four hours. We only had to sort out and copy government traffic and occasional suspicious characters in whom our security authorities were interested. I believe we never failed to return all the traffic, though many million telegrams must have passed through our hands… when the state of unrest in the world became intense, from 1935 onwards, it was found that the ten days delay granted by the warrant became intolerable. Maine was able to cut it down to twenty-four to forty-eight hours in the case of foreign companies, and to instant service, where necessary, in the case of the CTO [Central Telegraph Office] and Cable and Wireless. Between us and the companies there has never been any question as to why we wanted the traffic and what we did with it. The warrant clearly said scrutiny, and the traffic arrived back apparently untouched within a few hours. I have no doubt that the managers and senior officials must have guessed the true answer, but I have never heard of any indiscretions through all the years with so many people involved. In short, barring the delay, we always had as good service of cables when we dealt direct with the companies as in the periods of censorship.[320]

Interception was enacted by picking up sack loads of copied telegram forms in a van each day. Presumably, they were processed by hand according to lists of selection criteria. The secrecy of the so-called 'cable-vetting' arrangements was maintained until 21st February 1967, when journalist Chapman Pincher published a story under the headline, "Cable Vetting Sensation" in the *Daily Express*.[321] Apparently, the

[320] Denniston, 'GC&CS Between the Wars', 64–66.

[321] This sparked a crisis over governmental control of classified information in relation to mass media, see Christopher Moran, ***Classified: Secrecy and the State in Modern Britain*** (Cambridge: Cambridge University Press, 2012), 143–47; 'Report of the Committee of Privy Counsellors Appointed to Inquire into "D" Notice Matters' (London: UK Parliament Prime Minister's Office, 1967).

original warrants had not been updated in almost fifty years, and the Secretary of State responsible in 1967 was unaware of their existence when the story was published.[322]

As it was domestically, so it was internationally. Interception of global cable traffic did not take place in the wires, but on paper. It was carried out by rifling through paper forms one at time, human processors visually selecting individual messages according to standardised content. Below, we shall see how cable media changed.

3.3 Telephones

3.3.1 Operators

When the first telephone networks were installed by private companies in Britain beginning in 1877, a year after Alexander Graham Bell's first call, it was less than a decade since the government's compulsory purchase of all private telegraph networks. There was a sense that the government had overpaid for the monopoly, and little appetite for a repetition of the problem with telephones. But the governmental imperative to set the conditions of communication remained. Hence the Postmaster General simply asserted that a 'telephone' company and 'telegraph' company were the same thing, sending messages by wire apparatus. There was thus no significant legal distinction between the transmission of voice calls and the transmission of telegram messages, and therefore that the power of compulsory purchase in section 4 of the Telegraph Act 1868 automatically applied.[323] In *Attorney-General v Edison Telephone Co of London Ltd* (1880) LR 6 QBD 244, it was held that the GPO's purchasing power:

> … was intended to confer powers and to impose duties upon companies established for the purpose of communicating information by the action of electricity upon wires, and absurd consequences would follow if the nature and

[322] Gordon Corera, ***Intercept: The Secret History of Computers and Spies*** (London: W&N, 2015), 96. On the warrants, see 4.4.4.

[323] 'Telegraph Act 1868', accessed 31 August 2017, http://www.legislation.gov.uk/ukpga/Vict/31-32/110/contents/enacted.

> extent of those powers and duties were made dependent upon the means employed for the purpose of giving the information.[324]

For the purposes of the Post Office monopoly, then, a telegram and phone call did the same thing: information transmission via electrical wire. Medium and messages coincided in the legal definition of the object under consideration. Britain's telephone networks were first licensed by the GPO, then nationalised in 1910 (with the exception of Hull, which still has an independent network today).[325]

In his study of the development of relay communication systems, Bernhard Siegert draws attention to the gendered distinctions that were built into technical networks. For technical reasons, a third person was required whose voices could not enter into telephonic communication as active subjects. Just as the typewriter replaced the traditional scribal functions of a trained male secretary or scrivener with the passive female typist, female telephone operators were assigned the passive role of lending their voices to the telephone company. To make a telephone connection, the operator was required, as Siegert observes, to renounce the 'I' of vocalised self-reference, to abandon the personal sovereign position of the Cartesian subject. Men, Siegert writes, were "complete and consistent failures" as switchboard operators. This he suggests should be understood as inability to relinquish ego, as men "continued to train for personal responsibility and the ability to appropriate language. Consequently, women became indispensable as third persons." Their voices were chosen not only as a source of untapped labour, but also because only a feminine voice could occupy the depersonalised position of speaking on behalf of the switching equipment: "Operator. Number please."[326] And yet this depersonalised voice occupied the position of power over every connection she implemented.

[324] *Attorney-General v Edison Telephone Co of London* 6 QBD 244 (1880); The problem was that the American companies involved held the patents for telephone equipment. The Post Office might be able to purchase the network, but it could not provide telephones. As such, a thirty-one-year licence arrangement was agreed, with 10% of the profits to go to the GPO, see 'When a Telephone Conversation Was Actually a Telegram in the Eyes of the Law', *BT.com*, accessed 25 May 2017, http://home.bt.com/tech-gadgets/when-a-telephone-conversation-was-actually-a-telegram-in-the-eyes-of-the-law-11364121187126.

[325] Hemmeon, *History of the British Post Office*, 219–36.

[326] Siegert, *Relays*, 190.

The operator, like the telegrapher, occupies the invisible position assigned to the interceptor. The imaginary integration of the operator and the network disguised the governmental capacity built into the position she occupied. Switchboards enabled many thousands of possible end-to-end connections to be organised and monitored from the operator's seat. Whereas the telegraph eliminated space in regards the transmission of typographic symbols, telephones eliminated space for oral communication, and whereas the telegraph charged per symbol, the telephone charged by dividing time into units.

The point of a telephone network is that any handset can connect with any other, through a network of switching points that set up relay links between the two ends of the call. In order to have access to every call coming or going from a given telephone the interception point must be somewhere between that telephone and the first exchange switchboard. Before the domestic network was converted to automatic switching between 1958 and the late 1960s, callers who wished to dial outside their local area had to connect via an operator at their local exchange, which is where the tapper had to be. To 'tap' a telephone line is, electrically, the same thing as 'tapping' a telegraph cable. One simply connects a second line somewhere on the target's circuit with an amplifier and media-specific receiver attached; for telephones, that is a speaker or headphones. An officer from the Post Office Investigations Branch perched next to the female operators in local telephone exchanges, plugging headphones into a jack on the switchboard in order to monitor the target's call. This was the same technique used for telephone engineers to check for problems on a line, and perhaps gave rise to the clicking sounds that apparently indicated when a stranger was on the line. Operators processed calls, giving them the power to interrupt, to listen along, or to suddenly cut the connection.

3.3.2 Audio storage

Telephone tapping was barely utilised at all until recording technology advanced sufficiently. Tapping a telephone call as it occurs means constant careful listening even before anything interesting has occurred. When a call does come on the line, it is most likely without context, and certainly without the opportunity for the interceptor to intervene in the conversation and perform the usual reciprocal error checking that conversations take for granted. There is too much uncertainty in telephone communication, too much capacity for surprise. It is too informative to be listened to and processed meaningfully at once. Like all aural media, the telephone "registers real sounds rather than translating them into phonemic equivalencies as an alphabet does".[327] One has to be prepared to listen along to the real sounds made by others. As McLuhan puts it, "the telephone demands complete participation, unlike the written and printed page".[328]

While the call is taking place, and only while the call is taking place, one must be ready to pay attention. If an unknown language or code is used, which was a simple matter to arrange, the call is incomprehensible. If a target's call turns out to be completely unrelated to the reason for the interception, or made by another member of the household, the whole effort is wasted. Although early telephone networks required pre-booking lines in order to ensure they were available to connect particular long-distance calls, one generally did not know in advance whether the calls one was about to hear would be interesting or not. The game was not worth the candle. Frederick Booth, an MI5 'special censorship' men at the Post Office, who gave evidence regarding letter interception during the 1914 trial of Karl Gustav Ernst,[329] recalled,

> The only method of recording the conversation was by handwriting. The results were not accurate or useful and the written returns showed increasingly the remark 'Conversation in a foreign language – not understood.'[330]

Not understood, or simply not worth the patience and mental effort required to understand.

Intercepting telephone calls meant recording them. Reusable and reliable recording technology with sufficient fidelity to clearly record calls, which could be electrically

[327] Kittler, *Discourse Networks 1800/1900*, 232.

[328] McLuhan, *Understanding Media*, 291.

[329] See section 2.5.

[330] Andrew, *The Defence of the Realm*, 134.

stopped and started automatically when a called was connected and disconnected, enabled the implementation of functionally plausible telephone 'tapping' procedures.

The first home answering machines appeared in the late 1920s. One such machine, Recordaphone, was briefly available between 1927 and 1929, advertising itself as:

> The final link in the chain consisting of the Telephone, Telegraph, Wireless, Gramophone, and other means of transmitting the spoken word or sound. It is compact in design, simple to operate, and occupies no more space than a typewriter. It will record a telephone conversation between two or more persons, faithfully registering every inflection of the voices…[331]

As all telephone circuits in Britain were property of the General Post Office, it was for the Post Office to decide which machines could be affixed to its lines.[332] Recordaphone used wax cylinders, which proved to be less successful than anticipated. The Dictaphone Company ultimately emerged dominant, producing the first plastic recording cylinders in 1947, and magnetic tape recording systems shortly after. It was MI5's Frederick Booth who made secret arrangements with the Dictaphone Company for procuring a dedicated recording system for recording telephone taps.[333] By 1952, all local police stations in Britain were equipped with magnetic audiotape recorders for application to selected lines at the local exchange by Post Office engineers.[334]

3.3.3 Centralising tapping

When electromechanical exchange systems were replaced by electronic exchanges during the 1960s and 1970s, they were assembled so as to also enabled any telephone line on the network to be remotely selected for tapping. Rather than dispatching an investigator to the local exchange with headphones and a notepad, or a portable recording system with tapes that had to be regularly collected and replaced, the automated network directed signals on tapped lines to secure tapping locations,

[331] 'Devices for Recording Telephone Conversations POST 33/904' 1930, BT Archives.

[332] Ibid.

[333] Andrew, *The Defence of the Realm*, 135, fn 108.

[334] Patrick Fitzgerald and Mark Leopold, *Stranger on the Line: The Secret History of Phone Tapping* (London: The Bodley Head, 1987), 64.

where recording and transcribing could take place at a pace set by the interceptors, not their targets. As in the old electromechanical exchanges, each subscriber's circuit joined the telephone network at a main distribution frame in their local exchange. The frames were standardised, each measuring ten by thirteen feet. They linked all incoming lines onto a grid of electronic contacts. Each contact point was assigned a sequentially determined telephone number. In order to intercept all calls on a given line, the interception point has to lie between the telephone receiver and the distribution frame, the last point through which every signal must pass when connected to a particular line. All distribution frames were located in secure GPO buildings, closed to the public and guarded.

Investigation Branch engineers, who held the rank of Executive Engineers, would arrive early in the morning, before the bulk of staff had arrived to work. Their senior status meant they could direct any other workers present to leave while they completed their work.[335] Tapping a line simply involved attaching a red jumper cable to a standard socket on the main distribution frame, where the target line connected to it. The jumper was practically unnoticeable amongst hundreds of criss-crossing wires. A red cable was used, as on every 'special service' line, as a warning sign to local telephone engineers not to disconnect it. Red jumper cables did not necessarily mean interception; many were put in place to indicate vital services that were not to be disconnected, such as doctors' surgeries or business's data services. But as all intercepted line installations were logged in each local exchange as 'Defence Circuits', it wasn't hard to guess what they were for. While the subscriber's circuit connected as usual across the distribution frame into the mechanical exchange unit that selected and connected circuits according to the number dialled, the interception cable carried the signal into a spare outgoing line. Each local exchange had at least twelve dedicated lines running via the national trunk lines to the centralised tapping centres in London. Interception capacity was built into the fabric of the telephone network.[336]

[335] Ibid., 62–64.

[336] I am grateful to a former BT engineer who explained this process to me, see also Campbell, 'Big Buzby Is Watching You'; Fitzgerald and Leopold, *Stranger on the Line*, 62–64.

Telephone tapping became an ever-higher intelligence priority as encryption standards on telegraphic and wireless communications progressively improved throughout the Cold War.[337] When the network was rebuilt, all MI5 lines ran to recording and transcription rooms located on the upper floors of Leconfield House, London, where a team of women transcribers, fluent in Russian, worked on producing typed highlights. An MI5 case officer on requesting a line tap would provide the Transcription Department with a written brief, detailing the sort of intelligence he thought might be obtained from the intercepted audio, then they then scanned the conversation for the passages corresponding to the brief. This they did by first randomly sampling acetate recording discs at various points, listening for clues that useful information was being discussed at that part of the recording. They marked the disc with chalk where there was something potentially useful to transcribe, then went back over the recording to make the transcription.[338] By the 1970s, all tapped telephone lines were channelled into 'Tinkerbell', an anonymous-looking Post Office building that stood on Ebury Bridge Road, Chelsea. There, up to a thousand individual lines could be simultaneously intercepted. Computers filtered calls according to the particular number each target dialled, so as to eliminate trivial calls and only record potentially interesting connections.

3.3.4 Metering

It was also possible to produce an individual transcript of numbers called in order to identify networks of communicants. Ordinarily, telephone exchanges did not record the numbers dialled by each subscriber until digital exchanges were installed in the 1980s and 1990s. Before then, bills were calculated via analogue meters at the local exchange, which automatically counted units of time that each line spent on outgoing calls. The meter was calibrated to advance at variable rates, mechanically adjusted according to the time of day and the distances implied by dialling codes. The meters were physically attached to distribution frames and arranged in a uniform grid. They were photographed on a quarterly basis in groups of a hundred. Each subscriber's bill

[337] Richard Aldrich, *GCHQ* (London: Harper Press, 2011), 147.

[338] Wright, *Spycatcher*, 44–47.

was produced by magnifying the image and deducting the previous quarter's meter reading from the new one in order to calculate the units owed.

Occasionally, customers queried the accuracy of their bills, in which case a Meter Check Printer (MCP) was attached to their line. The MCP responded to the same electromechanical pulses that delivered call switching instructions. As an outgoing number was dialled, the MCP printed each digit, along with the time of day and duration of the call. The police and intelligence services used 'metering', without warrants, to monitor how a particular line was used without recording or listening to the content of calls. By converting calls into a textual list of numbers, MCPs recorded data on patterns of use that could be collated, compared, and analysed, providing second-order usage data for conducting telephone traffic analysis. Such techniques are now performed automatically by computer analysis of digital telephone metadata.[339]

While the capacity to access the transmission of a telephone call was always inherent in the network – it was the operator's function – interception always involves copying, and to that end synchronised recording media were required. Audio recording was, however, just an intermediate phase in the process. Transcription services were needed to turn recorded voices into text, and only then could it enter into the files through which human analysts processed intelligence information. That condition is only in recent years being supplanted by learning algorithms capable of recognising and automatically transcribing sound into text for the benefit of human operations.

Yet however much planning is involved, the time required for taping and processing conversations is not always available. In Belfast during the conflict in Northern Ireland (1968-1998), a different regime applied in a tapping centre run by the Army from the top of the Post Office's Churchill House.[340] Dubbed the 'hen house', it was the place of work for around thirty local women, recruited by the Royal Ulster Constabulary. Collectively, the station permanently listened 'live' to the telephone

[339] Fitzgerald and Leopold, *Stranger on the Line*, 206, 222–24.

[340] Campbell, 'Big Buzby Is Watching You'.

lines of targeted paramilitaries, politicians, and probably a few lawyers, journalists, and others, for information. The targets, who understood the capacities of the state, knew their telephones were probably being listened to. Small inflections, significant silences, unusual hints – these were the codes used, and knowledge of local accents and vernacular was essential.[341]

3.4 Radio

3.4.1 Common use of the ether

Wireless technology emerged as the result of a haphazard process of trial and error. Various engineers, scientists and commercial inventors tried to turn observable electrical wave effects into composite artefacts that could be calibrated and patented. Of the many attempts, Marconi's 'black box' was the most successful, and the most storied.[342]

Artificially generated radio waves can be modulated into ordered sequence, and thus carry information on frequencies that otherwise carry undifferentiated noise, signifying nothing but the entropy of the universe as it slowly unfolds itself. Information is the superimposition of patterns onto radio waves. Almost from the beginning, problems of security and secrecy drove investment and research into wireless technology, driving intense interest in a range of possible interception and evasion strategies. It was not clear to the experimental pioneers of radio that electromagnetic waves could not be bent to human will, and that radio transmissions were necessarily open to all receivers.[343] Attempts to impose end-to-end security onto transmissions to avoid interception drove the development of components that later found other uses.

[341] Aldrich, *GCHQ*, 499, in general terms, the scale of communications intelligence used by the security services in Northern Ireland is relatively under-researched.

[342] Sungook Hong, *Wireless: From Marconi's Black-Box to the Audion* (Cambridge, Mass.: MIT Press, 2001), 22.

[343] As Marconi recalled much later in life, see Kittler, 'Alan Turing', 183.

Marconi's early demonstrations of wireless telegraphy used spark transmitters and vertical antennas connected to basic 'coherer' receivers. Each 'spark' of the transmitter generated waves on multiple frequencies. The transmitter was used to broadcast damped radio waves in discrete bursts that mimicked on/off telegraphic cable signalling. But while the multiple resonance produced by spark transmitters allowed any un-tuned antenna in range to receive the signal, it had two major problems. First, super-positioning of waves of different frequencies meant that frequencies interfered with one another, limiting the overall transmission range. Second, just as any un-tuned receiver could pick up the signal, anyone with an equally primitive transmitter could generate interference. Nonetheless, after successful demonstrations at Salisbury Plain in 1896 and 1897 and the Bristol Channel in 1897, Marconi attracted investment from the Army, Navy and War Office. Compared to cable, the possibility of mobile reception made wireless technology a worthwhile investment, particularly at sea. By 1901, the year of Marconi's first confirmed transatlantic broadcast, there were already around one hundred shore stations and around two hundred ships communicating by wireless telegraphy.[344]

Secrecy and interception remained major concerns. First, syntonic harmony was held out as the answer. Syntony is harmonic resonance between the sender and receiver units; in short, it means that they are 'tuned' to the same wavelength. Tuning was initially developed with the express intention of eliminating both interference and interception.[345] The idea was that two sets tuned to a predetermined frequency would effectively produce a secret channel. But a series of public demonstrations of Marconi's syntonic technology soon demonstrated the opposite. Some were dramatically disrupted by rival radio entrepreneur Nevil Maskelyne, who embarrassed Marconi by beaming in a series of Morse code insults during one event. In another incident, Maskelyne set up a receiving aerial at Porthcurno, the cable hub of Empire, where the telegraphers were very grateful to receive live intercepted

[344] Norman Wymer, *From Marconi to Telstar: The Story of Radio* (London: Longman's, 1966), 22–23.

[345] Hong, *Wireless*, 89–100 Hong's book deliberately complicates the canonical stories about the invention of wireless technologies, which were from the beginning deployed in competing publicity-oriented demonstrations, disputes, and self-serving dramatizations. Here, we must risk once again reducing the complexity.

updates on the progress of Marconi's experimental transmitter at Poldhu, located a few miles up the Cornish coast.[346] Maskelyne showed Marconi that the 'airwaves' were open. Anyone could jump in uninvited, whether transmitting or receiving.

During the 1910s, generating and transmitting continuous syntonic waves over long range was almost prohibitively expensive. Longwave, as the low-frequency waves eventually became known, require transmission antennae commensurate to their wavelength, and must channel a large amount of electrical energy in order to transmit beyond the horizon. Shore stations could be supplied with sufficient electrical power, and giant antennae could be strung on pylons distributed across open spaces. This way, longwave signals could transmit over the horizon and across oceans. Ships, however, had a much more limited transmission range and therefore had to relay messages collaboratively on the open airwaves. Rudimentary rules and protocols were therefore required in order to bring order to the "common use of the ether", which is indifferent to geopolitical differences.[347]

Around the same time, audion valves were being configured to serve as both amplifiers and tuning oscillators in wireless sets. This triggered the mass production of cheap, small, and portable transmitters and receivers. Technology capable of sending and receiving signals over long range were suddenly affordable. Audion-based 'tube' radios, able to clearly pick up relatively weak signals, were marketed as one-way units build only to receive signals, and broadcasting was born. Wireless telegraphy "transmuted into radio."[348] The audion tube materialised the fact that end-to-end radio secrecy would never be established at the level of transmissions. Syntonic secrecy impossible, but in pursuing it, the capacity to 'tune in' was discovered. For radio systems, interception and reception are essentially identical: tuning hardware to oscillate syntonically in the presence of artificially generated electromagnetic waves

[346] See the chapter Tuning, Jamming, and the Maskelyne Affair in ibid., 89–118.

[347] The phrase appears in a memo from 1928, in 'Wireless: Interception by Amateurs on Shortwave POST 33/2905D' 1931, BT Archives.

[348] Hong, *Wireless*, 155.

carrying information. Rather than damped discrete waves, communicative messages became encoded via modulations in amplitude (AM), and, later, frequency (FM).

3.4.2 Juridical interception

By 1908, radiotelegraphy had generated concern within the Post Office as to whether or not section 2 of the Post Office (Protection) Act 1884, which updated the 1868 legislation criminalising interference with telegrams, was adequate. No change was made at that point; after all, the 'thing' that customers sent and received was still a Morse encoded telegram, regardless of whether transmission was via cable or wireless.[349] Thus in English law, for a while, the definition of 'telegram' included both telephones and radio transmissions.

With tuneable sets, frequencies were formally registered for different purposes, "just as a telegraphic address is registered".[350] Anyone tuning in to the same frequency would, within range, be able to receive the same signal. The regulation of frequencies and the establishment of rules for technical uniformity therefore became subject to governmental standards.[351] Unlike carefully mapped nodes on cable networks, wireless transmission bears no relationship to geographical distinctions. There could be no territorially defined 'all-red' frequency. Some international co-ordination was necessary.

At the third international radio conference, held in 1913 in London, state parties to the first International Radiotelegraphic Convention agreed that the wavelengths of 300m and 600m would be reserved for ship-to-shore and ship-to-ship communications for passing along "public correspondence". [352] All ships and all shore stations of states party to the convention would be constantly ready to receive and relay transmissions on these wavelengths, and would ensure their shore stations were connected to

[349] 'Radiotelegram Intercepted: Legislation to Enforce Secrecy POST 30/1904D' 1908, BT Archives.

[350] Hong, *Wireless*, 118.

[351] Ibid.

[352] Two preliminary conferences were organised by the ITU in 1903 and 1906, both in Berlin. For a complete list, see 'Complete List of Radio Conferences', *ITU*, accessed 8 April 2017, http://www.itu.int:80/en/history/Pages/CompleteListOfRadioConferences.aspx.

landline telegraph networks for onward transmission, regardless of the commercial company that initiated the transmission.[353] Standard lists of stations, universal Morse call-signs, worldwide hours of operation, and financial arrangements for the costs of transmission were detailed. Wireless operators were placed on constant 'listening watch', transforming sea traffic into a distributed network of moving relay points in a global commercial transmission system. Any ship or ship's owner that violated the Convention could face legal action. Ships hosting radiotelegraph operators from private communications companies, such as Marconi, became mobile telegram stations for passengers and police to communicate while in transit. The protocols enabled and accommodated a rapid growth in the volume of traffic; by the 1930s, radiotelegraph operators on different ships had to 'queue up' on their shared wavelengths, which constituted channels, each waiting for the chance to jump into the stream of traffic to transmit or receive their passengers' correspondence to shore stations.

The wireless 'network' was thus the effect of the protocols developed for the common use of radio wavelengths, fixed by international legal conventions. The law could not determine the status of the ether, so it instead determined juridical rules for operators. Licenses controlled access to the radio waves. Only licensed operators could participate in radio discourse, and only on the wavelength settings assigned them by the law. Licenses also distributed virtual addresses that referred not to any specified location or territory, but to the call-sign identity of the ship or station on the air. The legal convention was coupled to the technical operations of the network via the device of the license, which connected radio operators and their operations to the law. In the worldwide network of radio broadcast and reception, interception was produced as a purely juridical symbolic form, not a technical operation.

This point was crystallised at the next ITU radio conference, held in Washington D.C. in 1927, by which point audion technology and the exponential growth in radio

[353] 'International Radiotelegraph Convention, Signed at London, July 5, 1912. (London, 1912)', 187–189, see also Articles 8 and 9, accessed 8 April 2017, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.37.43.en.100.pdf.

enthusiasm saw contracting states introduce licensing systems for all radio operators, whether on ship or shore. Article 2 held:

> The holder of a license must undertake to preserve the secrecy of correspondence, both telegraphic and telephonic. Moreover, the license must provide that the interception of radioelectric correspondence other than that which their station is authorised to receive is forbidden, and that, where such correspondence is involuntarily received, it must not be reproduced in writing, communicated to others, or used for any purpose whatsoever.[354]

When using an open channel for correspondence, the moment of interception was not when the equipment receives a signal, or when the operator became cognisant of its content, which was inevitable, and frequent. Through the lens of the Convention's protocols, illicit interception had not occurred even if one had tuned to a wavelength outside the terms of one's license, or had received information not addressed to one's particular station. These were the legal preconditions of interception, but the primary act occurred at a media-technical level: writing down, communicating to others, or using information received under the proscribed conditions. In short, only when information was used could it be intercepted.

Interception required policing, particularly in respect of salvage vessels, which occasionally were penalised for offering unsolicited assistance to ships that reported mechanical difficulties back to their owners or fleets.[355] In effect, ships' radio operators were prohibited from responding to other ships' communication traffic. Only a ship's master, usually the captain, could order a radio operator to disclose signals against his legal obligation not to, in which case the captain became legally liable for any violation. Absent that, every message not specifically addressed to the ship had to ignored. In short, when transmissions were open to all, what had to be secured by law was the right to store or process information.

[354] 'International Radiotelegraph Convention of Washington, 1927 and General and Supplementary Regulations (Washington, 1927)', accessed 8 April 2017, http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.39.43.en.100.pdf.

[355] 'Radiotelegrams on Board Ships: Censorship Arrangements, Interceptions and Use of Radio-Telegrams by Salvage Vessels, Part 1 POST 30/2097' 1928, BT Archives.

The only exception was those transmissions prefixed by the letters 'SOS': the famous Morse sequence of *dot-dot-dot, dash-dash-dash, dot-dot-dot.* The SOS pattern is a strikingly obvious rhythm, it immediately grabs and 'tunes in' the conscious attention of otherwise disengaged radio operators. But at the same time, it has the juridical function of authorising the reception and disclosure of a message, and urgently responding to it. SOS suspends the interception norm by marking out universal emergency condition.

Armies, navies, and state intelligence agencies, of course, recognised no limits on what signals they received, occupying the position of sovereign receivers and universal listeners who stored and processes as much as possible. Yet radiotelegraphy presented new opportunities for resisting governmental control. On the evening 8th May 1932, unknown persons came aboard the ship SS *Reina del Pacifico*, a Liverpool registered ship, while it was docked in the Chilean port of Arica. They handed the ship's wireless office a typewritten message for transmission in Spanish and paid 205 Chilean pesos. As the ship was in port, transmission was not permitted, but the following morning the telegram was transmitted from sea at 10am, addressed to Ilo Receiving Station, Peru, on a wavelength of 700m. The message was noted on the log and filed away in the usual manner. On 14th May, the ship's commander was notified that the vessel had been fined 500 Peruvian pounds. Unbeknownst to the wireless operators, who spoke no Spanish, they had transmitted a 'Marconigram' addressed to the "Commanders General, Trujillo, Peru, from Commander Jimenez", giving them the signal to begin an armed insurrection: RISING UP HEALS OLD WOUNDS… THE HOUR IS DECISIVE FOR PRESENT AND FUTURE OF FATHERLAND. YOUR COMRADE EXPECTS ALL TO DO THEIR DUTY.[356]

3.4.3 Shortwave

By 1929, ostensibly to police radio regulations in light of developments in shortwave radio technology, new 'interception stations' were built. A GPO memorandum of 29th

[356] 'Radiotelegrams on Board Ships: Censorship Arrangements, Interceptions and Use of Radio-Telegrams by Salvage Vessels, Part 2 POST 30/2098' 1933, BT Archives.

February 1929 regarding a new interception hut at St Albans records that it was "for the purposes of ensuring that amateurs do not wander outside their allotted bands, and of detecting illicit transmitting stations".[357] However, the development of shortwave also meant that radio traffic from locations previously out of range could be intercepted and logged. Records of transmissions received at the St Albans interception station list signals picked up from various transmitters all around the world. The record-keepers scanned all available frequencies, noting time, language, signal types, and the likely location and topic of intercepted transmissions. Where possible they translated messages into English. As soon as shortwave radio became a functioning technology, monitoring became a standardised governmental practice.[358]

Shortwave radio uses focused beam antennae to generate wavelengths under 100 meters long. Signals in the shortwave band were discovered to reflect and refract from gases in the electrically charged band of the atmosphere known as the ionosphere. By 'skipping' signals between the surface of the planet and the atmosphere, shortwave transmissions could connect opposite sides of the planet. Because energy from the sun heats the gases in the ionosphere, certain shortwave radio 'links between fixed points are only available at certain times of day, and can be disrupted by bad weather. Improvements in engineering and predictive meteorological science helped make the system more reliable.

By the late 1920s, the vast majority of commercial telegrams were sent via shortwave. Shortwave transmissions cost five per cent of the price of longwave transmissions, needed only two per cent of the electrical energy, and could be multiplexed to carry three times as much information. Radiotelephony, the two-way transmission of the voice by radio, became an expensive but practical service. Cable networks, by contrast, did not achieve the bandwidth required to transmit voice information until coaxial submarine cables replaced Victorian-era multicore cables after 1945.

[357] 'POST 33/2905D'.

[358] Ibid., 29.

It was apparent by the second half of the decade that the commercial undersea cable companies faced bankruptcy. They were too slow, too expensive, and unable to do anything to lower costs to match the prices offered by shortwave systems. The potential bankruptcy of commercial cable networks was perceived as a threat to Britain's imperial security. The mathematicians of GC&CS had demonstrated by then that eventually, any encryption code could be broken. Transmitting coded signals on wireless would supply foreign government codebreakers with an ever-growing supply of material to work with. Regularly using codes on wireless exposed them to the world, and this inexorably eroded their reliability. Therefore, it was decided that all confidential and secret governmental communications were only to go via cable, which meant in turn that maintaining the cable infrastructure was critical to imperial power.

The solution was to ensure that government could prop up the cable network, even if it meant operating the network at a loss. In 1927, the Sub-Committee on Competition between 'Beam' Wireless and Cable Services, part of the Committee on Imperial Defence, decided to create a 'merger company' that would immediately acquire all of Eastern Telegraph and Marconi's shares, and a 'communications company' that would acquire all British communications assets. The two companies would have the same directors, of whom the British government would appoint two. No more than twenty-five per cent of shares would ever be owned by foreign interests, and an Imperial Communications Advisory Committee would supervise the whole operation. In 1929, the government founded Cable and Wireless.[359]

Cable and Wireless cable stations across the world were equipped with shortwave radio receivers, mobile detector vans, long-range transmitters, radio direction finders, and dummy cables for would-be attackers to target. Operators were trained to report back anything of intelligence value that they came across in their postings, even when off duty in the local towns and cities. The new wireless telegraphy services incorporated the interface devices used in telegraphy: Teletype machines and

[359] Headrick, *The Invisible Weapon*, 203–6.

undulators were transferred directly from the Central Telegraph Office at St Martin's Le Grand to the new 'Empiradio' receiving stations, with the same paper 'slip' being used to print off messages and glue them to telegram forms. As with cable networks, wireless messages were duplicated and retained.[360] During the Second World War, Cable and Wireless was heavily interpolated with British intelligence agents from MI6 and the British Communications Service. 'C&W' brought the entire telecommunication network of the British Empire together in a single cybernetic feedback loop that has persisted beyond the life of the company itself.[361] The company was an extension of the intelligence apparatus of the Empire.[362]

3.4.4 SIGINT, ELINT, COMINT

Semantically meaningful messages between humans were only one effect of the information that can be ascribed to intercepted wireless media. Radio Direction Finding (D/F) opened up an entirely new set of possibilities. Like syntonic tuning, direction-finding emerged as a side-effect of the attempt to build secrecy into radio transmissions. In 1905, the Post Office began conducting experiments with the Bellini-Tosi 'directive wireless' device. It was designed for directing radio waves in a narrow beam in a single direction, rather than in as radial emanations. By 1912, the device had been shown conclusively not to work for that purpose. Longwave radio transmitters of the time inevitably scattered their signals in all directions.

[360] 'Empiradio Beam Services: Method of Recording Received Signals POST 33/2227' 1930, BT Archives.

[361] Souden, *Voices Over the Horizon*, 132–54.

[362] In 2013, a PhD candidate at the University of Exeter was awarded his doctorate based on research at the Cable and Wireless archive in Porthcurno, Cornwall. During the course of his research he discovered entries in the archive stamped with 'Top Secret'. He contacted the Ministry of Defence and was subsequently informed that many of the entries had to be removed from the archive. He himself was invited to participate in the process of redacting and excising the archive. See Benjamin David Oldcorn, 'On the Wire: The Strategic and Tactical Role of Cable and Wireless during the Second World War', 26 September 2013, 61–70, https://ore.exeter.ac.uk/repository/handle/10871/14642; I discovered this after emailing the Porthcurno archivist requesting a copy of this unusual entry that appeared in the National Archives search engine. It is unavailable, being one of the items removed by the government in the course of Benjamin Oldcorn's research. 'Ministry of Economic Warfare' 1942, Cable and Wireless archive (redacted), http://discovery.nationalarchives.gov.uk/details/r/edf70107-39c9-4ba2-b750-68c7e2bb3b6f.

However, in 1914 a modified version of the Bellini-Tosi device was successfully deployed for a different function. Rather than altering transmitters, an inverted Bellini-Tosi device coupled to a receiver could successfully perform the inverse function: it pinpointed, to within a couple of degrees, the vector of an incoming radio transmission. This meant it could indicate the direction of a distant transmitter. Direction-finding apparatus was rapidly deployed at sea, enabling navigators to precisely fix their location relative to fixed D/F transmitters located at ports, lighthouses and along shorelines. Through basic triangulation, ships had constant access to their geographical location, even in heavy fog. Ever since, naval navigation has been based on artificially generated geographical referents. Radio waves became a medium for geometrically remapping the world and finding one's place in it.

Meanwhile, direction finders on land went to work "detecting irregular wireless installations".[363] As early as 1903, there were concerns about the use of private radio transmitters by foreign spies.[364] When war began, the Defence Of the Realm Act 1914 made it illegal to possess any wireless apparatus without express permission of the Postmaster General.[365] Police confiscated or sealed up 2,500 licensed sets and 750 unlicensed sets, using Bellini-Tosi detectors mounted on vans to locate transmitters.[366] But they missed some, and in the end it was amateur enthusiasts who had managed to keep hold of their sets that first alerted the authorities to the prevalence of openly available German naval traffic, enthusiastically passing on streams of coded messages they received.[367] Navies in the First World War used sophisticated and specialised codebooks to transmit in Morse.[368] The British began the war with only one official

[363] 'Marconi-Bellini-Tosi Apparatus for Directive Wireless Telegraphy POST 30/3139' 1914, BT Archives; 'Reports on Directed Wireless Telegraphy Systems Including the Belini-Tosi System TCB 274/10' 1915, BT Archives.

[364] 'Minutes of 23rd Meeting. (Home Defence; Possibility of Invasion; Use by Private Persons of Wireless Telegraph Stations in War-Time; Importance of Joint Naval and Military Manoeuvres.) CAB 38/3/72' 1903, National Archives.

[365] 'Suppression of Experimental and Private Business Wireless Stations during the First World War, Part 1 POST 30/3501' 1914, BT Archives.

[366] Headrick, *The Invisible Weapon*, 145.

[367] Ibid., 158.

[368] For a comprehensive account of the code systems used in the First World War, see Kahn, *Codebreakers*, 266–350.

interception station at Stockton. By the end of 1914, they had embarked on building a chain of 'B' stations along the coast from Shetland to Kent, in Ireland and Gibraltar, and were sending rudimentary mobile stations to the front-line trenches. The purpose of each station was not only to intercept communicative messages but also to triangulate using D/F techniques the shifting locations of enemy forces. Individual German ships were pinpointed as soon as they broke radio silence, and sometimes identified by the characteristic 'fist', the minute elements of style that, like handwriting, was bound to a particular operator.[369] The materiality of transmission and reception took on strategic dimensions far beyond the value of the information they transmitted.

Governments have remained on permanent 'listening watch' ever since. COMINT (communications intelligence) and ELINT (electronic intelligence) have been abbreviations for two distinct subsets of intelligence, grouped together under the abbreviation SIGINT. 'Signals intelligence' was driven by radio, and includes all dimensions of wireless media.[370] ELINT was differentiated from COMINT when, for the first time, intelligence could be gleaned not only by interpreting a target's use of communicative signs, but by measuring their position, movements, numbers, and other technical capabilities, and to seek to undermine their systems by remote technical countermeasures.[371] In the case of traffic analysis, COMINT and ELINT are sometimes difficult to separate, because although the task is to log everything about a transmission except the content of the message, this is often more informative about the target's intentions than the content. The addresses that commands originated from were more revealing than the data they contained.[372] Indeed, it was only through the application of algebraic geometry to D/F based traffic analysis that produced cribs for GC&CS codebreakers at Bletchley Park to break into the meaning of the messages encrypted by the Enigma machine.[373] The essential point is that new techniques for

[369] Ibid., 270.

[370] Herman, *Intelligence Power in Peace and War*, 69 Comint is the interception of communications, Elint is information gleaned from non-communicative transmissions.

[371] Ibid., 83–84.

[372] Kittler, *Gramophone, Film, Typewriter*, 256.

[373] Hodges, *Alan Turing*, 161.

using wireless media generated a new order of knowledge about the surface of the earth, and about the enemy. The data generated by targets was as revealing, if not more so, than the content of whatever messages they intended to relay.

Hence command and control radio signals that had no communicative content were productively intercepted. German night-bombing during the Second World War, for instance, was conducted by beam radio navigation, enabling relative accuracy without any visual cues. The *Knickebein-Verfahren* system employed one narrow shortwave beam to guide pilots to their target, where an intersecting narrow beam triggered the release of bombs.[374] During the course of the war, radio-based measures rapidly evolved. Both the 'passive' reception and directional pinpointing of radio emissions from enemy aircraft, submarines, and ground stations, as well as the 'active' use of radar to sweep the horizon with radio waves, in the air and on the ground, became increasingly important, as did jamming and other countermeasures.[375] Wireless media turned the electromagnetic domain into its own scene of strategic and tactical escalations. Transmissions no longer had to carry meaning to be informative. Individual messages revealed tactical commands, but techniques of 'traffic analysis' revealed entire networks of strategic operations.

In the twentieth century, the history of COMINT became the history of technical cryptography. Until the 1930s, cryptography was still based on addition and substitution, as it had been in ancient civilisations. When "a radio message to one was a message to all", better methods were required.[376] With ELINT, intelligence took a technoscientific turn. The mobilisation of electronic systems to detect, guide, map, disrupt, or otherwise seek strategic advantage introduced a dimension of scientific measurement and technical escalations into the *dispositif* of state security. Although the British Empire created Cable and Wireless to keep their most secret messages off the air, wireless transmissions were nonetheless essential for general governmental

[374] Alfred Price, *Instruments of Darkness: The History of Electronic Warfare 1939-1945*, Revised (Barnsley: Frontline Books, 2017), 24–26.

[375] See, generally, Price, *Instruments of Darkness*; Headrick, *The Invisible Weapon*, 248–50.

[376] Hodges, *Alan Turing*, 162.

and military purposes. At that point, the site of struggles over the strategic escalation of media technology and intercepted communication turned decisively towards cryptography.

3.5 Digital media

Between the 1920s and 1940s, developments in electromechanical transmission interfaces that converted alphabetic text into numerical code values led to the invention of automatic electromechanical cryptographic machines. Within a few years, Alan Turing's work at Bletchley Park had defeated the machines and inaugurated artificial intelligence. At that point, the critical element in interception became neither access to material in transmission or storage forms, but how it was processed. Until mechanical encryption machines, all processing of intercepted material had been performed by humans. Humans took instructions, made selections, made copies, and subjected cryptography to cryptanalysis in order to read coded messages. By the end of the Second World War, this changed utterly.

3.5.1 Mechanical coders

For around the first seventy years of telegraphy, practically every telegraphic messaging system required an element of human processing. In order to send and relay messages, someone had to be 'in the cage', or perhaps operating a relay station on a remote island in the middle of the ocean.[377] Mechanical instruments enabled this processing in different ways. The original Wheatstone and Cooke devices had 'needle' interfaces that had to be read visually. Some were relatively complex, with rotating indicators calibrated to move over a printed configuration of the entire alphabet of letters, plus a few key words, whereas others simply oscillated between a limited set of printed words relevant to railroad functions. Devices for marking strips of paper with incoming sequences of inked dots and dashes were in use before telegraphy became commercially popular, as were machines for punching out patterns on perforated ticker tape. But it transpired that telegraph operators were able to recognise the symbols coming through the apparatus without looking at the paper, instead they

[377] Cable and Wireless stationed men on Ascension Island and Direction Island, an uninhabited part of the Cocos, see Souden, *Voices Over the Horizon*, 113–30.

simply listened to the steady rhythm of the mechanical printing armature as it was magnetised and de-magnetised by the incoming signal.

Morse code is remarkably well adapted to human sensorial processing. The Morse alphabet is composed of different combinations of its basic elements, ‘dots’ and ‘dashes’, with translations selected so that the most frequently-used letters (in English, at least) are the simplest elements to ‘key’ into Morse patterns. Because an electrical circuit has only two states, on or off, the basic elements of any code language in an electrical telegraph system must be signified using these system states. Human aural cognition benefits from durational coding of elements. The brain can clearly distinguish a shorter ‘dot’ from a longer ‘dash’. In the early printer-based systems, a clicking sound occurred when the circuit was closed, bringing the printing arm down on the paper, and again when it was opened and the arm sprang back up. The ‘slip’ paper moved at a steady pace under the armature. The difference between a dot and dash could be aurally determined by the time between each click. Two clicks with a short gap between them marked a dot on the page, two clicks with a longer gap marked a dash. Every other gap was a space between characters. When telegraphers realised they could decode incoming messages without looking at the ‘slip’ but simply by listening to the rhythm of the armature, electric buzzers were installed to make the task easier. Because Morse is binary, the possible variations in information are limited to two elements. In each fleeting silence, the brain need only expect one of two options to follow, a dot or dash. With training, one can process a message into written words, transcribing sentences faster than the conscious mind can reflect on their meaning.

As long as human operators were needed, human senses and the brain’s ability to process information remained limiting factors on processing times. In large telegraphic hubs where multiple messages arrived simultaneously, machines were used to receive transmissions. Undulators reproduced telegraph signals as oscillating waveforms on paper, ticker-tape perforators spat out lines of binary coded slip paper, and ink printers marked out coded sequences on paper. But humans were still required to read the output and convert it into textual alphabetic language. Furthermore, even with rudimentary printers, senders and receivers had to be actively synchronised in order to ensure that the start of a message was recognised as the start and the end recognised as the end. A separate circuit with a bell attached to signal the start of a message, for instance, was one useful synchronising device that alerted a human telegrapher to get the receiving apparatus ready for a new message. Otherwise, incoming messages would run into one another irretrievably. In short, error-free data transfer required some human means of temporal coordination, a governing reference point to maintain synchronicity.

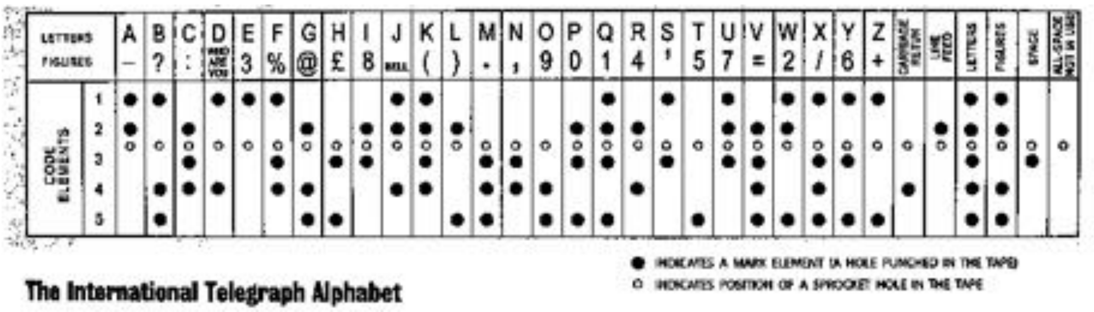
However, once typography and telegraphy had converted text into discrete and finite symbolic elements, machine processing became possible. During the 1920s, the need to synchronise human attention to the schedule of incoming messages changed with the development of the first Teletype machines. The crucial innovation involved solving the synchronisation problem. To this end, Teletype incorporated stop/start signalling, so that each discrete character was preceded by a START signal and followed by a STOP signal. START activated the receiving mechanism, and STOP halted it. STOP was essentially an inbuilt delay of a few carefully calibrated milliseconds, which stopped the entire printing mechanism long enough to ensure that the receiver had completed printing the previous character and stopped moving before allowing the next START signal to proceed. This meant that even if a sender typed in a message faster than the receiving printer could print it, it could not cause errors by jumbling the control signals. The STOP delay ensures each discrete movement of the printer mechanism is completed before the next can be activated.

Whereas Morse used a two-bit code comprised of dots and dashes, an alternative system based on a five-key piano keyboard had been devised in 1870 by French telegraphic inventor Émile Baudot.[378] By keying different combinations of the five elements, an operator indicated a letter or symbol. The International Telegraph Alphabet (No.2) code (ITA2) adapted this system for electromechanical Teletype systems. For instance, A = ZZAAA, B = ZAAZZ, C = AZZZA, and so on, where A and

[378] Gleick, *The Information*, 202.

Z represent switching between two electrical states.[379] Each key also instructs the receiver to start, transform the next five switching operations into a key-value, print the character corresponding to the key-value, then stop printing. A letter is thus printed directly onto a page. Typewriters could be remotely twinned over cable connections, and global text messaging was invented.

Teletype machines accelerated everything, and rapidly. In 1920, Morton and Krumm's first machine ran at 40 characters per minute. By 1931, the Creed Model 7 ran at 400 characters per minute; it was selected for use in the Post Office's new Inland Telex service. Telex integrated telegraph circuits to the telephone exchange. From then on, Telex subscribers no longer needed to physically interact with the Post Office at all. They simply paid a subscription fee, installed the line and equipment, and were from then on able to send typed text to any other machine on the Telex network. Now the signals flowing through most commercial channels, by wire or wireless, were entirely insensible to human cognition and could only be converted into alphanumeric text by machines compatible with the ITA2 protocol. Teletype and Telex took human processing out of the telegraphic transmission process altogether. Telegraphy became a field for electrical engineers and statistical mathematicians, defining and refining coding languages for closed systems of data exchange.



LETTERS		A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	CARRIAGE RETURN	LINE FEED	LETTERS	FIGURES	SPACE	ALL-SPACE NOT IN USE
FIGURES		–	?	:	WHO ARE YOU	3	%	@	£	8	BELL	(	)	.	,	9	0	1	4	'	5	7	=	2	/	6	+						
CODE ELEMENTS	1	●	●		●	●	●				●	●						●		●		●		●	●	●	●			●	●		
	2	●		●				●		●	●	●	●				●	●	●			●	●	●					●	●	●		
		○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
	3			●			●		●	●		●		●	●		●	●		●		●	●		●	●				●		●	
	4		●	●	●		●	●			●	●		●	●	●			●				●		●			●		●	●		
	5		●					●	●				●	●		●	●	●			●		●	●	●	●	●			●	●		

● INDICATES A MARK ELEMENT (A HOLE PUNCHED IN THE TAPE)
○ INDICATES POSITION OF A SPROCKET HOLE IN THE TAPE

The International Telegraph Alphabet

The International Telegraph Alphabet 2. Pic: Ali Lokhandwala, CC licence

[379] The system states can be 'on' or 'off' as in Morse code, but by the time Teletype was invented, alternators were widely available that maintained a steady voltage while switching the polarity of the current, each reversal signifying a difference in states. Strictly speaking, it is not the two states themselves that are significant, but the difference between them. See R. N. Renton, *Telegraphy* (London: Pitman Publishing, 1976), 1–10.

Automatic telegraphy meant that no special skills were required to operate radio interception stations, according to a letter to the Post Office from the Foreign Office.[380] In 1939, new Wireless Interception Stations were installed at Brora, Cupar, and St Albans in anticipation of war. The Post Office supplied telegraphers to operate the stations. Telegraphic messages arrived via wireless receivers, and "on tap" from cable circuits extended from the telegraph network. The apparatus included old-fashioned undulators and contemporary teleprinters, and the

> degree of skill called for, and the measure of responsibility involved, [were] considered to be no greater than apply in the case of Cable Rooms de rigueur.

Seven officers were required for each station, working in shifts on handling incoming transmissions. A further five officers would carry out "scrutiny work",

> …[Which] consists of scanning 'dead' telegrams and extracting certain of these in accordance with a prescribed list. A retentive memory is necessary to the performance of this duty which, owing to the large number of forms falling to be examined, has to be discharged at a fair speed. This work must, after some time, tend to become monotonous in character but it is of a purely routine nature and is not considered to call for any exceptional knowledge or skill… any telegrams sent to or by Foreign Governments… are easily distinguishable from other traffic by prefix and/or address. Accumulations of slip are examined very speedily as soon as opportunities offer, a very great percentage of the slip being of course discarded.[381]

The wages were identical to those paid to ordinary commercial cable room staff in the GPO, because the techniques used were identical. In fact, one memo on file states, there would be less pressure to work quickly than in a commercial setting, and therefore the job was in one sense less onerous than the ordinary work of a telegrapher. On the other hand, there would be some new technical difficulties in tuning in, monitoring, and relaying wireless signals back to 'Room 59' (a codename for Government Code & Cypher School, which by then had relocated to Bletchley

[380] 'Code and Cypher School - Erection of Wireless Interception Stations and Staffing FO 366/1059' 1939, National Archives.

[381] Ibid.

Park). Aural processing of signals using headphones would be required where the intercepted radio signal was too weak for the apparatus to differentiate, with such signals noted by hand and forwarded to Room 59 by teleprinter.[382] The automation of transmission systems put the interception officers in much the same role that cable censors had performed in the First World War, and would perform again in the Post Office during the second. They were to sort through all messages received on selected wavelengths, process the undulated or hole-punched 'slip' paper, identify the prefixes and addresses of the messages encoded in the signals, and compare those reconstituted messages against the listed selection criteria. If they found a particular format or addressee in a message, then they passed it on for cryptanalysis at Bletchley Park.

3.5.2 Cryptological machines

Automatic telegraphy produced automatic cryptography. As soon as typewriters gained the capacity to copy their output to distant printers, in addition to printing onto paper they simultaneously transmitted electrical patterns, signal elements of pre-programed Teletype code. Hole-punched paper tape was soon added to Teletype machines in order to store patterned messages for automatic transmission. When fed into the receiver of an automatic teletypewriter, the patterns were read as a sequence of linear binary operations and transmitted automatically. In December 1917, when Teletype was still an experimental technology, an AT&T engineer named Gilbert Vernon realised that the patterned signal generated when typing a message into an automatic Teletype machine could be synchronised and added to a second signal, generated by another punched tape machine, this one containing random key characters. With each stroke of the keyboard, the assemblage would pull through and automatically add on a randomised key value. The output of the two characters combined could be transmitted as an encrypted signal, appearing completely random to anyone intercepting the transmission. Provided that an exact copy of the random string of text, i.e. the key, was correctly synchronised with the receiving teleprinter machine, then the random masking values would be automatically subtracted from

[382] Letter from F Riley to Personnel Department, 14 June 1939, 'Interception Service FO 366/2381' 1938, National Archives.

each incoming symbol so that a perfect copy of the original plaintext would be printed.[383] This way, cryptography could be completely automated. Perfect secrecy was made available to parties who, for the first time, needed to have no knowledge whatsoever as to how the message was encrypted.

The Telekryption machine that AT&T manufactured is, effectively, an electromechanical instantiation of a 'one-time system', the only theoretically unbreakable method of cryptography.[384] The limiting factor is the production, distribution, and synchronisation of keys, which must be genuinely random and unique in order to be secure from cryptanalysis. Any duplication of a particular key would create repeated patterns, however obscure, and thus weaken the encryption of a message. Identical random key pairs cannot be mass-produced if they are to be truly random, and each key pair must be used only one time. Therefore, any agency utilising such a secrecy system must plan for and produce an equivalent number of random key pairs to the total number of encrypted transmissions they will need to make, and must distribute matching keys in advance to either end of each communication. In a complex network, in which communication cannot be perfectly predicted in advance, this is impossible. But one-time systems work well when applied individually to fixed two-way channels, such as corresponding with a spy, linking up military headquarters to a particularly important bunker, or contacting two fixed diplomatic posts.[385]

Based on a different approach, electromechanical code-wheel systems independently arrived during the 1920s. The most successful models were Hebern's Electric Code

[383] Kahn, *Codebreakers*, 394–96.

[384] 'One-Time' systems are any systems that use random, non-repeating keys. They can be manufactured on paper, almost like a booklet of bingo numbers. Ibid., 403.

[385] Ibid., 400–401; In 1942, the Soviet Union duplicated one-time pads in order to conserve resources during the war. By 1944 this was discovered by American cryptanalysts. The Soviets were tipped off in 1948 and changed their systems, but the 3,000 or so telegrams gathered in that time were analysed and decrypted slowly over the next 40 years. This project, codenamed Venona, uncovered a large number of spies including the Cambridge Five and the atomic spy, Klaus Fuchs. Aldrich, *GCHQ*, 72–78; see also Andrew, *The Defence of the Realm*, 365–68; see also West, *British Security Coordination*, 455–60.

Machine in the US, the Swedish Hagelin M-209, and most famously, Arthur Scherbius and his German *Geheimschrijfmachine*, or Enigma machine.[386] In each of these devices a series of combinatory rotors performed complex transformations that turned plain text into cipher text and back. The 'key' was the particular starting position of the rotor wheels, which was changed each day. Provided each setting was a randomly different from the previous setting, it was humanly impossible to solve the system before it changed again. As the rotors moved independently of one another, each individual letter input to the machine underwent a unique set of transformations. With Enigma, every cipher letter was the output of one of eight billion possible transformations. It was like a typewriter without an "unequivocal link between input and output… For the first time, hitting a letter key offered numerous combinatory surprises."[387] The British initially believed Enigma messages were unsolvable; and the Germans continued to believe it until after the war.

However, Polish mathematicians had devised mechanisms capable of simulating the Enigma machine's transformations, which they supplied to British intelligence. Because every Enigma setting produced a linear set of transformations – that is, each letter of cipher text corresponded to a single letter of plain text for each setting – it was mechanically possible to reverse the transitions, provided one had a good idea of what the original plain text words said. In other words, because Enigma was a machine, its mechanical transformation operations could be inverted. Doing so was structurally the same as designing any other discrete mathematical algorithm, the problem was performing the necessary steps sufficiently quickly to eliminate the incorrect combinations before the code settings changed again the next day. Alan Turing, who joined GC&CS on 4th September 1939, had a blueprint for a solution. The Enigma machine was defeated by simulators called Bombes, which electronically cycled through all possible encryption settings that could match intercepted code phrases to possible plain-text words. Once the machine found a pattern that matched coded letters to the assumed plain words, it stopped 'working', and its final configuration was the solution.

[386] Kahn, *Codebreakers*, 415–34.

[387] Kittler, *Gramophone, Film, Typewriter*, 251.

The Siemens Cryptwriter machine was more complex than Enigma, used only for sending and receiving top-secret signals from German high command. It worked on similar principles as the Telekryption machine described above.[388] It was eventually defeated by the first programmable computer: fifteen hundred vacuum tubes arranged to operate as a matrix of two-state binary switches, named Colossus, capable of processing patterns much more quickly. Crucially, the Mark II version had the capacity to automatically switch programs on the basis of its own previous calculations, making 'conditional jumps' that determined the best way for the machine to arrive at a solution. Previously, the cryptanalysts' job had been to enter possible encryption patterns for analysis, but Colossus could make those selections for itself better than the mathematicians. The programmable machine could sort, and discriminate between, different possible programs. Designed first as a theoretical flowchart in 1936,[389] the Universal Turing Machine, or 'universal discrete machine', had been operationalised.

A machine capable of seeking solutions for itself undid thirty years of technological progress in the pursuit of mechanical secrecy systems. As Kittler provocatively suggests, all that then remained for human spies was to create myths and legends to disguise the invention of the computer, and all of its radical processing advantages. During the war, a concerted disinformation campaign gave both Allied battlefield commanders and German generals alike the false impression that human ingenuity, not machines, had won the war, and this myth-making carried on until the truth about Turing and Colossus was eventually published during the 1970s and 80s.[390]

3.5.3 Harvesting data

After the war, technology and capital shifted across the Atlantic. Coaxial cables replaced the undersea network of copper-core cables, increasing the volume of data that could be transmitted following the introduction of automatic transmission

[388] Hodges, *Alan Turing*, 265–68.

[389] Turing, 'On Computable Numbers, with an Application to the *Entscheidungsproblem*'.

[390] Kittler, *Gramophone, Film, Typewriter*, 261.

systems. By the mid-1960s, worldwide US armed forces alone were connected via the Defence Communications System, transmitting over a quarter of a million messages a day on over ten million miles of coaxial cables, with over two hundred relay stations connecting more than 1,500 tributary stations, employing over 30,000 men.[391] As with the British empire, the US recognised that cables were inherently more secure than radio transmissions, and that their security depended upon hegemonic influence on the commercial companies building and operating the networks.[392] Daniel Kahn, historian of cryptography, recounts that Strategic Air Command alone operated six networks, combining radio networks and hard-wired cables, partly leased from commercial operators, transmitting messages to nuclear-armed aircraft on constant alert.[393] Integrating the military and intelligence services of allied nations was even more complicated. In order to produce a coherent and coordinated global military force, a global network for communications was essential. The speed of communications accelerated: supersonic aircraft and submarine ballistic missiles on permanent standby required a commensurate capacity to reliably send messages on the both sides.

In the latter half of the twentieth century, the critical issue was not so much intercepting transmissions or devising storage media as being able to effectively process what was intercepted. The NSA was formed in 1949 as the United States' international signals intelligence agency. From the beginning, it was tasked with intercepting communications and cryptanalysis. The agency rapidly grew in parallel to the computer industry. Between 1963 and 1973, for instance, the NSA grew its computing power by fifty per-cent and lowered its computing costs by twenty-five per cent, per annum.[394] As an early explanatory paper in the NSA Technical Journal explained, a 'computer', a name formerly applied to people working arithmetically with pencil and paper, is fundamentally an electronic arithmetical machine. Any sequence of discrete operations in any order can be computationally performed.

[391] Kahn, *The Codebreakers*, 672.

[392] Starosielski, *The Undersea Network*, 39.

[393] Kahn, *The Codebreakers*, 673.

[394] 'Report of the Second Computer Study Group', *NSA Technical Journal* 19, no. 1 (1974): 21–63.

Whereas a special-purpose machine had fixed functions and a single mode of logical organisation, digital computers can be programed to perform any set of sequential operations.[395] Transmission and storage techniques evolved, while processing techniques began to depend less on solving codes than on programming computers to find solutions.

At the first meeting of the NSA's Crypto-Mathematics Institute in 1958, Howard Engstrom, deputy Director of the NSA and one of the buildings of the UNIVAC computer, explained that the cryptologist working on intercepted material

> no longer had a piece of paper delivered to him which contained some meaning, but had to plumb the depths of the atmosphere to extract his raw material… extracting information from the atmosphere around us by the use of all possible scientific means available.[396]

Machine encryption, coupled with a vast increase in the number of radio signals available, made intelligence-gathering tasks progressively more complex to detect, filter, store, and process, all within an effective period of time. Selecting signals to collect and analyse became more complex because radio communication signals and command signals were hard to differentiate and both were encrypted, the latter being those addressed to machine operations rather than carrying informative intelligence. Throughout the 1950s, the largest part of interception 'front end' work was the manual task of translating Morse signals into alphanumeric characters for analysis. All intercept material was couriered back to Washington, often taking weeks to arrive, while interception stations around the world sent back overview summaries electrically.

In 1957, the NSA created a Special Intercept Typewriter (SPIT), a modified Remington-Rand Synchro-tape typewriter with special keys added for 'tagging' data, for instance, indicating call-signs or radio frequencies. The next generation of modified typewriter

[395] An early NSA explanatory paper gives an insight into how hard it was to work with early computing hardware, see J.A. Meyer, 'Computers: The Wailing Wall', *NSA Technical Journal* 1, no. 3 (1956): 69–90.

[396] Edward T. Engstrom, 'Science and Cryptology', *NSA Technical Journal* 3, no. 3 (July 1958): 2–3 (Declassified 2008).

included more tags referring to traffic data, like start-of-message and end-of-message, but more importantly added a perforated paper tape output. Tape could then be transmitted electrically into a remote processing computer.[397] From that point on, all NSA operations, and the US SIGINT system generally, was driven by computer and network requirements.[398]

Superior computing power became the essential element of NSA strategic planning. The first large-scale stored-program computer, the UNIVAC 1101, was built with secret assistance from NSA scientists. In the 1950s, a secret NSA project, LIGHTNING, funded the development of computer technology by corporations and academic researchers, including Norbert Wiener and John von Neumann.[399] As a report on LIGHTNING from 1959 put it,

> So long as it is possible to have computing facilities in excess of what others may consider feasible, it behoves us to have them. Eventually we foresee that natural limitations on speed and size will be encountered, and then the inevitable advances of our opponents will corner us, so that the duel will become one of pure wits. But while we can we must maintain our superior weapons.[400]

In 1959, the first digital 'word spotter' was developed, as described in an article in the NSA Technical Journal.[401] The prototype could process 50,000 Teletype words per minute, up to a maximum 12-character word-length. Input was from different sources of serial Teletype data, initially limited to magnetic tape or paper punch-cards, with a perforated tape reader later added to the system.

[397] Thomas R. Johnson, ***American Cryptology During the Cold War, 1945-1989, Book II: Centralization Wins, 1960-1972***, Excised & Declassified 2013 (National Security Agency: Center for Cryptological History, 1998), 361–62, https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/cold_war_iii.pdf.

[398] Ibid., 364.

[399] Engstrom, 'Science and Cryptology'.

[400] Howard H. Campaigne, 'Lightning', ***NSA Technical Journal*** 4, no. 3 (July 1959): 63–67 (Declassified 2012).

[401] Miles A. Merkel, 'A "Word Spotter"', ***NSA Technical Journal*** 4, no. 4 (1959): 91–100 (Declassified 2011).

In 1962, the NSA installed Harvest, which was then "the most sophisticated computer ever built… certainly the most advanced in the crypt community".[402] The conceptually unique system was originally proposed to the US government by IBM in 1955. Two were built, one for the NSA and one for the Atomic Energy Commission. The NSA's version included logical input processing units specially designed for NSA operations. A magnetic tape handling system called Tractor selected from 160 stored cartridges, transferring data at 1,128,000 characters per second. The other is still classified It was the fastest processing machine in the world for at least a decade, still running ten years later in 1972, having progressively increased its capacity through developments in programming. Harvest ran its own code language, Alpha, designed to operate on "large masses" of data.[403] The NSA continued to ensure it remained ahead of commercially available computing systems.[404]

The NSA had the world's largest collection of computers by the mid-1960s, in the United States and at field sites around the world. The average field officer "become a communications tape handler rather than a SIGINT analyst".[405] The aim was to differentiate computer processing from conceptual programming skill, so that computers could be made "conveniently accessible to users, who don't really know much about what goes on down in the basement".[406] Ideally, they would interact only with a specially-designed 'user environment' interface. This meant decoupling human operatives from the need to understand or direct computation processes so that what the computer actually does and what the user can interact with are separate things. At around the same time, as Krajewski and Vismann note, Xerox was doing the same thing with the first commercial desktop computers:

[402] Joseph Eachus et al., 'Growing Up with Computers at NSA', ***NSA Technical Journal***, no. Special Issue (1972): 12 (Declassified 2012).

[403] Ibid., 12–13.

[404] Bamford, ***Puzzle Palace***, 137–39.

[405] Johnson, ***American Cryptology III 1972-1980***, 1998, 169.

[406] Eachus et al., 'Growing Up with Computers at NSA', 13.

> Personifying the computer led to an incisive division between people and lawgivers, or, in computer terms, between *users* and *programmers*.[407]

Cryptanalysts were turned into users because the machines they were to use were too complex, too expensive, and had to service too many users to allow anyone to simply interact with them at the level of programming. Networking, in turn, required regulations in order to implement shared access to processing time. At this point, unnoticed to most, computers began to take on the properties of the law, assigning subjects what data they were permitted to access. The machine had taken over the sovereign position of the sorter of data.[408]

By the mid-1960s, NSA radio interception stations were equipped with automated collection systems, eliminating the need for radio officers to type out the signals they received. On-site computers filtered transmissions for keywords across a variety of signal types, triggering processing and forwarding routines automatically upon the recognition of high-interest text.[409] As a senior cryptanalyst put it in 1972,

> We find ourselves today in the position of beginning to be a factory… I think one of the biggest developments was when the target countries began to use Teletype equipment and began to send their data electrically… which led to our being able to forward this data electrically. We are currently handling by electric circuits some [REDACTED] per day which come directly into the building and are handled automatically.[410]

Whereas in the early days of computer cryptanalysis, all intercepted data had to be transferred onto machine-readable punch cards before it could be processed, the growth in Teletype data links around the world meant that signal-receiving hardware could directly interface with analytic computers. At that point, the targets did the input work for the interceptors. All sorting operations were performed internally in the NSA network. Interface equipment located in radio receiving stations and cable-

[407] Vismann and Krajewski, 'Computer Juridisms', 95.

[408] Ibid.

[409] Johnson, *American Cryptology III 1972-1980*, 1998, 373.

[410] Eachus et al., 'Growing Up with Computers at NSA', 14.

tapping sites applied algorithmic selection criteria to the signals passing through, selecting some for forwarding to the mainframe analysis machines in Maryland, deleting the rest. Interception was effected via (relatively) smooth transfers from the target's Teletype interface into the NSA's computers, located "down in the basement" where not even the analyst 'users' could directly interact with them.

The same applied to intercept officers stationed around the world listening for signals. Every NSA intercept officer became a key punch operator, and every stroke of the typewriter keyboard:

> produces an electrically forwardable signal which is sent to NSA and processed by computers. The feedback goes via reverse route such that in effect we are no longer a nice working team; we're a factory.[411]

The factory's input and output circuits stretched around the globe, feeding data back for processing. The long-term plan was for all NSA systems to be electronically connected by 1980, with users granted access to different computational processors according to their position and role. Intelligence would circulate fluidly around the world, permanently exchanging inputs and outputs across interfaces tailored to the human users who carried out instructions from the US government:

> I like to think of it in terms of a person working on a particular cipher system. He arrives in the building at eight o'clock in the morning and goes to a remote terminal… and twenty-nine messages appear on the screen of this cathode-ray tube. He decides what he needs to do with each message to get plain text and then he goes home.[412]

3.5.4 Cable Analysis

As military radio encryption systems advanced, targeting diplomatic and commercial cable traffic became increasingly important to western intelligence services.[413] Soviet military and command signals were effectively unbreakable, thanks to machines like Telecipher, which transformed a single line of plain text into around two hundred

[411] Ibid.

[412] Ibid.

[413] Bamford, *Puzzle Palace*, 488–89.

random letters. The only limit on the complexity of the cipher was the standard size of IBM paper used to feed random keys into the computer. Each Soviet communications encryption key was 'one-time', and never repeated. The Soviets sent Telecipher signals in a constantly modulating stream of data, twenty-four hours a day. This made it impossible to identify individual messages within the signals and to differentiate meaningful signals from 'dummy' data. Traffic data was masked, offering no way to determine the start, end, duration, or format of intercepted radio signals.[414] Effectively, the Soviets had achieved communication secrecy.

Hence the movement of money, markets, and third-party diplomatic communication along cables provided by telex and International Licensed Carriers (ILCs) became ever-more important, particularly market transactions concerning commodities like iron, steel and gas.[415] Given the complexity of the communications environment, with a large number of possible cable and wireless transmission channels, the easiest way to gain access to communications was, as before, while they were 'at rest'. This mean obtaining data directly from commercial companies.[416] Both the NSA and GCHQ carried this out on a daily basis. By the time that cable vetting was exposed in 1967, GCHQ operated a similar or identical processing system based on NSA hardware.[417] By then, the London international data exchange was computer-controlled, based on a ferrite-core computer memory matrix capable of storing and processing around 2,000 telegraphic characters at once.[418] Any message stored in the exchange could be selected for inspection or editing. The system generated copies of all processed messages on magnetic tape and stored them for at least thirty days in case of queries, delays, or diagnostic reviews.[419] The requirements to enable mass automated

[414] Ibid., 498–99.

[415] Ibid., 489.

[416] Thomas R. Johnson, ***American Cryptology During the Cold War, 1945-1989, Book III: Retrenchment and Reform, 1972-1980***, Excised & Declassified 2007 (National Security Agency: Center for Cryptological History, 1998), 83, https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/cold_war_iii.pdf.

[417] Moran, ***Classified***, 143; Aldrich, ***GCHQ***, 350.

[418] Renton, ***Telegraphy***, 322.

[419] Ibid., 320–22.

processing of daily cable traffic meant it was also readily available for processing by intelligence agencies.[420]

The US cable collection program was called Operation Shamrock. Only a small number of NSA officers aware of it, and with the cable companies having no knowledge of what the messages were used for. Tapes were couriered to the NSA each day for processing.[421] The Agency processed around 150,000 selected cable messages a month, the rest having been destroyed in the 'burn bag'. In four hours, the Harvest computer could scan about seven million Teletype messages, searching for instances or combinations of around seven thousand keyword selectors.[422] It was closed down when agency lawyers decided it was probably a violation of the US Constitution.[423] Diplomatic traffic was automatically selected and forwarded for deciphering, all disregarded messages were put straight into the 'burn bag', while the computer was fed a constantly changing set of key word search terms used to analyse traffic for matches and patterns.

Under the UKUSA pact, Britain and the US shared cable intercepts. Each agency had access to the miles of tape procured by the other, processing them through their word-recognition computers. In addition to monitoring foreign state activity, the NSA used the data procured 'incidentally' through its cable analysis to populate the Minaret database, the name for the illegal US 'blacklist' of domestic political activists collaboratively compiled by the FBI, CIA, and NSA.[424]

Since the end of the Second World War, GCHQ has been in some ways an appendage of the NSA. The 'special relationship' transfers technology and money into the interception apparatus of the UK. This is not the result of a particular Anglo-American

[420] Bamford, *Puzzle Palace*, 312.

[421] Johnson, *American Cryptology III 1972-1980*, 1998, 83–84.

[422] Corera, *Intercept*, 98.

[423] Bamford, *Puzzle Palace*, 313.

[424] Ibid., 418.

shared 'culture', but because one legacy of Britain's Empire was control over critical junctions in world communication systems.[425]

3.5.5 Extra-terrestrial interception

As well as collecting cable messages from commercial companies, interception stations were geographically distributed around the world, located according to the channels they aimed at intercepting. Global commercial cable traffic was carried by both cables and radio waves. Cables were intercepted near shore landing sites, which were licensed by the Post Office,[426] while radio receiving stations were located according to where shortwave channels were known to 'bounce' down from the ionosphere.[427] At twelve radio sites in the UK, intercepted transmissions were automatically filtered and forwarded on to GCHQ headquarters in Cheltenham. At Cheltenham, the ILC Control Party used a large wall chart to coordinate all the receiving stations, so that if weather conditions meant that on occasion a station lost reception on an important route, such as Bucharest to Moscow, then extra coverage could be temporarily provided elsewhere.[428] At 8-9 Palmer Street, London, a GCHQ station collected all radio messages in encrypted Teletype format to and from foreign embassies; later, the interception station moved to the Empress State Building near Earl's Court. All embassy signals were sent to Cheltenham for analysis.[429]

The first commercial communication relay satellites were successfully launched between 10th July 1962 and 21st January 1964. They relayed multichannel telephony and colour television channels on dedicated radio frequencies over the Atlantic, linking the US to the UK and France.[430] By 1970, the second generation of INTELSAT

[425] The exchange was 'terrain for technology'. The 'UKUSA' alliance in 1945 included Canada, New Zealand, and Australia under the 'UK' element. See, Richard Aldrich, *GCHQ* (London: Harper Press, 2011), 7, 329–39.

[426] James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (New York: Doubleday, 2008), 216.

[427] 'Hawklaw Intercept "Y" Listening Station (Former), Hawklaw | Buildings at Risk Register', accessed 4 November 2016, http://www.buildingsatrisk.org.uk/details/907213.

[428] Bamford, *Puzzle Palace*, 490.

[429] Ibid., 501–2.

[430] Stephen C. Pascall and David J. Withers, *Commercial Satellite Communication* (Oxford: Focal Press, 1997), 7.

satellites was in place, providing global satellite telecommunications.[431] By 1983, there were around 30,000 satellite communication channels in operation carrying telephone, telegraph, data streams, and television.[432] As with shortwave in the 1920s, wireless transmission again outperformed the submarine cable network.

Signals transmitted to earth from communication satellites rarely land entirely within the jurisdiction of a single state. Instead they illuminate large areas of the surface of the globe. Hence the international consortia that operate satellite systems devised frequency plans that assigned different baseband transmission frequencies to every governmental or commercial client using their satellites.[433] The UK's first fixed point earth station for sending and receiving satellite transmissions was built by the GPO in the early 1960s at Goonhilly Downs in Cornwall.

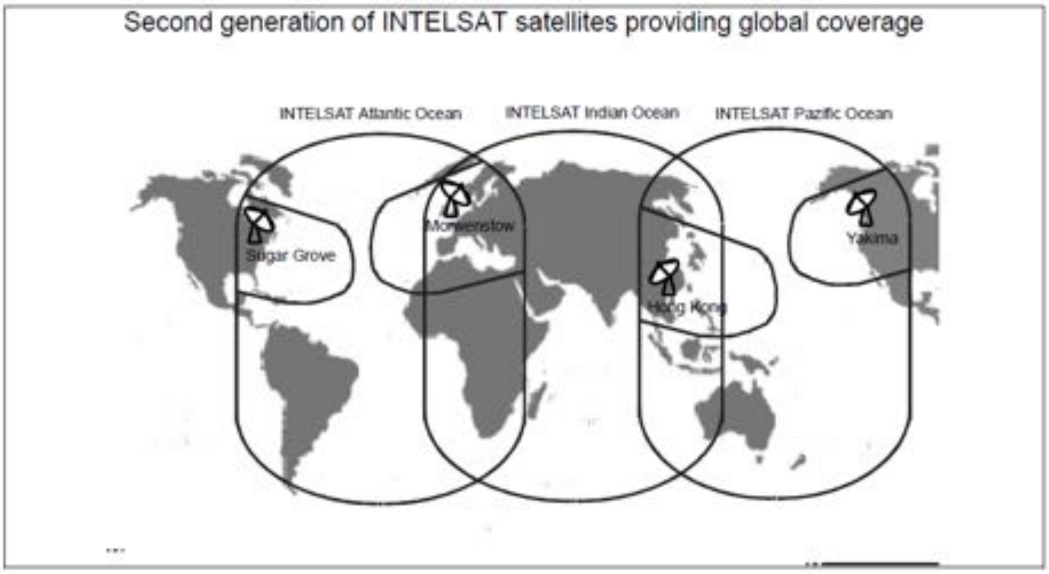
In 1967, GCHQ completed a duplicate receiver station, sixty miles along the coast at Morwenstow. There, GCHQ collected all traffic on all frequency bands transmitted by communication satellites in range. Satellite signals can be differentiated according to the operating protocols of the networks they serve: a baseband frequency differentiates a country, a local area code designates a city or region, and a particular telephone or Telex number, as it was, identifies an individual address. Similar 'shadow stations' were built in Cyprus and Hong Kong. The data received at each station was correlated, so NSA and GCHQ together covered both ends of any satellite communications, ensuring global coverage.[434]

[431] Bamford, *Puzzle Palace*, 420.

[432] Aldrich, *GCHQ*, 342.

[433] Pascall and Withers, *Commercial Satellite Communication*, 147–49.

[434] Fitzgerald and Leopold, *Stranger on the Line*, 94.



[435]

The flood of intercepted data that satellite interception produced exceeded all previous sources by several orders of magnitude. This presupposed the availability of digital filtering systems. The GCHQ word search program used for the purpose of sifting through satellite traffic was named Dictionary. It automatically combed the throughput of communications traffic for key phrases and words.[436] Once again, the selection and processing of intercepted information is a mirror image of the computerised systems that organise, multiplex, transmit and decode communication in their ordinary course of transmission.[437]

Unlike earlier transmission systems, satellite communications contained a mixture of 'internal' and 'external' communications. The totality of satellite transmissions sent and received on the UK's baseband frequency included communications with both 'ends' located within the UK, as well as communications that transit international

[435] This map is taken from the document: 'Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) - Temporary Committee on the ECHELON Interception System - A5-0264/2001', accessed 17 October 2016, http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=EN.

[436] Aldrich, *GCHQ*, 343.

[437] Bamford, *The Shadow Factory*, 217 the first two receiving dishes were named Pat and Louis, after the then-director of NSA and his deputy. GCHQ's director, Sir Leonard Hooper, wrote, 'Between us, we have ensured that the blankets and sheets are more tightly tucked around the bed in which our two sets of people lie and, like you, I like it that way.'

boundaries.[438] Consequently, there was concern within GCHQ about the legality of selecting transmissions on UK baseband frequencies, and about selecting UK telephone codes for bulk selection. Government legal advice was obtained, which apparently stated the practice was legal.[439] Obtaining information about that advice is currently impossible, as legal advice is exempt from Freedom of Information requests and is not released to the National Archives, regardless of the question of 'national security' exemptions. What is most significant for our purposes is to note that with satellites, the territoriality of communication ceased to map neatly onto the geographical division of the planet into national units. Now, national territories had to be delineated, differentiated, and selected according to purely technical criteria: the numbers that indicated baseband frequencies, and the codes that indicated local and regional network zones.

In the 1970s, interception hardware was launched into outer space. High frequency radio transmitters, designated as VHF, UHF, and microwaves, transmit narrow beams at high frequencies that are capable of much higher rates of data transfer than shortwave signals, and attract less interference. Such signals do not skip off the atmosphere but carry on in beyond the horizon, radiating into outer space.[440] Line-of-sight relays are required to intercept the beams and relay signals onwards, usually positioned no more than around forty kilometres apart. The Post Office Tower in central London, opened in 1964, is a conspicuous example. The use of high frequency relays meant that all such signals could be secretly intercepted from space. The US Rhyolite and the short-lived British Zircon projects were only the first generation of interception satellites, circling the globe in high synchronous orbits, ensuring collection occurred just above every horizon.[441] They created an orbital network that still collects and relays communications traffic down to dedicated earth-stations, like

[438] Aldrich, *GCHQ*, 343–44.

[439] Hugh Lanning and Richard Norton-Taylor, *A Conflict of Loyalties: GCHQ 1984-1991* (New Clarion, 1991), 69 I contacted Mr Norton-Taylor seeking further information, without success.

[440] Pascall and Withers, *Commercial Satellite Communication*, 4–5.

[441] Diffie and Landau, *Privacy on the Line*, 99.

the radomes visible at Menwith Hill in Yorkshire.[442] Similarly, high-frequency transmission can be intercepted by ground stations positioned anywhere in the line of sight of a transmitter dish. With a network of receivers located in Belfast and Derry in Northern Ireland, Anglesey in Wales, and Macclesfield, GCHQ collected all voice and data traffic passing over microwave communications circuits in the Republic of Ireland during the conflict in Northern Ireland.[443]

3.5.6 The network of networks

The Defence Advanced Research Projects Agency (DARPA) established the first operational packet-switching computer network, ARPANET, in 1969. Beginning with a small network of university computers in California, it was based on the TCP/IP protocol, which enables computers and local computer networks that use different languages to exchange data. ARPANET formed the basis of what became the internet.[444] One of its first practical instantiations was the NSA's Platform, a global packet-switched network that initially connected up to 125 NSA terminals on four host complexes, each connected by a Honeywell 316 Interface Message Processor (IMP: a precursor to contemporary internet servers). On the Platform system, intercepted data from computers processing communications from satellites, cable stations, radio stations, and telephone networks came together in a distributed network of networks, allowing data from any point in the global NSA network to be copied anywhere else. This enabled the analysis of bulk patterns of communication simultaneously derived from multiple media sources around the world. Intercepted data passing through the NSA network transited the same physical channels as the commercial data traffic that it was derived from, except NSA's traffic was encrypted using a system codenamed 'Blacker', showing that the NSA always recognised packet-

[442] Aldrich, *GCHQ*, 427–61; Menwith Hill is hardwired in the UK's telecommunications infrastructure, see Bamford, *Puzzle Palace*, 419–20.

[443] Aldrich, *GCHQ*, 501.

[444] Although the Internet has many genealogies, see Roy Rosenzweig, 'Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet', *The American Historical Review* 103, no. 5 (1998): 1530–52 and more recently; Tung-Hui Hu, *A Prehistory of the Cloud* (Cambridge, Mass.: MIT Press, 2015).

switching networks are an inherently insecure medium, in which one's intercepted data could potentially be intercepted by others.[445]

As it did for the internet, the TCP/IP protocol gave the Platform network the inherent capacity to expand.[446] The universality of the protocol is the critical element. As with the internet itself, it enables connectivity. The network can be expanded and individual components interchanged or upgraded. Platform set the scene for the complete digital integration of all NSA operations, and for digital connections to international partner networks. To do this, Transmission Control Protocol (TCP) processes data into standardised packets and assigns them a metadata header. Each address on the network is assigned an address by the Internet Protocol address (IP), which then routes them to that address. Packets are transmitted individually via any available connection between intermediate servers on the network. The best path for each packet is heuristically decided independently at each intermediate server, based only on the best available route to the next available relay point. Rather than switching relays to form a connection between two end points, as in a telephone network, TCP/IP switches packets into available channels on the basis of their present capacity. It increases the overall efficiency of a network by maximising the use of its overall transmission capacity to find a route to the destination IP address. Transmission begins without certainty as to the eventual transmission route each packet shall take. If part of the network is damaged, packets are automatically re-routed via available channels until they reach their destination address; hence its appeal to defence planners contemplating nuclear war. Packets may not arrive in serial sequence, as each has potentially taken a different route to the destination, so they are buffered, collated, and then reassembled in their original file format according to TCP at the destination IP address. Collectively, each message that is sent between two IP

[445] NSA, 'The PLATFORM Network Evolution', *Cryptologic Quarterly*, 1989, https://www.nsa.gov/news-features/declassified-documents/cryptologic-quarterly/assets/files/The_PLATFORM_Network_Evolution.pdf.

[446] Johnson, *American Cryptology III 1972-1980*, 1998, 155.

addresses is relayed via a large number of independent 'micro-decisions' regarding each packet at each intermediate server.[447]

Military and SIGINT circuits therefore populated the datalinks of the early internet before other forms of traffic, and they still do. Military, governmental, and civilian traffic share the same channels. This was the case even prior to packet-switched networks. In the United States and globally, some specific physical links are of course reserved exclusively for military or government purposes, but strategically, relying exclusively on a totally separate infrastructure is risky, as dedicated channels are obvious targets for disruption. The more lines are potentially available, the lower the risk of losing communication capabilities. Defence circuits are therefore deliberately integrated into civil communication infrastructure. As Hu puts it, any particular 'type' of network on the internet, from military circuits to cloud services, should be viewed as "a logical overlay, rather than a physical thing; it is a process, not a static moment".[448] Symbolically, the internet has always been a military installation, but no more so than it is a university installation, a commercial installation; a general purpose infrastructural medium that can be observed as mediating differentiated communication, none of which determine it.[449]

3.5.7 Collect it all

IP addresses are like postal addresses, they define the position of operations in the network, nothing more. The symbolic instantiation of meaning to those nodes depends on other techniques. 'Users', the position assigned to subjects (including both

[447] The mechanism and protocol was first described in publication in the classic paper by Baran, see Paul Baran, *On Distributed Communications Networks* (Santa Monica, California: The RAND Coporation, 1962), https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf; For an excellent introduction, see Florian Sprenger, *The Politics of Micro-Decisions*, trans. Valentine A. Pakis (Lüneburg: meson press, Hybrid Publishing Lab, 2015), 34–53, http://meson.press/books/the-politics-of-micro-decisions/.

[448] Hu, *A Prehistory of the Cloud*, 15.

[449] This is precisely Rosenzweig's point, Rosenzweig, 'Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet'; The genealogy of the relationship between the infrastructure and its effects is the central theme in Hu, *A Prehistory of the Cloud*; Conversely, for an attempt to read the relationship between infrastructure and effect according to the logic of contemporary 'cloud' computing, see Benjamin H. Bratton, *The Stack: On Software and Sovereignty*, Software Studies (Cambridge, Mass.: MIT Press, 2015) .

humans and intelligent machines), are bound to IP addresses via other indexes, primarily the databases compiled by Internet Service Provider companies. Those records convert IP addresses into human subjects, who are tied to their machine addresses using cryptographic authentication software.[450] Hence there is a genealogical link from interception techniques, via cryptography, computer processing, and computer networking, back to interception techniques performed on the data of internet 'users' today. Whereas the NSA aims to "collect it all",[451] the 'it' refers to operations that are in part derived from its own past operations. The internet was intercepted in advance.

The software programs and hardware used to intercept internet communication as described in the Snowden archive are not addressed here. They exceed the scope of this genealogy, and requires a more thorough exposition than can be accommodated. However, it is instructive to briefly consider how elements of the genealogy presented above converge. At the transmission level, interception is possible in the 'micro-decisions' taken at each server. Just as every Internet server is required to inspect the destination IP address of each packet it receives, it is equally possible a server to conduct 'deep packet inspection' on the traffic it processes. Such packet inspection is openly used in some markets, for instance where commercial Internet Service Providers offer their subscribers priority speeds on certain types of traffic. For instance, a company may prioritise the transmission of data packets carrying a live 'stream' of certain sports broadcasts, at the expense of other packets.[452]

If a particular server is equipped with sufficient specialised hardware to temporarily buffer (i.e., copy) all traffic, analyse the packets for key selector terms, and copy all selected packets to a storage and processing system elsewhere, then it can effectively intercept all internet traffic. The micro-decisions performed in each server of the

[450] Cornelia Vismann and Markus Krajewski, 'Computer Juridisms', *Grey Room* 29 (2008): 93.

[451] Glenn Greenwald, *No Place to Hide* (New York: Macmillan, 2014), 90.

[452] This issue of 'network neutrality' involves a long-standing debate between competition lawyers and civil liberties lawyers, for a useful overview see Lucie C. Audibert and Andrew D. Murray, 'A Principled Approach to Network Neutrality', *SCRIPTed* 13, no. 2 (2016): 118–43.

internet afford the opportunity to apply interception decisions. This undermines in advance "the dreamlike promise of a democratizing Internet" as an inherently open, architecturally democratic system.[453] As Florian Sprenger puts it:

> The extent of the subsequent automated surveillance is an effect of the architecture of digital networks. The place of decision-making during the time of interruption is the main gateways at which the necessary act of control is placed side-by-side with the act of surveillance.[454]

Both GCHQ and NSA apply this principle at points where submarine fibre optic cables come ashore, forming bottlenecks through which international internet traffic must pass. Fibre optic cables have reclaimed superiority from radio waves, facilitating an exponential growth in world communication.[455] The genealogy presented above reminds us that the data being intercepted and copied from the packet-switching internet is forwarded into another packet-switching network, the NSA-GCHQ global network that predates the public internet.[456] This 'upstream' collection carries on the inheritance of constant radio-watch and automated cable and satellite 'taps'. Hence within the internet, digital media intercept digital media. Intercepted packets flow past non-intercepted packets indifferently, their symbolic status to be determined at their destination. It just depends on gaining access to enough servers, bearers, or devices to ensure one has enough 'coverage' to intercept and re-assemble meaningful files that have been broken down and dispersed during transmission.

Nonetheless, intercepting data in transmission on the internet is as demanding on resources as it was in the era of the telephone. It remains easier to obtain data 'at rest', just as it was easier to collect telegrams, record phone calls, or obtain magnetic tapes. One of the biggest controversies arising from the Snowden documents was the

[453] Christopher M. Kelty, in the foreword to Sprenger, *The Politics of Micro-Decisions*, 15; This observation has been made before, of course. See, Galloway, *Protocol*; the classic 'cyberlaw' account is Lawrence Lessig, *Code 2.0*, CC Online (Basic Books, 2006), http://codev2.cc/download+remix/Lessig-Codev2.pdf.

[454] Sprenger, *The Politics of Micro-Decisions*, 54.

[455] Starosielski, *The Undersea Network*, 45–46.

[456] The distributed network of NSA and its allies also operates its own search engine, XKeyscore, see 'XKeyScore - NSA Presentation', *Snowden Doc Search*, 25 February 2008, https://search.edwardsnowden.com/docs/XKeyScore2013-07-31nsadocs.

existence of the NSA's PRISM system, through which major internet service providers granted access to user's data: stored, processed and profiled.[457] 'Users' are preconfigured for interception. At scale, the semantic content of messages becomes irrelevant when compared to the information generated by observing patterns 'mined' from datasets.[458]

3.6 Conclusion

According to the theory of cultural techniques, media condition the transmission, storage, and processing of information. The techniques by which they perform these operations define their agency. The way that things can be handled is predetermined before any wilful subject claims control over them. In this chapter, organised interception, which began with the postal service and continued across new technical media, is the outcome of a radically different array of techniques performed through different technical media. In a chain of substitutions in which one medium displaced or replaced another, the role assigned to persons in the interception of communication disappeared. Now, human analysts who are nominally making decisions about interception work from carefully designed user interfaces.[459] Different media and prescribed different interception techniques, which like media themselves, either replaced older media and techniques, or existed diachronically alongside them.

With the emergence and implementation of digital media, however, interception has slowly become fully automated. Where cultural techniques are performed through persons and bodies, the cultural techniques of the law functioned to assign subjective action to the person executing the technique. But where techniques are performed by media and therefore executed independently of bodies, they are formalised as rules, directions, instructions, and other symbolic means of applying rules in order to explain and assign subjective responsibility.[460]

[457] Greenwald, *No Place to Hide*, 108–15.

[458] Experiments in automatic pattern recognition and its correct interpretation are ongoing, see 'GCHQ Problem Book'.

[459] See section 6.1.

[460] Vismann, 'Cultural Techniques and Sovereignty', 88.

At the media-technical level, all interception techniques surveyed in this chapter are performed at defined spatio-temporal points of privileged access. Communication operations, through which a 'sender' and 'receiver' appear to exchange information across space or time, are themselves generated from the operations of transfer media, symbolically articulated through techniques by which each assumes their position in relation to the message. Media transfer information regardless, and in so doing they designate both 'ends' of the communication. The poles of each transfer operation do not pre-exist the transfer operation itself. Hence interceptors, too, are assigned their roles by transfer operations. Their position is the one from which all communication can be selected. Intended receivers, by contrast, are assigned their position by each communication operation.

The distinction between a legitimate and illegitimate act of interception is symbolically designated by the normative order of law, which assumes that interception is the result of the will of one subject who wishes to know the communications of another without that information being visible to the other. As demonstrated by the prohibition of interference with telegrams in the absence of a warrant, and the prohibition on acting on radio signals addressed to someone else, there is nothing in the transfer operation itself that discriminates between legitimate and illegitimate interceptors. Materially speaking, they are exactly the same. Addressing translates the physical nodes in networks of metal wires, radio waves, or optically connected interconnected servers into the symbolic domain of alphabetic text and thereby into the domain of law and subjects. But addressing does not determine or exhaust the possible operations of the network. For an interceptor, all addresses in a network are universally accessible. Hence the data used to address communication to a specific point in a network is reconstituted as the data required to secretly select information from the network medium for copying. Addresses function as commands carried in interception warrants and executed by interceptors.

The interceptor is thus the one who occupies the position of sovereign observer who sorts data, which is a position assigned by the medium itself. The 'sovereign' position is used here figuratively, indicating whatever agent occupies a technically "privileged position of observation and intervention".[461] Sovereignty in relation to communication media is the position that the interceptor must occupy, a position derived from the medium itself, which determines the capacity to process information. The role of governments in legislating for interception has been to ensure that they have access to that position in relation to each medium at stake, and to ensure that others are relegated to the positions of 'sender and receiver', or 'user', who must communicate through the interface available to them and accept the risk of interception.

When humans are out of the picture and all communication and interception is automated, media are sovereign. Media intercept media. All that is required is a quantum of information issued by the 'user' of the digital command system to send instructions to the sovereign-interceptor system, which executes its instructions in the form of a 'conditional jump'. An IF-THEN command instructs a processor, whether human, mechanical, fibre optic, or silicon, to make a coded selection among the data it is processing. It copies the selected element and returns the copy for further processing, while releasing the original element to complete its transmission circuit.

Controlling access to the symbolic position of the interceptor-sovereign is a long-standing function of the law, which claims the right to define the media that transfer the data required to make 'conditional jumps'; that is, to make selections from the privileged position of interception. That data is transferred through the making of legal media named warrants, to which we now turn.

[461] Pottage, 'Power as an Art of Contingency', 13.

4. Programming Warrants

4.1 Introduction: execution

Since 1710, the British state has used warrants to direct interception. In 1710, legislation concerning the Post Office made it an offence to interfere with the post, except pursuant to an express warrant made under the hand of the Secretary of State. Since then, it has been a criminal offence to interfere with communication other than where authorised to do so by a Secretary's warrant.

Warrants are typically understood to be legal tools used for administering political power. A warrant legally authorises its addressee to do something that, but for the warrant, would be illegal. Where a warrant commands the searching of premises, or the arrest of a suspect, it authorises the bearer to do something to a third party. Its target is the object of administrative power; the warrant transforms its addressee into its agent. A warrant may be seen as a way of transmitting or extending power, giving a longer reach to the command of the authorising authority by recruiting its addressee to perform the task. In this sense, it acts as an instrument, a medium for the extension of the sovereign's will, voice, or presence, allowing the power inherent in the sovereign, whether that be a person or an office, to extend beyond their immediate locus.

Warrants do not merely authorise actions, however. There is an imperative: the warrant's command must be performed. It is wrapped up in the official status of its addressee. For instance, a police officer does not arrest a suspect under a warrant as an optional exercise of delegated authority, but because it is their duty to do so. It is inherent in the official status that they hold. In this sense, the addressee of a warrant must obey it; the instructions that it delivers must be executed.

Warrants command their own execution. It is no coincidence that the word 'execution' is the term used in computer science for performing the instructions contained in a program of commands. The ability to enter different conditional programs into a warrant is one reason for the durability of the form as a symbol of legal authority. In their execution, warrants define and order operations according to the terms of their programming. In relation to interception warrants, the symbolic role of the Secretary of State as the authorising authority is programmed into the device. She appears to command the interception of communications, regardless of what operational steps 'interception' involves. The old juridical schema of sovereign power is repeated in the programs of warrants, and the law in turn has confirmed this symbolic authority through its own programs, as shown in chapter five. But that is only an effect of how the warrant is programmed. This chapter decompiles the warrant to present a genealogical account of their making.

4.2 Medieval warrants

Warrants belong to a sort of primal scene in the history of written legal culture in England. During the reign of Edward I (1239 – 1307), a survey was made of holdings of the nobility, asking by what warrant (*quo warranto*) they held their franchises and privileged jurisdictions. If they could not trace their claim to a documentary source, it would not be recognised by the King. The word 'warrant' comes to the English language from the French 'warrant' or 'warand', a regional variation on 'garant'. For a while, it was commonly used generally to signify a guarantee, protection, defence, a place of refuge, or taking safeguards,[462] and the time of the *quo warranto* hearings, 'warrant' did not specifically refer to a particular species of document, but what documents could do.

The documentary form typically used in the thirteenth century for granting and proving legal title was a charter, typically obtained from the Chancery by donors passing title to a beneficiary. Charters were not addressed to the beneficiary directly but to an undetermined future readership, for example, to "those whom the present writing shall reach".[463] Legal rights began as specific grants. Charters awarding titles and privileges had long been the mechanism of rule for Germanic and Anglo-Saxon

[462] 'Warrant, n.1', *OED Online* (Oxford University Press), accessed 19 June 2017, http://www.oed.com/view/Entry/225837.

[463] Clanchy, *From Memory to Written Record*, 85.

kings.[464] Although some pre-date the Norman conquest of 1066, by the thirteenth century they had become the only recognised form of legal title, and tens of thousands of charters were issued. For Clanchy, Edward I's *quo warranto* prosecutions mark the differentiation point between a law that recognised oral or object-based claims, and a law that recognised only documentary claims.[465] During the trials, the following was said to have occurred.

> [The] Earl Warenne was called before the King's judges. Asked by what warrant he held, he produced in their midst an ancient and rusty sword and said: "Look at this, my lords, this is my warrant! For my ancestors came with William the Bastard and conquered their lands with the sword, and by the sword I will defend them from anyone intending to seize them".[466]

Clanchy observes that the survival of the story in legend is itself reflective of the fact that, at the time, an oral culture of memory and law was being supplanted by the centralisation of legal authority under the King.[467] Until the *quo warranto* trials, objects including swords, knives, and cups had indeed served to materialise titles to property, in some cases such artefacts were physically attached to charters. Regardless of what actually unfolded, Clanchy claims that the Earl Warenne story serves to memorialise both the injustice of undocumented legal titles being seized, and to simultaneously mourn the loss of oral culture in itself. And indeed, in 1290 the King compromised on *quo warranto*, passing a statute stating that charters were only required to authenticate legal title transfers post-dating the accession of Richard I in 1189. That somewhat arbitrary date, which remained significant in English land law for centuries thereafter,[468] marks the point from which all property titles have been warranted by documentary transfers, an economy based on possession of authenticated material

[464] Alan Harding, ***Medieval Law and the Foundations of the State*** (Oxford: Oxford University Press, 2002), 17.

[465] Clanchy, *From Memory to Written Record*, 42.

[466] Ibid., 36.

[467] On the story's connection to the complex evolution of the King's authority, see, Harding, ***Medieval Law***, 215.

[468] Clanchy, *From Memory to Written Record*, 42.

objects, rather than the physical act of occupation and possession. What mattered was the document, not what it said on its face.[469]

Clanchy's description of 'warrants' symbolising a shift from oral law to written law is borne out in other sources. The Oxford English Dictionary lists John de Trevisa's *Polychronicon Ranulphi Higden* of 1387 as an early example of the word 'warrant' in use; here in reference to a documentary form of royal authorisation, which proved a particular command even "in absens of þe kyng".[470] Another dictionary definition, that of "a writ or order issued by some executive authority, empowering a ministerial officer to make an arrest, a seizure, or a search, to execute a judicial sentence, or to do other acts", was in use by around 1490: 'warrant' was by then a species of writ.

Writs are the earliest forms of 'letters' in England, in the sense of a written missive sent between two people. Most writs were destroyed upon reading, hence not many have survived, but in essence the writ was originally a brief (Latin: *breve*) written message, authenticated by sealed wax. Their use dates from at least the tenth century. It was a uniquely Anglo-Saxon administrative device; the Normans knew of no equivalent prior to invading England in 1066. According to Clanchy, writs were simply "a written command given by one person to another".[471] The device of the writ held "immense administrative possibilities, without as yet any exact analogy on the continent", and the production of Chancery writs soon gave rise to:

> … a flow of documents quite different in character to the formal and solemn charters… [with] no invocations… specifically addressed with a bare

[469] Yet until the advent of central registration, each transfer relied on local knowledge to confirm the status of the property that the document purported to refer to, see Alain Pottage, 'The Measure of Land', *The Modern Law Review* 57, no. 3 (1994): 364.

[470] "Warrant, n.1", *OED Online* (Oxford University Press), accessed 19 June 2017, http://www.oed.com/view/Entry/225837.

[471] Clanchy, *From Memory to Written Record*, 90.

> salutation, [they are] brief informal notifications of what the King has done or wishes to be done, and are direct and to the point.[472]

Writs were issued in considerable number and their validity was independent of time, with the result that no one knew exactly how many writs were in circulation, when they had been made, or what rights and privileges they assigned. Hence, according to Clanchy, clauses like, "I forbid you do X, no matter what writ might be produced" became necessary, in order to give supremacy to a command against unknown rival writs that could be in circulation. For Clanchy, their emergence exemplifies Weber's notion of the "routinization of charisma", in that the presence of God was constantly invoked to bless standard legal transactions, and was therefore "multiplied into tens of thousands of trivial pronouncements".[473]

Until the reign of Edward (1272-1307), writs of the Crown were issued on demand. A person came before the King to complain about a wrong. For a fee, the King issued them a writ to remedy the complaint. For instance, an aggrieved party might purchase a writ addressed to the local sheriff (*shire-reeve*), ordering him to seize the offender in his shire, or a writ addressed to the offender himself, ordering the return of an item on pain of death. Given the slow progress of courts, a royal writ was generally preferable to going to court. But these peremptory writs often only deepened disputes. As a consequence, the number of valid writs in circulation rose assigning incompatible and ambiguous rights and duties. This lead to a "war of writs" in which canny operators accumulated writs in order to pitch them against others, sometimes anticipating the writs that their opponents would present and seeking to purchase countervailing writs in advance.[474] This excess of authority results from the non-discursive products that the Chancery produced. The production of so many documents had the effect that writs could not achieve the performative effects that their rhetorical messages demanded, but instead produced a sort of secondary

[472] S. B. Chrimes, *An Introduction to the Administrative History of Mediaeval England*, 3rd ed., Studies in Mediaeval History (Oxford: Blackwell, 1966), 14; Raoul Van Caenegem, *The Birth of the English Common Law*, 2nd ed. (Cambridge: Cambridge University Press, 1988), 31.

[473] Clanchy, *From Memory to Written Record*, 87.

[474] Van Caenegem, *The Birth of the English Common Law*, 37–39.

economy in which the aim was to monopolise as many declarative statements as possible.

However, in Cornelia Vismann's genealogy of law's writing instruments, the presumption that writing supplanted an oral legal culture, and the related desire to situate the device of the 'warrant' as a kind of *ur*-writing for the law, is precisely not how law's media should be approached. Legal instruments – files, or *akten* in German, which better expresses the duality of taking action and of writing and recording something on paper – do not transmit an absent presence, nor do they simply record and extend the primarily oral expression of subjective will. The prevalent sense that documents have these functions is itself an ascription generated when files are symbolically used – that is, when their commands are executed. Documents and files are not the residue of past oral expressions or commands, but of processes. Their genealogy is protocological rather than oral.[475]

4.2.1 Warrants and the making of writs

The Chancery was responsible for producing and authenticating legal documents, including charters, diplomas, certificates, and writs. It emerged from the *scriptorium* of the King's royal household by the tenth century.[476] The King's household remained a mobile assemblage that had no fixed location, travelling around the kingdom, but by the mid-thirteenth century the volume and complexity of documents being issued by the Chancery necessitated a permanent fixed site. By 1310, the Chancery, like the Exchequer before it, was established at Westminster. There the Chancellor kept possession of the great seal used for authenticating documents. Access to the Chancery was barred except for the scribes and the Chancellor himself. Behind the latticed screen, the techniques of document production were carried out according to strict protocols. Medieval documents carried their authority with them, and so the precise techniques of production were secret, because they constituted the ultimate guarantors of authenticity.[477] The need to confirm the authenticity of documents gave

[475] Vismann, *Files*, 8–10.

[476] Chrimes, *Administrative History of Mediaeval England*, 25.

[477] Ibid., 26.

rise to the discipline of diplomatics, concerned only with differentiating authentic documents from forged ones.[478]

Before a writ was issued, a warrant for the use of the great seal had to be received and entered on the Chancery Rolls. Warrants for the Great Seal are described as:

> … writs, bills or letters, nearly all on parchment, giving the Lord Chancellor, as keeper of the great seal, authority to affix the great seal to them to solemnise the Crown's wishes. Royal commands were expressed, if not verbally, chiefly through the privy seal or smaller seals, later through the signet, and subsequently by signed bill, using the sign manual. Privy seal writs, mere strips of parchment, are much more numerous than letters and "bills", which are a later, but equally formal, development of warrants from the early fourteenth century.[479]

According to Pollock and Maitland, the great seal was the "key of the kingdom" and few actions are attributable to kings that are not evidenced by a document bearing its mark. The earliest surviving great seal of an English King belonged to Edward the Confessor (1042-66). None survive from Harold's reign. William the Conqueror's is therefore the second-oldest surviving seal.[480] While most authenticated formal documents that emanated from Chancery were authenticated by the great seal, other seals – privy seal and signet seal, and later the signature – were introduced over time, sometimes to issue writs, but mainly to make the warrants that operated the Chancery. As they did not publicly circulate, there were fewer warrants than writs outside the confines of the royal apparatus, and far fewer warrants than writs have been preserved. Hence, unlike writs and charters, they were not well known to contemporary writers and historians of the period, and they are not often referred to in documents that were issued from the Chancery. For a time, they were unfamiliar to

[478] Vismann, ***Files***, 74.

[479] "Chancery: Warrants for the Great Seal, Series I, 1230 - 1485 C 81", National Archives, accessed 28 June 2017, http://discovery.nationalarchives.gov.uk/details/r/C3641.

[480] P. D. A. Harvey and Andrew McGuiness, ***A Guide to British Medieval Seals*** (London: British Library and Public Record Office, 1996), 27.

many historians and antiquarians.[481] This is a consequence of diplomatics, which was concerned only with determining the validity of transmitted law, not with how the transmission was made; and historiography, which searched archives assuming that documents could be read as accounts of past events, and paid no attention to texts "neither designed for perpetuity nor [to] carry any probative force… the administrative operations, the transmission medium itself remains a blind spot of legal history."[482]

Early medieval government was conceived of as entirely 'public', in the sense that everything was manifested in the form of issued documents and open proclamations, and the enactment of legal powers of the King under the great seal was typically prefaced with an oral address, performed before his entourage of barons.[483] Yet prior to the ceremonial realisation of a formal document, there was an administrative process, and it is in that process that the warrant has significance. After the Chancery took up residence at Westminster, the Chancellor no longer accompanied the King and the court as it travelled around the territory dispensing justice. He remained at Westminster, presiding over the "great secretarial bureau" of Chancery clerks producing writs and charters under the great seal. The privy seal became the King's "instrument of communication with the Chancellor".[484]

To issue a writ, a warrant made under the privy seal was sent to the Chancery, where it was registered on rolls and counter-rolls that noted the type of writ ordered, the price (the poor had their writs for nothing), and the clerk responsible for making it.[485] A high-ranking clerk was responsible for each writ, but the "almost mechanical" penning of ordinary writs was assigned to lowly cursitors (*cursarii*), and "consisted chiefly of filling with names and sums of money the blanks that were left in the forms

[481] Ibid., 36.

[482] Vismann, *Files*, 74–75.

[483] Sir Frederick Pollock and Frederic William Maitland, *History of English Law Before the Time of Edward I*, vol. 1 (Indianapolis: Liberty Fund Inc, 2009), 205.

[484] T. F. Tout, *The Place of the Reign of Edward II in English History* (Manchester: University of Manchester, 1914), 61.

[485] Chrimes, *Administrative History of Mediaeval England*, 191–93.

that they found in their registers."[486] The rolls listed types of available writs, but the list was not exhaustive. Over time, new forms were ordered by justices in court, and others were occasionally tailored for individuals. No action could be brought before the King's courts without an 'original' writ issued by the Chancery under the great seal. As the law developed primarily in the King's courts, original writs became increasingly valuable, and the power to direct the making of writs increasingly a matter of concern.

Under Henry II (1133-89), a "system of standardized writs" was introduced to "automate and depersonalize the legal process".[487] Forms were standardised so that clerks did not require drafts or personal authorisation for each writ. A seal-press was created, and the number of clerks increased so as hundreds of writs could be produced per week.[488] Disturbed by the proliferation of writs, and the installation of a register of common forms that required "a Chancellor who was such only in name", the barons demanded a 'real' Chancellor sworn to issue writs only under warrant from the baronial Privy Council.[489] The privy seal was originally held in the King's privy, the most intimate and secret (*secretum*, separated) part of the King's household,[490] and was transplanted instead to a fixed office under an appointed keeper. If the barons did not approve of a measure they withheld the privy seal. While royal authority was externally manifested outside the *curia* in documents, the internal relationship of authority between the King and the nobility was articulated through control over seals, which in turn held the power to order writs.

During Edward's reign, writs were occasionally issued directly by the King under the privy seal, and once again the barons constrained the monarch, who promised in 1300 that no writs concerning the common law would be issued except under the great seal. Thereafter, many privy seal writs were issued to the Chancellor simply instructing

[486] Pollock and Maitland, *History of English Law Before the Time of Edward I*, 1:207.

[487] Clanchy, *From Memory to Written Record*, 67.

[488] Ibid.

[489] Pollock and Maitland, *History of English Law Before the Time of Edward I*, 1:208.

[490] On the etymology of secrecy, see Eva Horn, "Logics of Political Secrecy", *Theory, Culture & Society* 28, no. 7–8 (2011): 103–22.

him to set the great seal to some instrument as the "final expression" of the King's will.[491] In 1314, Edward II introduced a new form of personal seal to authorise documents,[492] using a 'secret' seal to communicate orders directly to the Chancellor. By the Ordinances of Walton of 1338, the King was again constrained, agreeing that only writs for simple legal matters could be issued under the great seal via warrants under the secret seal. The measure of its success is its recognition: Pope Urban III wrote in August 1363 to Edward III, "As the pope sees by the King's secret seal that he has the matter much at heart, he will grant the request if possible."[493]

In 1377, King Richard II introduced a signet seal in place of the secret seal, which his personal secretary kept for protection. The *secretarius* had been the personal assistant to the King, and the signet seal thus marked the beginning of the modern symbolic power enjoyed by the Secretary of State.[494] Records from the fourteenth century bear different combinations of the three distinct seals. Impressions of the signet seal alone appear on warrants to the Chancellor, the Exchequer, to Justices of the Peace, and to local sheriffs and other officials.[495] Some recorded writs from the Chancery bear both the signet and great seal, but not the privy seal. Most of the time, all three are present.[496] The earliest surviving English royal signature is that of Edward III, made in 1362.[497] Medieval seals lost currency as the "personal sign-manual" (i.e., the King's handwritten signature) evolved, particularly with the growing availability of paper in Europe.[498]

[491] Pollock and Maitland, *History of English Law Before the Time of Edward I*, 1:206.

[492] Harvey and McGuiness, *A Guide to British Medieval Seals*, 35; David Kynaston, *The Secretary of State* (Lavenham, Suffolk: Terence Dalton, 1978), 2; During the reign of Edward I (1272 -1307) clerks began noting on the backs of documents issued under the great seal, and on the copies of them entered on the rolls of Chancery, a "note of warranty". For instance, "*per breve de private sigillo*" was an entry warranted by a writ made under the privy seal, "*per ipsum regem*" was a personal decision of the King, and "*per consilium*" was one made by the privy council, A. L. Brown, "The Authorization of Letters under the Great Seal", *Historical Research* 37, no. 96 (1 November 1964): 125–56.

[493] Kynaston, *The Secretary of State*, 2.

[494] Ibid., 1.

[495] Chrimes, *Administrative History of Mediaeval England*, 158–66.

[496] Kynaston, *The Secretary of State*, 3–4.

[497] Harvey and McGuiness, *A Guide to British Medieval Seals*, 5.

[498] Kynaston, *The Secretary of State*, 15.

The long struggle for control over making warrants was a struggle for the authority to make law. Warrants did not simply instrumentally mediate between the sovereign and the law, they produced and defined the relationship. As Vismann explains, while the Chancery came 'before' the law, synchronically speaking, it was the place where the law was processed into existence, and therefore the relationship between Chancery and law was also diachronic.[499] Only when an original writ emerged under the great seal did the law, as such, commence. The arcane barriers behind which the Chancery produced its writs, which were copied from exemplars by scribes according to their secret protocols, excluded all others from making enquiries into the origins of the law. Warrants that ordered the making of writs are amongst the non-discursive processors that kept the processing of law moving, products of techniques and agencies that transfer authority within the apparatus of medieval government. They were not part of the law itself, however, and therefore had no legal status. They were executed by being entered in the Chancery's rolls. Warrants served to operate the barriers of the Chancery, to activate the process of writ-making.

Warrants appear to stand 'behind' writs only if one assumes there must be some authoritative origin 'behind' the law; some secret link back to the sovereign's presence or record of his orally expressed will. But as Vismann explains, the erasure of origins was the precondition of law-making. In the Chancery, it was the deletion of writing, not its positive production, that established the validity of the law. Once a draft document had been copied into the final version to be sealed with wax and thus become the 'clean' copy, that is, the 'original' writ, the draft from which it had been copied was made illegible by 'cancelling' it, i.e. crossing it out so that it was obliterated from legibility.[500] The secret of the Chancery was that it had no secrets, it obliterated what lay before the law in order to produce documents that gave no account of their origins and could be compared against no higher power. A warrant was not the secret presence of sovereignty behind each writ, but another barrier, another gateway that stood only for itself and gave no account of its origins. One cannot truly account for

[499] Vismann, *Files*, 17.

[500] Ibid., 25–26.

law in the making, because it is made by destroying and denying its origins.[501] One can only offer opinions.[502]

4.2.2 Seal and persona

The point may become clearer if we address the mechanism by which warrants to the Chancery were fabricated. According to Bedos-Rezak, the protocols of royal seals mattered because seals first and foremost "produced an order of reality grounded in permanence by obscuring the contingency inherent in the individual ruler as a person", and therefore seals "achieved meaning as constitutive agents of the very conditions and framework that made their production and function possible."[503] A royal seal was not simply the validation of a particular warrant or document, but a medium for manufacturing the concept of kingship itself. Seals affixed authority to a document by "incorporating the author into the text", and thereby "transforming the document into a monument, which is the name by which sealed charters came to be known during the twelfth century".[504] This in turn enabled sealed documents to transform individuals into official personae.

Official positions within a-temporal structures, like the state, depend on their ascription as such in the documents that name the holder as an authority. The "individual person was represented on seals as a person subsumed within his group", marking a distinction between the rational individual, their legal personality, and their position in a fictive collective, corporate person that acts through its individual agents.[505] By impressing wax with the medium of the seal, the individual was re-

[501] Ibid., 20.

[502] Vismann identifies this in the sermons of the priest in Kafka's 'The Trial', ibid., 24.

[503] Brigitte Bedos-Rezak, *When Ego Was Imago: Signs of Identity in the Middle Ages* (Leiden; Boston: Brill, 2011), 79–80.

[504] Ibid., 152; 'A written document or record; (Law) a legal instrument' 'Monument, N. : Oxford English Dictionary', accessed 9 September 2017, http://www.oed.com/view/Entry/121852?rskey=wWf7oU&result=1#eid.

[505] Bedos-Rezak, *When Ego Was Imago*, 236; This points towards the sense in which 'the *corpus republicae mysticum* not only acquires identity as a juristic person (a *universitas*) but is also conceived as an infinite perpetuity', see Loughlin, *Foundations of Public Law*, 42; and therefore the precondition for the theocratic distinction between the King's physical body and his perpetual one, as detailed in Ernst H. Kantorowicz, *The King's Two Bodies* (Princeton, New Jersey: Princeton University Press, 1957).

constituted as the "effective site for the production of symbolic activity".[506] The imago of the seal encoded legal identity, materially reproducing it as a replicable resemblance. The *auctores* – the authority of the document – was an imprint of the persona linked to their office,[507] while *officium*, the nature and powers of certain officers, "bestowed distinction on the holder, conveying the almost paradoxical sense both of the honour accorded the recipient and his personal unworthiness".[508]

Therefore, it is a mistake to view medieval documents as instrumental devices that aimed at performing certain ends. Rather, sealed documents produced the identities that then found their own purposes as they were wrapped up in procedures elsewhere, such as in the production of documents by the Chancery. The authority of an office-holder, including the King, is an effect of the mobilisation of particular seals and documents, and the correct application of protocols for its use. This is why the economy of seals could not simply be overridden by royal command. There was no other way to make royal commands.

Seals took effect in all areas of medieval society, not just law and monarchy. Seals were incorporated into both practical and philosophical investigations into signification, "distributing meaning across the spectrum of human experience in a manner at once supportive and constitutive".[509] Seals "trafficked in world disclosure", producing documentary media that generated new relationships and understandings with effects far beyond the legal and administrative context.[510]

Warrants, like writs, generate the administrative power that they were wrapped up in. The point, however, is not to begin by claiming that the secret of authority is that there is no authority, that the symbolic seat of the sovereign is in fact empty, and so on, which has been the work of deconstructionist accounts of law. The originality and

[506] Bedos-Rezak, *When Ego Was Imago*, 157.

[507] Ibid., 159; Harvey and McGuiness, *A Guide to British Medieval Seals*, 41, 95.

[508] Loughlin, *Foundations of Public Law*, 26.

[509] Bedos-Rezak, *When Ego Was Imago*, 253.

[510] Ibid.

force of Vismann's work is that it demonstrates that the symbolic position is an effect of the a priori agency of files, documents, and other modes of writing that take effect by producing law. What needs to be accounted for is not a theoretical replacement for the absent sovereign, but the notion that there should be a sovereign in the first place. The symbolic order of juridical authority does not need to be explained, rather it is the explanation that emerged to account for the production of documents.

4.2.3 Administrative writs

The legal order, then, begins with the need to process the meaning of the writs and charters that emerged from the Chancery. For Van Caenegem, the organisation of a coherent, institutionalised, and singular common law emerged as a consequence of the need to process the conflicting claims that competing writs generated. Amongst the proliferation of the common forms of writs under Henry II, a critical innovation was the 'returnable' writ, which instructed a sheriff to produce the writ before a royal justice at a specified time and place, and coupled sheriffs to the commands of the law.[511]

> The return of the writ [to court] was a practical device completely in line with the increasing bureaucratization of the time and its careful keeping of records; it put the commission to hear the case before the judges and immediately showed them the essential data of the case.[512]

In order to deal with the sheer volume and variety of competing writs in circulation, all referring in some way to the King for their authority but lacking any hierarchy, the transfer medium had to be transferred back to the symbolic authority of the King, this time in the setting of the King's courts. Whereas disputes might begin over a piece of land, theft, or disputed entitlements, writs drew them into documentary form and delivered them to the court for adjudication.

[511] S. F. C. Milsom, ***Historical Foundations of the Common Law*** (London: Butterworths, 1969), 212.

[512] Van Caenegem, ***The Birth of the English Common Law***, 53; Milsom says the writ was "the court's warrant to act", a figurative use of the word indicating the slippage from naming a thing "warrant" to describing its symbolic function, Milsom, ***Historical Foundations of the Common Law***, 22–24; Pollock and Maitland called writs "the justices" warrant for entertaining [an] action", Pollock and Maitland, ***History of English Law Before the Time of Edward I***, 1:206.

> Judicialization turned these executive measures into original writs and judicial instruments initiating formal lawsuits only at a later stage; this was done piecemeal, each new type of writ commanding a specific form of process, so that a good deal of procedural variety resulted… [The writ *praecipe*] was not devised *ex nihilo* as a writ of summons for the royal courts, but started as an executive order of redress addressed to an alleged wrongdoer. In the course of time this sort of order was judicialized in that the alleged wrongdoer was given the chance to come and state his case in the King's court. [513]

In this manner, competing claims were enfolded into legal proceedings, becoming instruments through which a progressively centralised form of royal justice came to absorb other local modes of legal adjudication and set the material conditions for elaborating a coherent common law.[514] The administration and centralisation of the courts transformed writs into procedures.

> A judicial system which was created by the naked will of the King, but made to relate his powers to his people's rights, provided a fruitful context for the definition of the 'state of the King' (*status regis*) in England.[515]

As all disputes referred to law had to be articulated through writs, conversely, writs became the singular form around which both the substance and procedure of law, and the powers of kingship, came to be articulated. Around the documents that attracted opinionated explanations for their existence, dogmas emerged in judgments, commentaries, procedural rules and judicial orders, establishing "normative forms at the margins of a legal corpus, programmes for legal acts and actions, algorithms of the law".[516] Common law grew epiphenomenally around the need to process the symbolic transfers effected by the proliferation of documents. The 'original' writs above evolved into devices for initiating specific legal procedures before courts. Each writ could initiate a case according to a set of procedural rules known as 'forms of action'. Anyone purchasing a writ had to carefully select the correct form of action, because the legal procedure that followed was determined entirely by that selection. The text

[513] Van Caenegem, *The Birth of the English Common Law*, 34.

[514] For a thorough exposition, see Harding, *Medieval Law*, 128–46.

[515] Ibid., 140.

[516] Cornelia Vismann, 'Jurisprudence: A Transfer Science', *Law and Critique* 10, no. 3 (October 1999): 283.

attributed to Glanville, commonly regarded as the earliest compendium of the English common law, is nothing more than a "juridical alphabet", an "exposition of the writs which controlled such cases as were then brought before the court,"[517] and "an insider's handbook for the royal bureaucracy".[518]

As Murphy points out, the "artificial reason" of common law cannot be disentangled from matters of procedural and formal rules. Both government and adjudication were the products of long practical experience in managing disagreement, providing vehicles through which disputes could be articulated and, moreover, society could be apprehended.[519] Common law forms of action are comparable to the *formulae* of Roman law as presented by Yan Thomas, insofar as a given form "was not instrumental; it was not a vehicle for anything other than itself."[520] Writs and warrants defined the world rigidly, not in the service of other latent social goals. The medieval order conceived of the world as a natural hierarchy that unified all things in a coherent structure. Legal instruments did not provide particularised abstract representations of the natural hierarchy, but rather recursively re-generated and re-inscribed people and things into it,[521] service as preconditions for a particular mode of legal discourse through which objects were assigned meaning within a particular frame, each of which made available "a range of remedies which has as it were came down from the skies".[522] To bring a dispute to law, one had to fictionalise it in the terms provided by a particular form of action, as such, "the problem was made real by its very unreality."[523] For hundreds of years, legal technique concerned the ability to fictionalise a dispute so as to make it fit into an available form of argumentation, which then determined the entire legal procedure that would follow. This unreality is

[517] Milsom, *Historical Foundations of the Common Law*, 26–27.

[518] Clanchy, *From Memory to Written Record*, 67.

[519] Murphy, *The Oldest Social Science?* 88.

[520] Alain Pottage, "Law after Anthropology: Object and Technique in Roman Law", *Theory, Culture & Society* 31, no. 2–3 (1 March 2014): 152.

[521] Niklas Luhmann, *Social Systems*, trans. John Bednarz and Dirk Baecker (Stanford University Press, 1995), 282.

[522] Milsom, *Historical Foundations of the Common Law*, 266.

[523] Ibid., 267.

precisely what secured the reflexive stability of the law, which in its operations "secured the world".[524] The procedures of common law are better understood, as Murphy puts it, as ritualisation rather than rationalisation.[525]

This way, law reflexively administered to its own procedures, with registries, rolls, writs and warrants providing symbolic forms for "sending confidential instructions in writing and of checking on whether those writs were obeyed".[526] When Matthew Hale wrote his seventeenth century survey of criminal law, *Historia Placitorum Coronae* (published posthumously), he gave an account of judges' ability to issue warrants for:

> [Arrests] of felons or persons suspected of felony by warrant or precept, namely not of precepts that issue upon matter of record, as upon appeal or indictment, which regularly are to be by writ, but such warrants as a preparatory to it, or for conservation of the peace.[527]

Whereas judicial writs solemnised a final legal decision on a case, warrants preceded them by permitting preparatory orders to be issued according to fixed procedures. On Hale's account, only a Justice of the Peace, coroner, or sheriff could independently "give out a warrant for apprehending the felon before indictment".[528] While warrants were normally directed to sheriffs, bailiffs, and constables, they could be addressed to "any private person or his own servant". Any officer so addressed by a warrant was required to execute it, within their jurisdiction.[529] Hale recognised the potency of these devices. By authorising action before the determination of a case by the law, warrants risk supplanting the law. Hale was particularly concerned with elaborating the correct protocols for making writs of the Crown, particularly the issuance of general, open-

[524] Murphy, *The Oldest Social Science?* 76.

[525] Ibid., 71.

[526] Clanchy, *From Memory to Written Record*, 91.

[527] Sir Matthew Hale, *The History of the Pleas of the Crown (Published from His Lordship's Original Manuscript, and the Several References to the Records Examined by the Originals)*, Reproduction from British Library, vol. 2 (London: Gyles, Woodward, and Davis, 1736), 105.

[528] Ibid., 2:106–7.

[529] Ibid., 2:110.

ended warrants.[530] He states that each warrant had to make clear the reason for its issue, except in cases of felony or treason, and that warrants should not be issued blank by the court so as to be filled in with names later.[531] The form of the warrant had been reconfigured as a legal instrument, and subjected to legal protocols. What was ultimately issued, necessary for the law to have agency in the world, was a physical warrant.

The instrumentalisation of the law, which generates and applies normative rules and sees that they are executed, is built on and preceded by the techniques and practices of document production. The elaboration of jurisprudence, for Vismann, is the effect of the transfers of rights and entitlements that documents perform. Legal technique is the putting into order of the files and documents of the law, which process the symbolic order that the law produces. The text inscribed in legal documents is the software that describes and orders the operations of their hardware.[532] Documents transfer and transact rights, powers, debts, and attribute legal subjectivities. The particular instrumental ends that legal media are put to are protocological responses to symbolically account for those operations.

4.3 The interception warrant

By the sixteenth century, the Secretary of State had emerged as the primary "agent for communicating the king's pleasure".[533] Beginning as keepers of the signet seal in the fourteenth century, the secretaryship grew in importance as the signet, like the great seal and privy seal before it, became formalised and integrated into procedures that explained its operations and effects. Secretaries of State kept the signet in their custody, receiving it in a formal presentation on appointment and delivering it

[530] Ibid., 2:114; "A written document or record; (Law) a legal instrument", "Monument, n.: Oxford English Dictionary", accessed 9 September 2017, http://www.oed.com/view/Entry/121852?rskey=wWf7oU&result=1#eid.

[531] Hale, *Pleas of the Crown*, 2:111.

[532] Vismann, 'Jurisprudence', 284.

[533] Mark A. Thomson, *The Secretaries of State 1681-1782* (Oxford: Clarendon Press, 1932), 65; Jill Pellew, *The Home Office 1848-1914: From Clerks to Bureaucrats* (London: Heinemann, 1982), 2; according to Kynaston, Thomas Cromwell, Secretary to Henry VIII, marks the decisive shift in the Secretary's role, from medieval functionary to active political agent. Kynaston, *The Secretary of State*, 13.

directly into the King's hand on resignation.[534] The signet seal was affixed to all 'personal' communication issued by the King. Registers were kept of all letters issued under the signet seal. The staff of the signet office, employed by the Secretary of State, drafted and transcribed formal letters on behalf of the King, which he signed and the Secretary sealed.[535] By the time of the reign of Charles II in the late seventeenth century, there were four signet clerks, with at least one attending the court wherever it moved.

Although all administrative acts were recorded in writing, they were stored in a disorderly fashion created a "general and unclassifiable mass of documents."[536] The secretaryship was a sinecure; effectively, a secretary was his King's client. Offices were essentially viewed as property.[537] Secretaries (like other officials) charged for their services, and often took their papers away with them on leaving office.[538] As Luhmann observes, today it would be called "corruption".[539] There were two conflicting theories about the status of secretarial papers; the Secretary was a private and personal servant whose staff, papers, and techniques were his own concern; but at the same time, the office-holder was responsible for the most important administrative questions of state, and therefore considered to be a public servant under the law, who produced public records.[540] A distinction was also drawn between formal documents passing the signet as a stage towards the making of a writ under the great seal, and the "personal correspondence or private commands of the King, which were sealed with the signet only… the distinction between them is, in the main, one between administration and

[534] Florence Greir Evans, The Principal Secretary of State: A Survey of the Office from 1558 to 1680, (Manchester: Manchester University Press, 1923), 197.

[535] Ibid., 194.

[536] Under Arlington's Secretaryship, the 'papers of state' were housed in the chimney of the office. Ibid., 177.

[537] Sir Daniel Norman Chester, *The English Administrative System 1780-1870* (Oxford: Clarendon Press, 1981), 18.

[538] Thomson, *Secretaries of State*, 144–46.

[539] Niklas Luhmann, *Theory of Society*, trans. Rhodes Barrett, vol. 2 (Stanford: Stanford University Press, 2012), 71, 'real politics was made and exploited above all in patron-client relationship – partly to generate loyalty in one's own territory, partly to intervene conspiratorially in other territories".

[540] Evans, *Principal Secretary of State*, 189.

politics."[541] The elements of the symbolic order of the medieval juridical hierarchy had survived, although they had been rearranged and reconfigured.

4.3.1 Command and reason of state

During the seventeenth century, the concept of *raison d'état* was promoted by the Stuarts as the basis of their rule. As a result, their dynasty (1603-1714) was interrupted by the execution of Charles I and Cromwell's 'Interregnum' government. According to the logic of *raison d'état*, the juridical order was founded on the absolute authority of monarchs. Put briefly, where necessity demands, *raison d'état* held that the monarch could personally determine the situation and make decisions that could not be questioned or examined by judges.[542] Viewed historically, the insistence on the absolute power of the sovereign was an attempt to secure political survival after theology had exhausted its capacity to compel obedience. In France, the doctrine of the "will of the sovereign formed part of the solution to societal instability".[543] But in England, the Crown's authority relied on a "different overall cognitive and normative environment" to the rest of Europe,[544] so that rather than securing social order, the absolutist model of government in England only led to greater instability.

While *raison d'état* invoked the mysteriousness of divine monarchy under the rubric of *arcana imperii*, in fact the real "secret of authority was that it was none",[545] and so-called 'state secrets' were "neither more nor less mystical than the modern concept of the secret 'know-how' of a business."[546] To some extent, it simply meant keeping things off the record. James I, for instance, attempted to use the signet as "the private seal it had originally been", but finding it already "too formalised", he instead used a "bedchamber" practice to issue secret orders. Charles II, making a secret treaty with France in 1676, did not let the "dangerous document pass the seals", instead he

[541] Ibid., 195.

[542] Loughlin, *Foundations of Public Law*, 379–81.

[543] Murphy, *The Oldest Social Science?* 79.

[544] Ibid., 79–80.

[545] Luhmann, *Theory of Society*, 2012, 2:71.

[546] Carl Schmitt, *Dictatorship*, trans. Michael Hoelzl and Graham Ward (Cambridge: Polity, 2013), 10.

"sealed it with his cipher, himself lighting the taper to melt the wax."[547] The true secret was the one that did not enter the register.

Yet reason of state did manifest itself in written forms. The Secretary of State Henry Coventry wrote on 13th September 1677 to the Postmaster General that "a Secretary of State may demand an Account of any letters that come to the post house from anybody employed there". To intercept letters, Secretaries of State needed no permission except the King's,

> to all inferiors their Order is sufficient or else our Warrants to the postmasters are illegal, they not being our servants. The opening of letters is what no man can justify but from reason of State or the King's particular Command.[548]

As Evans notes, the Post Office was created for the transmission of state dispatches, not private correspondence. Transmitting and receiving state dispatches was the "essential function" of the secretariat; the posts grew out of that function, which "naturally brought them under the influence of the chief writer of those dispatches."[549] Yet even reason of state remained indexed to documentary forms. In another letter, Secretary Coventry recounted that Charles II orally ordered him to intercept the letters of Edward Coleman, a Catholic courtier executed under false charges of treason in the 'Popish plot'.[550] Coventry asked for a written order, but Charles "told me there was no need of an order because the matter was to be kept secret". Coventry explained he wanted only "to justify myself in case of his forgetting", because Charles was capricious. But Charles replied that his memory would suffice. The Secretary had no choice, he instructed the Deputy Postmaster to intercept and copy Coleman's correspondence with "severall Roman Catholiques both at home and abroad".[551] If Charles would not commit his command to writing, it would have been unwise for Coventry to do so in turn.

[547] Evans, *Principal Secretary of State*, 203–4.

[548] Ibid., 284.

[549] Ibid., 283, 285.

[550] Coleman was beatified as a martyr by the Catholic Church in 1929, 'Edward Coleman', *Catholic Online*, accessed 16 September 2017, http://www.catholic.org/saints/saint.php?saint_id=3052.

[551] Marshall, *Intelligence and Espionage in the Reign of Charles II, 1660-1685*, 83.

Charles' oral command, and the concern it caused Coventry, is instructive. On one hand, Coventry formally had to accept that the King's decision was law, absolute and supreme; on the other, he knew that without a written record, his own actions risked being deemed illegal. The law held that the prerogative power of the King to govern was "no more than what the law has determined", and that where it was exceeded, the ministers involved were personally responsible, because the "King could do no wrong". Oral statements remain off the record. The action that does not enter the register is secret, and the one that can be denied, but only Charles would be exempt from the consequences if he later decided to discuss it. If a warrant or other instrument was found to be illegal, there always had to be someone who could be held legally responsible for "deceiving" the King, thereby inducing him to commit a "temporary injustice".[552] Indeed, on 18th November 1678, another Secretary, Williamson, was sent to the Tower of London by Parliament for illegally signing commissions in favour of "popish recusants". Williamson's claim that he merely counter-signed orders from the King only made things worse for him, as his function – his only function – was to take the signing of warrants seriously.[553]

Hence Coventry's problem was not simply a matter of obtaining a written record of the King's true will at a fixed point in time. Even under conditions of *raison d'état*, files generated responsibilities that had to be respected. For a Secretary, doing something that went unrecorded in writing was a very real risk because it was to abdicate his status as office-holder and act only as a person. The authority of his office was wrapped up in the protocols for making signet warrants.[554] Outside those protocols, he had no legal authority. Only through the practices of registering, drafting, counter-signing, and sealing could a Secretary of State take effect. The problem was not the legality of letter interception against the rights of Coleman – a Catholic, accused of treason, who was ultimately condemned to death on the basis of letters found in a search of his home – but how it was to proceed.

[552] Chester, *English Administrative System*, 12.

[553] Evans, *Principal Secretary of State*, 142–43.

[554] Niklas Luhmann, *Law as a Social System*, trans. Klaus Ziegert (Oxford: Oxford University Press, 2004), 463.

Warrants, then, do not merely represent or confirm lawful oral commands even under conditions of *raison d'état*. Oral commands cannot take effect in administrative terms. Only writing can, and only writing produced according to the procedures that make the correct form, which do not follow the logic of speech.[555] A warrant unsigned, unsealed or prepared incorrectly could not take effect. Documents issued under signature and seal, however disorderly they ended up when stored, functioned by providing their addressees with both "imperative and information",[556] recursively generating the 'culture' that transformed offices "from mere collections of independent employees to departments of state".[557]

4.3.2 The function of warrants

By section 40 of the Post Office (Revenues) Act 1710, interference with the post was criminalised except where subject to "an express warrant in writing under the hand of one of the principal secretaries of state".[558] The necessity for recording all imperatives in writing, and naming such documents as 'warrants' was thus confirmed in legislation. The implication of the legislative formulation is that the Secretary of State's warrant gives lawful form to a type of decision or command that the Secretary of State is uniquely empowered by law to make, and thus responsibility for the interception operation that results is made attributable to the Secretary alone by the law. The Secretary acts autonomously through warrants according to the law, but from the perspective of media, the ascription of decision and autonomy to the Secretary is merely the recognition of long-standing techniques for processing the administrative effects of warrants.

More importantly, the legislation defines the privileged position of interception. Anyone who works in the sorting office of the Post Office has, at least in theory, the capacity to intercept communication. The position is defined by the processing of

[555] Vismann, ***Files***, 4.

[556] Ibid., 8.

[557] Evans, ***Principal Secretary of State***, 168 fn1.

[558] Section 40 and 41, 'Post Office (Revenues) Act 1710', 9 Anne I, c. 11 § (1710).

letters through the Post Office. Intercepting letters therefore had to be inscribed into the symbolic order of the law in order to assign authority to the Secretary of State by excluding all others.

The earliest surviving interception warrant identified by the parliamentary Secret Committee of 1844 was dated 20th September 1712, not long after the passage of the 1710 Act. Incidentally, the only earlier case that the Secret Committee mentioned was that of Coleman, the target of Charles's oral command to Coventry. The Committee noted that despite the Post Office Act 1710 and a Parliamentary resolution of 1735 which stated that a Secretary's warrant was the only lawful means of authorising letter interception,[559] until 1799 "it was not the practice to record such Warrants regularly in any official book".[560] The Committee reported that general interception warrants were issued during the Jacobite rebellion of 1745 and on the declaration of the Seven Year's War against France in 1756, but makes no mention of any record of those documents.

The image at figure 1 is an example of a copy of a Home Office warrant dated 28th April 1792.[561] It is contained in a Home Office entry book of copies of 'Out Letters' in the National Archives. Based on this copy, the document loosely resembles a letter. It begins:

> To His Majesty's Post Master General,
>
> This is to authorize and direct you to open and take copies of all letters which pass through the Post Office directed to any of the following persons.

There follows a list of eleven names, headed by two notable entries, Thomas Paine and John Horne Tooke.[562] No reasons are provided as to why they are targets. Some

[559] Thomson, *Secretaries of State*, 154.

[560] 'Secret Committee', 9.

[561] 'HO 42/208 Letters and Papers. Correspondence Relating to Post Office, Customs, Excise, Auditors' Office, College of Arms, Lord Chamberlain and the University of Oxford.' 1792, 101, National Archives.

[562] This marked the era of the so-called "treason trials". John Horne Tooke was a politician, one of the last people tried for sedition on account of criticising the monarch in 1794. Paine was an English-American philosopher and political activist.

of the names are located in particular cities: Bruxelles, Rotterdam, The Hague. The warrant's authority is confirmed with the phrase,

> And for so doing this shall be Your Warrant. Given under my hand and Seal at Whitehall, the 28th day of April 1792.

Here is the administrative function of the warrant: making lists.

For the interceptors in the Post Office, lists of targets provided them with the information required to discriminate between the letters that they searched. The cities mentioned would direct the sorting clerks to provide the relevant foreign mail bags for searching, and the names would enable them to identify individual letters, seals, and handwriting to recursively include in their search operations. Interception warrants existed as elements in an information exchange, a two-way transfer operation by which the Home Office transferred lists of selected targets to the Post Office, which performed the technical operations of searching, selecting, and copying, then returned intercepted material to the King and Secretary of State for the Home Office for processing. For interception techniques to take effect, conditional instructions are required. They enable the differentiation of targets from non-targets, and thereby provide the input that operationalises the whole procedure.

The process was bookended by lists, which also controlled the output from the Post Office, where in the eighteenth century, original warrants were burned after use. A 'Distribution List' controlled the transfer of intercepted material outwards. Everything intercepted in plain text went directly to the King, while enciphered messages were couriered to members of the Deciphering Branch for analysis, and sent on to the King as soon as possible. The King passed them to the Secretary of State for circulation to selected ministers, who received them in a distinctive envelope known as the 'Long Packet', then returned them to the secretaries' office for filing and storage under the category of 'private' papers. Ellis suggests that not more than thirty people overall ever saw intercepted material.[563]

[563] Ellis, *Post Office in the Eighteenth Century*, 69–70.

4.3.3 Storage protocols

Record keeping improved after 1782, when the offices of the Secretaries of State became institutionalised as the Home Office and the Foreign Office. Clerks became employees of a bureaucracy administering to programs and policies rather than servants of a patron.[564] According to the Secret Committee, between 1799 and 1805, a registry was maintained of all interception warrants issued by the Home Office. From 1806 until 1844,

> the practice was introduced at the Home Office of recording the issuing of every [interception] Warrant in a private book belonging, not to the head of the department, but to the Office, and always accessible to the two Under Secretaries of State and the Chief Clerk of the Domestic Department.[565]

The separation of interception warrants as a categorised type of Home Office correspondence, and the implementation of record-keeping protocols, confirms a change had occurred in the organisational conceptualisation of power.[566] Files that contain instructions for their own preservation rather than allowing themselves to be discarded or destroyed create the conditions under which historiography first came to conceptualise files as records of things that really happened, rather than manifestations of particular ritualised practices. The 1844 Secret Committee report is in itself an example of this historiographical approach. This explains why it was unable to account for interception warrants any earlier than 1712, the year of the earliest surviving example.

The same thing happened in other government departments. From 1822 onwards, "original warrants [were] preserved at the Post Office; the earlier warrants having been destroyed."[567] By recording and storing the interception warrants that were generated, they became events that linked together actions and time. When a warrant

[564] Chester, *English Administrative System*, 123, 282; For more on this theme, see Pellew, *Home Office: Clerks to Bureaucrats*.

[565] 'Secret Committee', 9.

[566] Vismann, *Files*, 95.

[567] 'Secret Committee', 10, unfortunately, no trace of these warrants remains in the contemporary Post Office archives, nor do they appear to be present in the Home Office sections of the National Archives.

is registered, it becomes an event in time with two valences: an authorisation in the Home Office register, and an instruction in that of the Post Office.[568]

Procedures became more clearly defined. In 1844, the Secret Committee described the contemporary warrant processes as follows. For a criminal investigation warrant,

> The application is made, in the first instance, to that one of the two Under Secretaries of State who is of the legal profession; and the usual course is for the applicant to state the circumstances in writing; but if the case be very urgent, owing to the time being too short, before the departure of the post, to draw out a written statement, that condition is sometimes dispensed with… If the Under Secretary accedes to the application, he submits the case to the Principal Secretary of State; with whose approval, a Warrant is drawn by the head clerk of the Domestic Department, under the instructions of the Under Secretary, and is then signed by the Principal Secretary of State. A record of the date of the Warrant is kept under lock and key, in a private book, to which the two Under Secretaries and the above-mentioned head clerk have access.[569]

Investigators applied to the Home Secretary for authorisation of the interception of correspondence. They provided the names to populate the list. The Home Secretary's staff would then transfer the list into the form of a warrant, enter a copy in the records, and present it to the Secretary for his signature. His 'will' extended to adding his name and, for a while, the signet seal. This way, operations passed through the processing bottleneck of the Home Office warrant, even if the particular ends were not Home Office business. For political warrants, by contrast, the process came from the top down, initiated by the Home Secretary.

> The Principal Secretary of State, of his own discretion, determines when to issue them, and gives instructions accordingly to the Under Secretary, whose office is then purely ministerial. The mode of preparing them, and keeping record of them in a private book, is the same as in the case of Criminal Warrants. There is no record kept of the grounds on which they are issued,

[568] Vismann, *Files*, 81.

[569] 'Secret Committee', 14–15.

> except so far as correspondence preserved at the Home-office may lead to infer them.[570]

There were, therefore, two circuits for interception warrants in existence. In relation to criminal matters the Home Secretary was an administrative element in an investigation process that began and concluded elsewhere.[571] His role was merely to provide access to information thought to be circulating in the postal system. On the intelligence front, the Home Secretary issued instructions "of his own discretion", but he did so on the basis of information received from spies, informers, and information returned from the Post Office. The functional differentiation of interception is manifest in the transfer of information through each of these procedurally differentiated circuits, both inflexions on the repetitive copying operations carried out all day by the clerks.

The Secret Committee's report is itself a governmental document. It is the result of recovering and processing stored files, putting them in order, and giving legal and historical accounts of their existence. It sought to account for the existence of interception techniques that for the previous two centuries, since the foundation of the Post Office in the mid-seventeenth century, had been the preserve of the King's closest ministers. The production of a historical account of those practices by the Secret Committee transformed the status of secrecy itself. It converted it into procedures that could be accounted for, and thus transformed the making of interception warrants into a normative realm. The report anticipated that the archive of warrants would continue to be maintained and that warrants could therefore be counted and reviewed. Therefore, the power to intercept letters, while remaining out of 'public' sight (of which more in the following chapter), would nonetheless provide a material account of itself. Procedures were no longer required simply for a warrant to take effect as a first-order symbol of authority, they were required in order to assess how that authority was made and exercised. From then on, as Vismann puts it, storage of files matters, and "administrative acts reveal themselves to be historical

[570] Ibid., 15.

[571] See, generally, J. M. Beattie, Crime and the Courts in England, 1660-1800 (Oxford: Clarendon Press, 1986).

anticipations."[572] The Secret Committee's report is itself a monument to the new order it inaugurated.

The Committee put forward possible procedural rules for making warrants: granting interception warrants for the investigation of crime only on receipt of clear written reasons; recording those reasons; recording the period of time that each warrant remained in force; recording the number of letters opened under each warrant; maintaining a record of the results it achieved.[573] No such action was taken. But these suggestions prove Vismann's hypothesis that the emergence of the constitutional state, which had become a question for legal theorists and historians in the nineteenth century, did not depend so much on the 'world-spirit' of history or the accumulated wisdom of judges as it did on the "profane administrative techniques" that materialised such spirit in the effort to produce official state archives.[574]

4.4 Office media

From 1848, all papers arriving in the Home Office each day were registered centrally in order to better manage the growth in the bureaucracy. Older papers were selected for disposal, and those that were retained were re-numbered retrospectively into four series that overlap in terms of both subject and date.[575] An inspectorate was created to review and reduce 'waste' by assessing the utility of retaining older materials.[576] During the same period, new technologies changed the administrative procedures and media through which warrants were created. Such media-technical transitions are materialised in an entry book of outgoing letters and warrants send from the Home Office to the Post Office.[577] It is the only collected set of interception warrants available

[572] Vismann, *Files*, 120.

[573] 'Secret Committee', 19.

[574] Vismann, *Files*, 122.

[575] The National Archives, 'Home Office Correspondence 1782-1979', *The National Archives*, accessed 11 September 2017, http://www.nationalarchives.gov.uk/help-with-your-research/research-guides/home-office-correspondence-1782-1979/.

[576] Pellew, *Home Office: Clerks to Bureaucrats*, 64.

[577] 'HO 151/7', 7.

in the National Archives – although its position in the catalogue suggests that similar records once existed and have been destroyed.

4.4.1 The letter copying book

The orderly storage of interception warrants was aided by new copying technology. In 1887 the Home Office acquired copying presses, eliminating the need for clerks to work as scriveners.[578] Copy presses and 'Letter Copying Books' vastly reduced the time required to duplicate items,[579] thanks to the invention of quick-drying aniline ink. They were sold as blank bound entry books containing sheets of tough tissue paper. Dampers, sheets of oiled paper, and blotting material were also required. An office boy counted the number of outgoing letters of the day and prepared the corresponding number of pages in the copybook by dampening them with a sponge. Taking the first available blank page in the book and putting a fresh outgoing letter face up beneath it, he placed an oiled sheet on either side to prevent water and ink from soaking through, then closed the book and compressed it in the copy press for about two minutes, which was essentially a vice-like clamp. When all the letters had been copied, the boy took them to be posted and the book was left to dry by the fireplace. The method gives the records in the entry book a distinctive blotted appearance (figure 2), a consequence of a relatively short-lived cultural technique bracketed by handwriting and typing.[580]

Copied warrants stored in the entry book did not merely register and store past authorisations of warrants, they also recorded cancellations. When a cancellation letter had been sent to the Post Office, the copy of the initial warrant was overwritten with the word 'cancelled', and the date of cancellation added. The practice of writing 'cancelled – date' on copies of letters persisted until 1933, by which point it had simply become an inherited practice. The use of typed cancellation notices had allowed carbon copy 'flimsies' to be put on files, and this negated any functional value that

[578] Pellew, *Home Office: Clerks to Bureaucrats*, 98.

[579] Vismann, *Files*, 298.

[580] Delgado, *The Enormous File*, 78.

overwriting had once served. The practice itself was cancelled on 17th October 1933.[581] The need for cancellation practices was driven by the Post Office. The Postmaster General wrote to the Home Secretary at various stages with lists of names that had returned no intercepted materials asking that their names be formally cancelled. While the Home Office issued warrants and, apparently, simply forgot about them, for the Post Office, the validity of each warrant took effect as an ongoing process by which all mail had to be checked each day for the specified names. The development of efficient file-checks in order to ensure timely cancellations thus began as an administrative efficiency, a kindness to the interceptors rather than to their targets.[582]

In the entry book, the copied warrants are preceded by copied covering letters addressed to the Postmaster General stating the purpose and target of the warrant. Warrants merely repeat the information stated in the covering letter, distinguished only by variations on the phrase we saw used on the warrant of 1792, *And for so doing this shall be your sufficient warrant*, and the formal application of the signature of a Secretary of State. This indicates the symbolic difference between a letter and a warrant. The difference mattered, a warrant needed to be made. Unlike the warrant from 1792 discussed above, there are no references to seals, only signatures. Rather than the medieval symbol of the seal, the Home Office switched to a new system for guaranteeing authenticity: the reference number. The Home Office first adopted a numerical file reference system in 1871, updated in 1880 with an alphanumerical series that began with an 'A' prefix.[583] Earlier entries in the interception copybook, which began in 1876, show reference numbers overwritten in pencil at some point after the

[581] 'Cancellations of Postal Warrants: Practice HO 45/25957' 1933, 25957, National Archives, according to a note in that particular file, however, it went missing until May 1958 when it 'turned up in the Private Office after some years of hibernation'.

[582] Letters from the PMG requesting cancellations appear in collections of in-letters from the Post Office in the early nineteenth century, see 'HO 33/1'; 'Home Office: Post Office Correspondence 1823-1837 HO 33/3' 1837, 3, National Archives; establishing efficient cancellation procedures remained a matter of concern in devising filing protocols, see 'Signing Cancellations of Postal Warrants HO 45/25956' 1928, National Archives; 'HO 45/25957'.

[583] The National Archives, 'Home Office Correspondence 1782-1979' in 1902 a six-digit series starting at 100,001 which continued until 1949, when separate series were introduced for each function, each distinguished by letter symbols.

warrant was initially issued and copied. From around 1890 onwards, file references were included on the face of the original letters (figure 3).

Entries in the copy pressed book end abruptly. The Home Office acquired two typewriters in 1890, with some reluctance. Typing was considered a feminine job, and the subject matter that the Home Office dealt with too distressing and vulgar for women.[584] At that point, typed warrants superseded handwritten warrants. The final letter impressed into the copybook is dated 22nd March 1899; fittingly, it was typed (figure 4).

The file replaced the entry book, centralising all case-matter into one location. Whereas the copybook stored copies of outgoing letters arranged by topic, the file and the filing cabinet brought all elements in a given case together as particularised matters of concern.[585] In figure 5, a stenographer's draft warrant appears in handwriting and next to it is a typed carbon copy of the final document, which includes the standard phrase, *and for so doing this shall be your sufficient warrant*, but bears no signature. From then on, the signature would only be applied to the version that was posted. Intercepted telegrams were copied onto telegram forms and inserted into files (figure 6). A case file concerning correspondence on the interception of telegrams in relation to a murder suspect in 1901 contains a copy of a letter received from the Postmaster General, illustrating the difference between a typed carbon copy slip and an outgoing pressed copy (figure 7). After typing took over, 'original' documents are differentiated from their otherwise identical file-copies by their materiality: the use of pre-printed stationery, embossing, the weight of paper, and handwritten signatures.[586]

[584] Pellew, *Home Office: Clerks to Bureaucrats*, 24 in addition, women would require a separate working area away from men.

[585] Vismann, *Files*, 128–29.

[586] 'Warrants: Post Office Warrant for Search of Private Correspondence, HO 144/674/100653' 1903, National Archives.

With the shift from entry books to individual files, collected case material is bound together with a lace tag and kept in a single uniform cardboard file. Files themselves contain their own protocological procedures. All files can be operated by one administrator, while files can be universally shared amongst bureaucrats who can add their own memos and amend one another's draft letters before they are typed. Files themselves become the active agents in bureaucracies.[587]

4.4.2 References and indices

The introduction of reference numbers evidenced in the copy pressed entry book indicate that warrants had begun to be produced within a new order of knowledge, which grew in complexity as new copying and filing systems accelerated the production of files and letters. More efficient modes of information management were required.[588] In March 1901, two Home Office employees, Locke and Boehmer, devised an index card catalogue for the Home Office registry. They apparently spent several years deciding which older items were worth preserving as indexed 'precedents' and which were not. By 1908, Boehmer had presided over the categorisation of fifteen years' worth of arrears and had destroyed over twelve tons of correspondence and generated several new categories of governmental knowledge from stored papers formerly regarded as 'miscellaneous' matters. In 1909, the Home Office moved to larger premises, allowing the Registry to expand into its own dedicated room – it grew to employ thirty-five members of staff by 1911. It became the model for other government departments, whose staff regarded it with envy.[589]

Krajewski explains that index catalogues act as idiosyncratic information retrieval systems, coding information according to the functional aims of a particular office.[590] They install "formal representational structures", allowing discrete entries to be selected and combined in different ways. In the Home Office's first iteration of a card index system, approximately four thousand cards performed different operations.

[587] Vismann, *Files*, 138.

[588] Krajewski, *Paper Machines*, 101.

[589] Pellew, *Home Office: Clerks to Bureaucrats*, 101.

[590] Krajewski, *Paper Machines*, 52.

Some referred the user to entries in notebooks that contained instructions for performing different operations. Others, cross-referencing cards, drew connections between different categories of governmental knowledge. Some referred to specific files containing useful precedent materials that could be referred to in future.[591] Everything produced in the office required a reference number, which in turn provided an address for the storage of material within the office's own paper memory system.

4.4.3 Making connections

The coding of entries to a reference system was the precondition for developing connections and comparisons between cases. This in turn generated a new mode of visibility that was formed by making connections within the Home Office's registered memory system itself. This is demonstrated in the counter-espionage campaign conducted before the First World War. The 'Special Intelligence Bureau' was originally created within the Home Office to investigate German espionage in Britain.

In 1911, the Home Secretary Winston Churchill signed a general warrant authorising the opening of letters addressed to suspected spies in Britain. The bureau quickly generated an enormous amount of paper-based knowledge about suspected foreign national spies and their intermediaries. In 1921, a post-war report explained that the index card catalogue had created 1,189 separate entries on named individuals between 1911 and 1914.[592] By issuing one Home Office Warrant (HOW) in relation to a given suspect, the information returned from the Post Office regarding their correspondence generated new suspects and drew connections between them. Each subject was indexed individually and the entries were cross-referenced. The new entries, in turn, were made subjects of HOWs, and thus their mail was opened and checked and specially recruited policemen were sent to observe them. This in turn produced new

[591] Pellew, *Home Office: Clerks to Bureaucrats*, 106.

[592] Andrew, *The Defence of the Realm*, 37.

and previously undetected connections.[593] General warrants for wartime censorship enabled the system to carry on efficiently throughout the war years.[594]

Networks were diagrammatically described through the collection, collation, and crosschecking of communications, enabling counter-intelligence agents to proactively observe meetings, infiltrate networks, or arrange for the police to make arrests. Several spies were executed as a result. Authority was formally provided by issuing warrants,[595] each one generated by the connections discovered through previous warrants in a chain leading back to the general warrant. The point of the warrant was not to legally authorise interception, which was formally permitted by the general warrant anyway. Nor did warrants exist in this context to provide the Post Office with lists of targets, or express any formal decision made on the deliberations of the Secretary of State, as new targets arose from the data generated by interception operations in the Post Office in the first place. Rather, their function was to generate and authorise new files, and thus new individual entries in the registry, which constituted the principle elements upon which the entire intelligence system functioned. Warrants served to initiate files, and thereby coupled together records of different individuals across time and space, abstracting them into collections of intercepted material and other intelligence observations, while tying them to the symbolic coding of the indexing system that allowed them to be connected in diverse ways. The indexing of information served as the first-order recording process that enabled selective recall of stored information according to second-order observations of the connections they formed, materialised through the reflexive sorting of files.

The same principle served to reorient the operations of the English civil service in general. Past decisions provided authoritative instructions for future decisions, regardless of the circumstances and the particular civil servants involved. Precedent forms of action were connected with unfolding events, securing uniformity of

[593] On the potential creativity of cross-referencing, see Krajewski, *Paper Machines*, 63–67.

[594] See 'Censorship Warrants Which Should Be Revoked on Cessation of Hostilities in Europe HO 45/25973' 1946, National Archives.

[595] 'KV 1/48', 33, 36.

governmental policies over time. In relation to interception powers, when legal questions arose during the twentieth century as to the ambiguous status of warrants, reference was made to older legal advice and exemplary cases.[596] Moreover, policies of secrecy were implemented and maintained through recursive references to precedent practices. It is possible that, paradoxically, the relatively little material on interception that has survived and been disclosed to the National Archives was spared from total destruction only because it had precedent value for indicating when similar files should be eradicated rather than retained.[597]

4.4.4 Linking registries

If the indexing of the registry enabled internal connections to be drawn within the Home Office's paper memory machine across time, its capacity to absorb complexity also enabled connections to be made with the Office's external environment, in particular with commercial communication services. Once again, warrants provided a coupling mechanism.

In 1920, the President of Western Union publicly informed the US Senate that, despite censorship supposedly having ended in Britain, his company and others were required to pass copies of all international telegram traffic to British intelligence each day. In response, a new version of the Official Secrets Act entered force on 23rd December 1920. Section 4 stated:

> 4. Power to require the production of telegrams.
>
> (1) Where it appears to a Secretary of State that such a course is expedient in the public interest, he may, by warrant under his hand, require any person who owns or controls any telegraphic cable or wire, or any apparatus for wireless telegraphy, used for the sending or receipt of telegrams to or from any place out of the United Kingdom, to produce to him, or to any person named in the warrant, the originals and transcripts, either of all telegrams, or of telegrams of any specified class or description, or of telegrams sent from or addressed to any specified

[596] See 5.4.3.

[597] There is scope for a media-focused analysis of English law and administration, akin to Vismann, *Files*.

> person or place, sent or received to or from any place out of the United Kingdom by means of any such cable, wire, or apparatus, and all other papers relating to any such telegram as aforesaid.
>
> (2) Any person who, on being required to produce any such original or transcript or paper as aforesaid, refuses or neglects to do so shall be guilty of an offence under this Act….[598]

Secretaries of State had issued general warrants over foreign correspondence in times of war before, but the Act marked the first public statement of such a capacity. It also introduced a formal distinction between domestic and foreign communication in law. It is, technically, the first legislative grant of a positive power to intercept communication, albeit framed in relatively narrow terms.[599] It marked a break with a long-established practice of official secrecy, but given the publicity already generated by the President of Western Union, it was presumably calculated as a risk worth taking to prohibit any future disclosures. The Foreign Secretary, Lord Curzon, noted at the time, "it is important to leave this part of our activity in the deepest possible obscurity."[600]

As described in chapter three, the practice of so-called 'cable vetting' continued consistently from 1920 onwards. In 1967, when a whistle-blower revealed details of the practice, it was reported that authority was provided by warrants signed after the passage of the 1920 Act. As the first head of the Government Code & Cipher School recalled in 1944,

> The warrant clearly said scrutiny, and the traffic arrived back apparently untouched within a few hours. I have no doubt that the managers and senior officials must have guessed the true answer, but I have never heard of any indiscretions through all the years with so many people involved.[601]

[598] 'Official Secrets Act 1920', accessed 19 October 2016, http://www.legislation.gov.uk/ukpga/Geo5/10-11/75/contents.

[599] See 3.2.5 on international cable 'vetting'.

[600] Corera, *Intercept*, 96.

[601] Denniston, 'GC&CS Between the Wars'; cited in section 3.2.5.

In 1967, the then Home Secretary was apparently unaware of the existence of those warrants or the authority they conferred.[602] The warrants were apparently lost, yet their efficacy had not been diminished. As official secrets, they prevented the companies from having to explain or justify their collaboration. At that point, all that mattered was the recursive transfer of storage material for processing – first ink and paper telegram forms, later digitally encoded magnetic tape – which enacted the transposition of symbolic entries in one registry system into another.

The Official Secrets Act 1920 did not only address cable services. Section 5 addressed private postal systems that moved physical media, explicitly mobilising the interface capacity of registries. Section 5 required anyone in "the business of receiving for reward letters, telegrams, or other postal packets for delivery or forwarding" to register their business with the police and to keep and make available for police inspection records of the following particulars,

> (a) the name and address of every person for whom any postal packet is received, or who has requested that postal packets received may be delivered or forwarded to him;
>
> (b) any instructions that may have been received as to the delivery or forwarding of postal packets;
>
> (c) in the case of every postal packet received, the place from which the postal packet comes, and the date of posting (as shown by the post-mark) and the date of receipt, and the name and address of the sender if shown on the outside of the packet, and, in the case of a registered packet, the date and office of registration and the number of the registered packet;
>
> (d) in the case of every postal packet delivered, the date of delivery and the name and address of the person to whom it is delivered;
>
> (e) in the case of every postal packet forwarded, the name and address to which and the date on which it is forwarded.

[602] Corera, *Intercept*, 96.

These protocols became preconditions for all private delivery services. In 1925, a file was opened on a recently opened private mailbox and property registry company named Monomarks. It was marketed as a service for registering personal property, in order to "establish Identity, Ownership, Citizenship, the Law of Property and the Inalienable Rights of Man", according to a newspaper advertisement contained in the file. It also offered a document delivery and storage service, and in this capacity the company is still in business today. The concern arose from the fact that it operated in more than one country. While Monomarks' registry was located in London, if the company moved its files abroad to an office overseas, the registry would lie outside the jurisdiction and therefore section 5 of the Official Secrets Act would no longer apply to it.[603] A series of confidential letters exchanged with Monomarks eventually resolved the concern. From looking at the file, it seems likely that all private communication companies in the UK have been secretly required to open their registries for inspection for almost a century.

The critical point concerned the registry, and the ability to interface with it. In Vismann's phrase, registries act as "universal exchangers",[604] symbolically linking diverse discrete events. Items may already be delivered, but the particular connections that delivered items materialised could be reproduced from records of past transmissions. Private communication networks were thereby integrated into the apparatus of government. This practice is analogous to compelling Internet Service Providers to retain complete records of past communications metadata today.

4.5 Warrants and interception

Interception warrants in the twentieth century came to function in a number of different registers. For the Home Office, the police, and the intelligence agencies that had been created prior to and during the First World War, they served as reference points for ongoing and past intelligence operations. For the Post Office and companies who were addressed by warrants, they provided inputs that commanded what items

[603] See 'Monomarks: System of Identification: Instructions to the Commissioner's Office and the Position under the Official Secrets Act 1920 (1925 – 1978) MEPO 2/9582' 1978, National Archives.

[604] Vismann, *Files*, 82.

or categories of items were to be selected. As explained in chapter three, every communication medium defines its own parameters for interception, the privileged position from which all communications are potentially available for selection. But as this was in each case a technical question, it did not particularly affect the administrative form of the warrant, which functioned symbolically to reproduce authority rather than prescribe techniques.

The form of the warrant could adapt to any technical medium. For instance, the warrant copy shown in figure 5 simply requires the collection of "all letters, telegrams or other postal packets believed to come from Lawrence Jones", or other named targets, and those pertaining to anyone else at the listed addresses. For the Post Office, the warrant was a transfer medium containing selection data for target messages. The warrant transferred information required to make the 'conditional jumps' that discriminate between messages and channels, address data, locations, and so on: the information required to actualise interception as selections made against the horizon of traffic – which, as wartime censorship showed, could include total interception of all traffic. The warrant, once its elements are assembled so that it is recognisably materialised as a warrant, transferred information to be added to lists of active targets across different communication networks. The cancellation of a warrant removes an entry from the list. It takes effect as a simple conditional command actualised in interception techniques: *if* an item matches these terms, *then* select it for copying and distribution procedures. Archival examples of warrants pertaining to different technical media illustrate the point.

4.5.1 Radiotelegraphy

After the First World War, communication between Britain and the Soviet Union became a topic of concern for British intelligence, which was concerned with communist espionage. It was decided to intercept all "non-official telegrams" as an experiment, so as to see "what they amount to after a month". In March 1920, direct telegram communication with Moscow was only possible via radio as there was no cable link, and a radio-telegram service was provided by Marconi Wireless Telegraph Ltd on shortwave frequencies. Due to atmospheric interference, radiotelegrams could only reach Moscow from Britain during a window of around ninety minutes each day. However, a submarine cable connecting Peterhead in Scotland with Alexandrovsk in Russia was soon to be extended directly to Moscow, offering another source of intelligence.[605]

The Security Service, MI5, wanted to ensure that both media were targeted for interception. To this end the Post Office drafted an appropriately formatted warrant and sent the text to MI5 to formalise and sign. The draft and the final warrant are both relatively simple, but the exchange itself is interesting as it demonstrates the role of the Post Office in framing its own operations. The Post Office could ensure that the widest possible technical reach was granted, while still specifying a relatively narrow set of parameters, so that Post Office staff tasked with carrying out the interception would have clear unambiguous instructions. The Security Service, on the other hand, had the operational interest in the material collected, and could provide more granular lists of future intelligence targets once the flow of information was operational. The Security Service's task was to make the formal warrant and have the Secretary of State apply his signature to it. The warrant, eventually signed on 16th June 1920, ordered interception of all

> …telegrams which have been received or transmitted from or to those parts of Russia which are under the control of the Soviet Government or from or to any officers or agents of that Government. And for so doing this shall be your sufficient warrant. [606]

Intelligence expertise was contained within the Security Service, technical expertise in the Post Office. The only role for the Secretary of State was to assign a signature so that the connection between Security Service files and Post Office files could be linked via the correct protocological medium.

[605] 'Warrants Authorising the Production of Letters and Telegrams to and from Russia for Inspection HO 144/1684/400430' 1921, National Archives.

[606] Ibid.

4.5.2 Telephone warrants

Although the Home Office had had its own telephones since 1896,[607] telephone interception was conducted without warrants until May of 1937, when they were introduced as a matter of policy, as opposed to law.[608] As observed in chapter three, this coincided with the availability of portable magnetic recording equipment, which made telephone interception feasible as an investigatory device. Six months later, on 22nd November 1937, the Labour Member of Parliament for Nuneaton, Reginal Fletcher, raised the topic in Parliament. He asked the Home Secretary when the government's policy on telephone interception warrants had been established and what the practice had been beforehand.

In response, the Home Secretary consulted Vernon Kell, Director of the Security Service. The file contains a memo stating that there was no legal requirement to use any particular form of warrant for telephone tapping, but that some "authorisation" had always been sought from the Director-General of the Post Office.[609] A pencilled-in margin note says this information should not become public. According to a note from Kell,

> In May last it was decided that as an additional safeguard against a too free use of this procedure there should always be a written warrant under the hand of the Home Secretary.

By bringing telephone interception into the Home Office loop and indexing it to the production of warrants under the protocols applied to other modes of interception, the use of the technique would be regulated in case of over-zealous police activity led to it being publicly disclosed. Standardising warrants meant the practice itself would

> become standardised and this authority, if given, should always take the form of a warrant under the hand of the Secretary of State.[610]

[607] Pellew, *Home Office: Clerks to Bureaucrats*, 98.

[608] Birkett, 'Report of the Committee of Privy Councillors Appointed to Inquire into the Interception of Communications (the Birkett Report)', 1957, paras 40–52, http://www.fipr.org/rip/Birkett.htm.

[609] 'Warrants: Listening-in to and Recording of Telephone Conversations under Written Authority of Home Secretary HO 144/20619' 1937, National Archives.

[610] Ibid.

The idea was not that the Secretary of State should personally assess all applications but that the 'warrant under the hand of the Secretary of State' had come to symbolise a set of filing procedures and protocols that regulated the practice according to wider governmental priorities, not the least of which was maintaining secrecy. To be controlled and accounted for, activities had to be channelled through the prescribed steps.

A draft of the proposed telephone interception warrant form is contained in a carbon copy of a letter dated 1st May 1937 (figure 8), following legal advice of 14th April 1937 that had criticised an earlier draft, (figure 9). A pre-existing template for telegram warrants had been directly copied over, but it was deemed inappropriate to speak of "detaining" or "opening" phone calls. The phrase "imposing a check" had been suggested, but rejected as "too ambiguous". A note added 15th April 1937 suggests that time limits should be included to prevent the Post Office or police from having to indefinitely listen in to calls on the targeted line. Other than these semantic details, which were designed to avoid ambiguity when addressed to telephone engineers, the form itself remained the same.

4.5.3 Standardisation of interception warrants

General censorship warrants were implemented in both World Wars. In the Second World War, in addition to warrants covering postal packets and telegrams, separate warrants were produced for telephone lines. The Postmaster General was required

> to divulge to any person acting under the authority of the Secretary of State for Foreign Affairs, the Secretary of State for War, the Secretary of State for Air, the Lord Commissioners of the Admiralty and the Minister of Information any information which may be obtained from any telephone call, and to provide them with facilities to listen to any telephone call or on telephone line.[611]

However, as in the years prior to the First World War, general censorship powers were intended to identify potential spies or enemy sympathisers. Individually targeted warrants were required to investigate them further, so that each distinct target would

[611] 'Policy with Regard to the Interception of Private Lines by Telephone Units without HOWs 1941-1944 KV 4/445' 1944, National Archives.

be assigned an individual entry in the registry. This applied to postal and telegram communication but also to telephones. The centralised trunk network that enabled remote telephone tapping, discussed in chapter three, had not yet been created. Mobile Telephone Censorship Units were used to make general checks on any given local telephone exchange. Only in exceptional cases were the mobile units to be used to actively target individual lines for ongoing monitoring under the general warrant of 1940.[612] In this regime, if a suspected individual had more than one telephone line, there was to be a separate warrant for each, as "the check was imposed on the telephone number and not the individual concerned". This is counter-intuitive if one thinks of warrants as imposing the authority of the state upon human subjects, whose privacy is at stake, but if one considers instead that in the telephone network, connections are made between numbered lines and not between individuals, its intelligence value becomes clear. Warrants began to address themselves to communication systems rather than their human users.

Prompted by the increased level of interception activity, on 21st May 1942, a set of standardised procedural guidance notes was issued within MI5 regarding letter and telephone checks,[613] to bring all interception warrants together into a carefully prescribed protocol (see figures 10-15). Pre-formatted slips and cards were printed with their own identifying catalogue numbers. Detailed protocols were included; one listing the procedure to be followed when applying for postal or telegram warrants, another in relation to telephone warrants. Samples of how to correctly complete the basic pre-printed forms were also included, including both warrants and warrant cancellation forms. The circular is instructive also as to the complexity of the internal communication networks based on registry references and filing techniques. Marked as a circular, the copy of the covering letter addresses itself to "All Officers" within certain coded categories. In the first paragraph, it states that "all previous circulars on this subject are cancelled", thereby indicating the supremacy of the new protocols over the old.

[612] Ibid.

[613] 'Policy and Procedure for the Imposition of Home Office Warrants for the Interception of Mail and Telephone Communications in the UK 1939-1945 KV 4/222' 1944, National Archives.

Pre-printed forms produce standardised feedback so that any of the intelligence analysts receiving data, regardless of their prior knowledge of the file, can immediately see all relevant information in a single location (see figure 16). Forms have agency, they prompt action. In order to complete the form, all the administrative and legal requirements pertaining to the execution of the warrant must be correctly entered, processed, and thus recorded for the future in the pre-printed blank spaces.[614] The form establishes and elaborates the correct procedure to be used when storing intercepted data, to format it in advance of processing. Henceforth the warrant is no longer just making a command, or unifying two entries in two different registries. It is also prompting further action from its addressee beyond the bare command to intercept communication. It demands feedback from its addressee in a standardised, coded manner that bring uniformity across files.

Ultimately, a 'warrant' is compiled of the protocols and connections that are unfolded in the process of issuing it. When it takes effect, it always refers back to governmental authority. It allows governmental power to appear as an effect of all the operations that are organised around it. The 'textocracy' of government is an effect of the processes that go into making the symbolic products of government, which in turn take effect by commanding the execution of other technical operations elsewhere – in sorting rooms or telegraph offices, for example. Hence the form of the warrant is flexible, as they can be programmed in different ways. Warrants are capable of symbolising diverse worlds, technologies, and subjects. It articulates connections between such operations by referring them back to its symbolic authority.[615] The warrant is the switch point at which diverse circuits of technical knowledge and governmental practices meet.

Public knowledge of the state's capacity to carry out secret surveillance on the population meant that secret files came to be regarded as a dangerous and repressive

[614] Vismann, *Files*, 128.

[615] The word 'textocracy' is borrowed from Krajewski, *World Projects*, 186.

resource, with which citizens' personal lives could be monitored and assessed without any democratic oversight. In the second half of the twentieth century,

> … files have been the medium instrumentally involved in the differentiation processes that pit state against society and administration against citizenry. The state compiles records, society demands their disclosure.[616]

In relation to interception power, the production of warrants and information erupted as a topic of public concern following a scandal about telephone tapping in 1957.[617]

4.5.4 Procedural norms

In 1957, a group of Privy Councillors (i.e. retired ministers of state sworn to secrecy and loyalty to the Queen) led by Sir Norman Birkett were appointed to investigate and publicly report on the legality and procedures of telephone interception. The legality of telephone tapping was confirmed, albeit in carefully chosen and somewhat ambiguous terms (the legal analysis is discussed in greater detail in chapter six).

Administratively, the report confirmed that the Home Secretary acted as the authority that authorises applications for interception warrants. Applications to the Home Secretary were made by other agencies, indicating that investigative work was completely differentiated from the operations of the Home Office. Fourteen different agencies had been granted interception warrants between 1937 and 1956, although most applications came from just three agencies: the police, customs, and MI5. Apparently not all agencies had adopted the uniform protocols circulated by MI5 during the war, each used their own internal application procedures for seeking Home Office warrants. At paragraph 78, the report states:

> … the keeping of full and accurate records is a necessary part of any procedure to ensure that the use to which interception may be put is effectively controlled. The Home Office records of warrants issued for the detection of crime are reasonably full. Each case is separately recorded in

[616] Vismann, *Files*, 147.

[617] Fitzgerald and Leopold, *Stranger on the Line*, 116–17.

> a file. These all contain the ground on which the warrant was issued, a copy of the warrant itself and the date of its cancellation.[618]

The report recommended standardising applications across all agencies in order to implement firm procedural norms. It recommended that individual warrants should always be sought for individual targets. Some existing warrants contained long lists of named targets on the same warrant. Few warrant applications contained any reason for interception, thus failing to justify the intrusion into privacy that would follow. And as there were no records of any refused applications, it was apparent that the Home Office did not give any consideration to the normative question of which applications could be justifiably granted and which could not. The records gave the Privy Councillors the impression that applications were always granted regardless of the circumstances. The report recommended reasons for applications be included, and a record of all refusals maintained. Furthermore, it stated, time limits should be built into every new warrant so that their validity would automatically lapse unless positively renewed by further application.[619] Responsibility for making cancellation and renewal requests to the Home Office should always rest with the agency concerned.

Long-term filing practices were deemed inadequate; many internal documents had been disposed of, making any detailed audit impossible.

> Until 1947 the Home Office kept a card index of names and addresses showing alphabetically by name and geographically by area all the warrants issued for security purposes. In 1947, at the suggestion of the Security Service, which was disturbed by the existence of these records in the Home Office, all of them were destroyed and no complete records

[618] Birkett, 'Birkett Report', para. 78.

[619] The problem of cancellation of warrants has been mentioned in relation to eighteenth century practices, above. Cancellation was an ongoing concern throughout the early twentieth century too. See 'Indecent Wares from Abroad: Warrants for the Detention of Illegal Postal Packets (1911-1923) HO 144/1837' 1923, National Archives; cf. 'HO 45/25956'; 'Constitutional Authority to Stop Letters in the Post HO 45/25962' 1935, National Archives; 'Precedents in Common Law for Opening Letters in the Post HO 45/25961' 1935, National Archives.

> were kept thereafter except for the serial numbers of the warrants issued.[620]

This implies that the Security Service (MI5) maintained its own card index. Only the Home Office was to destroy theirs, which from a security perspective represented an unnecessarily risky redundancy. The Home Office was simply processing and granting warrant applications without any means of assessing the assessments that lay behind applications. Since 1954, records of the minutes on each file had been kept by the Home Office, but they gave only a brief account of the reason for each warrant. Meanwhile,

> The Metropolitan Police destroyed all warrants between 1937 and 1946 upon their cancellation, and the same practice was followed from 1946 – 1953, except that a bare record was kept of the number of interceptions authorised by the Secretary of State. Detailed records exist only from 1953. The Security Service also destroyed detailed records before 1952 although it kept figures of the numbers of warrants issued. It was not possible to discover the exact number of interceptions in earlier years, but only the number of warrants issued; the discrepancy between these two figures would, however, be very small indeed.[621]

Since the Privy Councillors began their inquiry, the report notes, the Home Office had implemented a new protocol for making and retaining records. In every application, the following points should be noted, in one place:

> (a) The ground on which the warrant is applied for,
>
> (b) A note of any subsequent decisions concerning the warrant.
>
> (c) A copy of the warrant issued or, alternatively, a note that the application has been rejected.
>
> (d) A record of the date of the cancellation of the warrant and the reason therefore.[622]

[620] Birkett, 'Birkett Report', para. 80.

[621] Ibid., 81.

[622] Ibid., para. 84.

This data would be collated and transformed into statistics, and the statistical figures would then be made subject to *post facto* monthly reviews.[623] All of this, however, would be done secretly, particularly where Security Service tapping was concerned. Reviews should remain within the administrative chambers of government:

> We are strongly of the opinion that it would be wrong for figures to be disclosed by the Secretary of State at regular or irregular intervals in the future. It would greatly aid the operation of agencies hostile to the State if they were able to estimate even approximately the extent of the interception of communications for security purposes.[624]

The Birkett Report marked the first time that the procedures for making interception warrants had been observed from outside the Home Office and interception agencies since 1844. Whereas the Secret Committee made some general suggestions on procedure, the Birkett Report demanded them in stronger terms, and the government publicly approved of the suggestions.

What mattered, in media-technical terms, was that protocols and procedures be implemented so that the normative considerations demanded by abstract values were integrated into, and evidenced by, the filing processes that generated warrants and processed their effects. The Home Office was to ensure that senior officials independently recorded and reviewed each application, so that while the agencies – police, Security Service, customs, and so on – used their index systems for intelligence and investigation, the Home Office would retain a copy of their applications and perform reviews over its own master-index of applications, including any refused applications, in order to supply a second-order normative review. This way, normative standards could be superimposed on technical standards, and the application of technical standards could become a medium for normative self-assurance. Provided the new procedures were implemented and followed strictly, whatever warrants resulted – and whatever information the files processed – would in advance be normatively acceptable, and would remain so provided the ongoing

[623] Ibid., para. 74.

[624] Ibid., para. 121.

files were properly handled, cancelled, and correctly stored (and not destroyed) for *post facto* review. In short, files had to be made according to new procedures, and the implementation of those procedures in turn had to be evidenced in the file. Whereas the making of medieval writs had involved a fictionalised chain of *ex ante* authority culminating in the King, the making of modern warrants became subject to a chain of *post facto* reviews, ultimately reporting statistics back to the ministerial offices of the Secretaries of State. They thus occupied two positions in a symbolic circuit, acting both as the authorisers and the auditors of interception.

Although no samples of warrants post-dating 1957 are publicly available, the recommendations of the Birkett report were apparently put in place and operationalised throughout all the government agencies concerned with interception, as evidenced by a report obtained under the Freedom of Information Act 2000 in the course of this research.[625] The report was prepared by a Working Party of the Home Office established in 1979 to prepare for the possible requirement to draft legislation concerning interception powers. It refers frequently to the "Birkett arrangements", which all the agencies concerned confirmed had been rigorously complied with within their bureaucracies since 1957. These procedures, in turn, were felt to guarantee the propriety of interception and ensured that it was only used where warranted by the Secretary of State.

4.6 Conclusion

This chapter has demonstrated that the Secretary of State's authority to direct interception has always been a consequence, not a source, of the making of warrants. The Secretary's ongoing power is an effect of the ongoing operations that give the Secretary's position its appearance of timeless continuity. Warrants express the symbolic authority to define operations, and thereby reproduce the notion that "only the subject can carry out actions and rule over things."[626] Communication media define the course of action that results in the interception of information, warrants

[625] The Working Party report is discussed further in the next chapter, see 5.4.5; 'Interception of Postal and Telephone Communications: Interception Working Party Correspondence' HO 325/536' 1979, National Archives.

[626] Vismann, 'Cultural Techniques and Sovereignty', 84.

attribute those results to the will of the Secretary of State. Yet the Secretary of State is today neither the source of decisions to intercept communication nor the one who determines the lawfulness of the process. The techniques of warrant making, which were always drafted by under-secretaries and merely brought before the Secretary to sign, link the body of the office-holder to the authority that the warrant ascribes to them. They have always been products of particular procedural rules, which must be obeyed in order to reproduce authority in a recognised form.[627]

The Birkett arrangements transformed procedures for making warrants into normative prescriptions. To make a warrant, one had to follow the new procedures, and this way one would be assured of making a document that respected civil liberties, privacy, and so on. Yet such arrangements could not rectify the fundamental split that the creation and processing of files and warrants had come to symbolise between state and society, in Vismann's formulation.[628] They sustained the split. The Birkett arrangements were the latest edition in a line of administrative recipes and formulations that resulted in files, and thus they simply reproduced the existing symbolic authority of the state and its offices, now reconfigured to function as auditors of their own decisions.

Interception warrants were administered in secret and they excluded the law. Appeals to the law – meaning courts, judges, and open hearings – were impossible in relation to interception powers, until a surprising event in 1978 forced the issue.

[627] Ibid., 88.

[628] Vismann, *Files*, 147.

5. Secrecy and Surprises

5.1 The law of interception warrants

In this chapter, the implementation and function of legislation about interception powers is analysed. First, the chapter examines the judicial decision that preceded the creation of legislation. The suggestion is that the problem to be solved was not simply the need to give interception a legal footing, but to manage the publicity that law depends on. Legislation, rather than representing the subjection of political power to law, is better understood as a technique of media-management.

5.1.1 The warrant before the law

In January 1979, an interception warrant appeared on the bench of the High Court in London, presided over by the Vice-Chancellor of the Rolls, and Privy Councillor, Robert Megarry. Journalists Patrick Fitzgerald and Mark Leopold described the scene.

> The Solicitor General, Peter Archer, arranged for a copy of the warrant to be brought to court where it lay, like some sacred scroll, untouched upon Megarry's bench inside a sealed envelope.[629]

The interception warrant came before the law unexpectedly. In the summer of 1978, a London antiques dealer named James Malone was one of five defendants tried in the Crown Court for offences connected with handling stolen property. He was acquitted on some counts and the jury failed to agree a verdict on others. At a retrial in 1979 he was fully acquitted. On 18th July 1978, during the first trial, a notebook belonging to the lead investigator in the case was entered in evidence. It happened to contain details of a 1977 conversation between Malone and a co-defendant, with a note indicating that it was obtained by 'tapping' Malone's telephone line. Counsel for the prosecution admitted,

> In the circumstances I am authorised to say that there was such an interception carried out on the authority of the Secretary of State's warrant.[630]

[629] Fitzgerald and Leopold, *Stranger on the Line*, 135.

[630] *Malone v Metropolitan Police Commissioner* [1979] 344 Chancery Division, 349.

Malone wrote to the Post Office directly regarding the line tap. Apparently, a senior executive wrote back and confirmed the tap had been removed.[631] Malone issued a writ against the police on 17th October 1978, seeking an injunction against further line-taps, delivery of copies of all intercepted information and destruction of any in police custody, and damages. He also sought a subpoena against the Post Office requiring they produce the warrant in court, which is how it came to be before Megarry.

The warrant required an explanation from the court. The problem facing Megarry was that there was none readily available. This was an unusual situation in relation to a purportedly legal instrument that had, for three centuries, assigned to Secretaries of State the power to direct and determine the interception of communication. By 1979, the symbolic authority assigned to the Secretary of State by interception warrants referred to highly complex operations of information transfer, constantly flowing between the public and private interceptors of various forms of postal and technical media on the one hand, and the consumers and processors of intelligence on the other. The warrant also functioned to exclude, by omission, everyone else from accessing the privileged position in which interception operations are performed. It reserved access to those from whom the warrant demanded execution.

However, the law operates according to a different set of programs and protocols. In all the stores of textual decisions and statutory rules that were then available as resources, the law lacked a text that clearly assigned to the telephone interception warrant a definite position within the legal system. This was not in itself an insurmountable problem. The common law is a textual production machine, its resources are old texts that it turns into new texts. The cultural-technical skills required to operate texts of the common law are flexible. As Murphy puts it, the specific genius of common law lies in "the mobilization of virtual orders, and a realism of the 'as if'".[632] Common law is non-epistemological and non-empirical. There is no dogma as to how material objects must be constructed. Law selects its facts in each case. It is

[631] Fitzgerald and Leopold, *Stranger on the Line*, 133–34.

[632] Murphy, *The Oldest Social Science?* 113.

> a science of the hypothetical – but not the experimental hypothesis. It is a paradoxical knowledge of the 'what if?', or society understood and characterized through its pathology (as that pathology appears in the courtroom), a science of imagined possibilities which is simultaneously the basis for the elaboration of a range of techniques for avoiding in advance the possibility of a pathology, pathology being defined as the need to go to court.[633]

The telephone interception warrant presented one such pathology. To remedy it, a new decision had to be written that would account for the existence of the warrant and ascribe it a settled position within the law. If a place could not be found for the warrant, then it would have to be declared illegal.

5.1.2 The danger of judgment

The problem, however, was not in making a decision that would make the warrant legal, but the potential consequences of doing so. Law functions by making analogies. If the decision were to bring the informational content of the warrant into legal discourse and assign it a position, it would mean bringing the content of all past, present, and future interception warrants into legal discourse. Whatever decision was arrived at, if it engaged with the content of the warrant, then future cases could do so too. This is an unavoidable consequence of the techniques of the common law, which mobilises texts to recombine and develop them analogically in a "continuing consolidation of a perpetual present which was somehow out of time."[634] Rather than being determined by the past, each decision must reconstruct the present, but with an eye on the future. The future is what always remains changeable. A judicial decision must look forwards as it mobilises the past. Judgment "cannot be determined by the past but attempts to treat the future differently".[635]

The operational function of the content of the warrant was, as we have seen, to provide interceptors targets that are added to lists. The targets varied with each warrant while the general symbolic form that linked authority to execution remained the same. The

[633] Ibid., 118.

[634] Ibid., 89.

[635] Luhmann, *Law as a Social System*, 283.

lists mattered because they directed the application of interception techniques that were, by definition, state secrets. State secrets are not the same as religious mysteries or mystical powers, they are technical operations that are understood according to a political logic of time that addresses itself to the future. To open the envelope and discuss the legality of its content would mean bringing the conditions of listing targets directly into the legal order, which would, in turn, damage the state by reducing the effectiveness of the techniques in the future. If the targeting of individuals, organisations, or communication channels were made subject to law, then they would be made subject to legal protocols that would, in turn, have to be legally reviewed. Hypothetically, everyone who even suspected their name might appear on such a warranted list could go to the law and demand an account.

On the other hand, to simply declare the warrant illegal would be worse. That would be to declare that its symbolic attribution of legal authority to the Secretary of State, and to the actions of interceptors, was also illegal and always had been. By analogy, every other telephone interception warrant would, potentially, be made illegal. It would, to put it mildly, trigger a crisis. At the very least, it would require Parliament to urgently pass interception legislation in order to create a legal position for the interception warrant. That would generate even greater attention, causing political embarrassment as well as tactical problems for the agencies that depended on intercepted data.

Moreover, in his position as a judge, Megarry could not simply refuse to decide. The only true imperative he faced was that he had to produce a decision. Courts can rule one way or the other on the issues before them, but they cannot abdicate the duty to decide. If they did, the law would come to a halt. Luhmann calls this the "prohibition of the denial of justice."

> Courts have to decide even when they cannot decide… And if they cannot decide, they must force themselves to be able to decide. If the law cannot be found, it must simply be invented… the decision must be translated into

> distinctions which can be managed, for example the distinction between decision and consequence or between legal principle and its application.[636]

The translation of a decision into the distinction between principle and application is precisely the course that Megarry took.

5.1.3 Materialising political secrecy

We can more clearly delineate the delicate status of the warrant as it sat on the bench by reference to terms drawn from political history. As an administrative device, the warrant appears as an *arcanum* of state. A political *arcanum* (from *arca*, meaning treasury, coffin, or chest) refers to an essential tool of political security that is wielded by the state to maintain its own security. The definition includes any technique of state power that is based on "silence and concealment" or any information that is "locked away and hidden". Modern *arcana* are mundane techniques typically identified by their formal classification as official secrets. Formal classification of the *arcana*, in turn, is a technique of political time management. To remain silent about the *arcana* is to maintain their effectiveness. Silence about the use of interception warrants stabilises the environment in which they take effect, this way, the warrant remains an effective option for future use, keeping secure the status quo.[637] In other words, *arcana* are techniques that must be kept out of the mass media, such as newspapers, television, and broadcast radio.

In a different register, the English word 'secret' is etymologically derived from the Latin verbal participle *secretus*, which refers to a thing having been separated. A *secretum* refers to a thing that has been separated from something else. In this sense, the 'secret' indicates a structural distinction in relation to a given piece of information. The secret is constituted by the difference between access (inclusion) and restriction (exclusion). The form of the 'secret' describes the unity of the difference between those in the know and those in the dark. Borrowing from Derrida, Eva Horn observes that this relationship of inclusion and exclusion is generative of a 'secrecy effect' produced

[636] Ibid., 289.

[637] Horn, 'Political Secrecy', 108.

whenever withheld information is known to exist.[638] The *arcana*, if properly managed, generate only silence. An *arcanum* of state should never enter into discussion at all, beyond the small circle constituted by those who 'need to know'. The secrecy-effect, on the other hand, generates an over-abundance of communication. Horn compares it to Foucault's observation that in modern society, supposedly 'repressed' sexuality is discussed endlessly. Similarly, the effect of the secrecy-relationship is that everyone talks about secrets.[639]

The story of the warrant sitting on the bench was formally recorded only by journalists. Its presence in the courtroom is not mentioned at all in the judgment, which refers only to the application for a subpoena. This is not surprising, as the biggest consumers of secrets are the mass media. This shall be discussed further below. For now, we return to the courtroom.

5.2 Re-programming the problem

One does not necessarily construct the components of a judgment in the order that is suggested by the final draft of the text. Like a mystery novel, or a thesis, it may be easier to work out the ending and work backwards. Megarry, who as a Privy Councillor had formal duties to the state that were equal if not superior to his duties to the law, had to arrive at a final judgment that would both legitimise the warrant in the symbolic order of law and simultaneously avoid saying anything about it that might require him to open the envelope as a consequence. The task was to include the warrant symbolically within the law by excluding it from any direct discussion. Its presence in the courtroom had to be dealt with by using the law to make it legally absent from the discussion.

There were two possible arguments for excluding the warrant presented to Megarry. One came from the police, who were represented in the court because they had been named as the defendants by Malone's writ. The other argument came from the Solicitor-General, who was there to represent the Secretary of State for the Home

[638] Ibid., 109.

[639] Ibid., 105.

Office. The Home Secretary, a fellow Privy Councillor, had 'intervened' in the case on Megarry's invitation. It was, after all, his authority on the line.

The Solicitor-General invited the judge to find that the common law would not open the envelope and reveal the warrant's contents for "reasons of public safety". This option was not unprecedented in the common law, and therefore was a valid response open to the court. Only two years earlier, in the case of *Hosenball*, before the Court of Appeal, Lord Denning had said,

> When the public interest requires that information be kept confidential, it may outweigh even the public interest in the administration of justice.[640]

But the police's lawyer made a more elegant suggestion, which Megarry ultimately adopted in his judgment. Focusing on the part of Malone's writ that sought an immediate interlocutory (i.e., interim) injunction against the police to ban them from further telephone-tapping, Megarry cited the case of *American Cyanamid Co.* v *Ethicon Ltd.* [1975] A.C. 396, 407, a commercial case that dealt with the question of the correct legal procedure to follow when dealing with applications for injunctions.

American Cynamid provides a procedural rule for the common law: that an interlocutory injunction should only be granted if the illegality of the alleged action is already settled in law, so that only the facts are to be determined during a full trial of the action. Such an interlocutory injunction should not be granted in cases where the legality of the alleged facts is unclear, because if, after a full trial has been adjudicated, the assumed legal basis for the injunction turns out to have been incorrect, then the defendant who was subjected to that injunction has suffered unnecessarily during the period of the trial. Conversely, if an injunction is refused and the legal argument later shown to be correct, then the plaintiff has to suffer the ongoing activity until the law has been clarified. Between these two options, the court in *American Cynamid* decided

[640] *R v Secretary of State for Home Affairs ex p. Hosenball* [1977] 1 WLR 766; Mark Hosenball, an American journalist, was facing deportation from the UK for his part in writing a story about GCHQ's existence and operations. His co-authors were tried under the Official Secrets Act in the so-called 'ABC Trial'. Hosenball was simply deported; see also, 'ABC Case', accessed 8 June 2017, http://www.duncancampbell.org/content/abc-case.

that the law will only intervene in the world by issuing an injunctive writ once the legal basis for doing so is clear. Where the law is unclear, the hypothetical 'status quo' is to be maintained by non-intervention.

Using the cultural technique of legal analogy, Megarry applied this line of conditional programming to the case before him. He held that it would be "inappropriate" to alter the situation by issuing an interlocutory injunction against the police without first allowing for "detailed argument and mature consideration" in respect of the underlying legal issue. As the judgment explains,

> The upshot was that on Day 2, by consent, the motion was transformed. It was agreed that the motion should be treated as the trial of the action and heard on the existing affidavit evidence, without more. The statement of claim was heavily amended in relation to the relief sought. All claims to any injunction, order for delivery up, order for destruction and damages were deleted. Further, all allegations that there had been a conspiracy between the Post Office employees and police officers (for which the defendant was liable under section 48 of the Police Act 1964) were withdrawn; and no allegations of criminal conduct were made. In lieu of the relief sought by the statement of claim, various declarations were claimed, relating to the legality of telephone tapping; and these were substituted for the relief sought by the notice of motion.[641]

Rather than seeking disclosure and damages on the basis of unlawful behaviour, Megarry 'deleted' the material facts from the case before him and 'substituted' in 'various declarations' instead. He responded to an impossible set of imperatives by side-stepping them, and thus eliminated the need to address in any way the empirical status of the sealed document before him. By this protocological recoding of the matter, the trial was transformed to a simple hypothetical question, which Megarry phrased as, "Is telephone tapping in aid of the police in their functions relating to crime illegal?"[642]

[641] *Malone v MPC* [1979] 344 Ch., 350.

[642] Ibid., 355.

5.2.1 Assembling a judgment

Once the materiality of the specific warrant was out of the way, the path was clear to assembling an abstract account of its status in the law. After two days of preliminary argument on the warrant, Megarry formally dismissed the subpoena application as irrelevant, handed the sealed envelope back to the envoy from the Post Office, and sent him on his way. Once the material presence of the warrant had been removed from the court, it could be dealt with solely by reference to the legal meaning of its long-standing symbolic effects. In short, did the abstract office-holder of the Secretary of State have in law the power that the warrant ascribed to him?

The judgment began by considering the possible laws that telephone interception may have violated. First, Megarry found no general right to privacy in the common law. Although Malone's counsel presented analogies in the common law that could, when taken "together with the requirements of justice and common sense", amount to the finding of a right of privacy, Megarry decided this was too much to ask of a court as it would have political consequences far beyond the immediate facts of the case. Whereas he avoided assigning a political boundary to legal decisions in relation to political secrecy, he was happy to inscribe a political limitation around more comfortable topics like the notion of privacy. Ultimately, he said, "it is no function of the courts to legislate in a new field."[643] Telephone tapping was clearly an invasion of privacy in fact, but invading privacy was not legally forbidden by the common law.

Turning to the jurisprudence of the European Court of Human Rights, Megarry agreed that it was "impossible to see how English law could be said to satisfy the requirements of the Convention" in relation to interception of communication, which demanded some legislative basis for the practice. The law had to give positive assurances that it would only be used 'proportionately' and according to 'necessity' in a democratic society, and supply a right of recourse in case the law was breached.

[643] Ibid., 372.

However, as the Convention was not justiciable in English law in 1979, it had no validity and was thus irrelevant to the determination of the case.[644]

Megarry next identified two sources for a duty of confidentiality in English law. The first was contractual confidentiality, but that was eliminated because Post Office legislation explicitly stated that the relationship between the Post Office and subscribers was non-contractual.[645] The other was the equitable duty of confidentiality, but this could be found only in certain situations involving the abuse or unauthorised disclosure of sensitive information. For a court to find such a duty depended first on the particular quality of the confidential information in each case, second on a finding that there was expectation of confidentiality when the information was imparted, and finally on some measure of harm done by the disclosure. As these fact-dependent criteria could not apply generally to the relationship between the Post Office and all telephone subscribers, it could not apply to the abstract question of the general legality of telephone tapping. On the contrary, Megarry held:

> When this is applied to telephone conversations, it appears to me that the speaker is taking such risks of being overheard as are inherent in the system […] so much publicity in recent years has been given to instances (real or fictional) of the deliberate tapping of telephones that it is difficult to envisage telephone users who are genuinely unaware of this possibility.[646]

In other words, users of the Post Office telephone network should presuppose that their calls were anything but confidential. He went on to state that even if telephone tapping in aid of the police did constitute a breach of confidentiality in the case of police interception, the countervailing public interest in the prevention and detection of crime would justify the breach.[647]

Having concluded this review, Megarry found that there was nothing to outlaw telephone tapping in English law. It was not illegal because nothing forbade it. What,

[644] Ibid., 380.

[645] Ibid., 375.

[646] Ibid., 376.

[647] Ibid., 378.

then, was the purpose of a warrant? On Megarry's reading, interception warrants are simply administrative tools for delegating orders, but they neither recognise or generate any legal authority. Statutory rules that prohibited the interception of posted letters and telegrams without a warrant existed, but they simply criminalised unwarranted interception. That alone did not assign any positive authority to the Secretary of State. Warrants simply frame orders in a form that immunises Post Office staff, and nothing more.[648]

In respect of telephones, however, there was no reference whatsoever to warrants in any legislation. The only analogous rule was found at section 80 of the Post Office Act 1969. It stated that Post Office staff could be made subject to 'requirements' compelling them to inform 'officials of the Crown' of any matters 'transmitted' by telephone. These 'requirements' were undefined. Megarry concluded simply that,

> A warrant was not needed to make the tapping lawful: it was lawful without any warrant. But where the tapping was done under warrant (and that is the only matter before me) the section afforded statutory recognition of the lawfulness of the tapping.[649]

Having found that there was nothing in English law to make telephone tapping illegal, Megarry ruled that it therefore

> requires no authorisation by statute or common law; it can lawfully be done simply because there is nothing to make it unlawful.[650]

By implication, the law does not require governmental power to have a specific legally defined source. This is a controversial finding, summed up by Megarry's infamous quip:

> England, it may be said, is not a country where everything is forbidden except what is expressly permitted: it is a country where everything is permitted except what is expressly forbidden.[651]

[648] *Malone v MPC* [1979] 344 Ch., 370

[649] ibid.

[650] Ibid., 381.

[651] Ibid., 357.

Here, the analogical nature of the common law worked against him. The judgment served up the desired result: telephone interception was not illegal, and the existing warrants regime could lawfully continue. However, once the logical steps taken in order to arrive at this result are analogised, they imply that there is no legal difference between a person acting as a private citizen and a person acting as a public official. Like anyone else, then, government officials are free in law to do anything that is not otherwise illegal. This particular finding is considered so controversial by English public lawyers that it is now the main reason that the case is remembered, often viewed as a bad decision.[652]

There are hints that suggest Megarry realised the controversy that would follow. Towards the end of the judgment he states that the topic of interception "cries out for legislation",[653] and emphasises that his decision is confined narrowly to the specific question of facilitating telephone tapping by the police where they have "just cause" for the request.[654] It is hard to resist the impression of Pontius Pilate, as Megarry distances himself from the bigger picture. On this reading, the judgment appears as a placeholder, a temporary fix to an unpredictable and unlikely situation. It enabled interception to continue for the immediate future, while the government formulated the legislation that would inevitably be required once Malone had taken the country to the European Court of Human Rights in Strasbourg. Malone did go to Strasbourg, which moved slowly at the time. Six years later, for reasons that Megarry himself had identified, he won.[655]

[652] Adam Tomkins, 'The Authority of Entick v Carrington', in ***Entick v Carrington: 250 Years of the Rule of Law***, ed. Adam Tomkins and Paul Scott (Oxford: Hart Publishing, 2015), 183; Keith Ewing and Conor Gearty, ***The Struggle for Civil Liberties: Political Freedom and the Rule of Law in Britain, 1914-1945*** (Oxford: Oxford University Press, 2001), 14.

[653] ***Malone v MPC*** [1979] 344 Ch., 380.

[654] Ibid., 384.

[655] As we shall see, the outcome was fully anticipated by the British government, see ***Malone v. The United Kingdom*** [1985] ECHR 5.

5.2.2 The symbolic meaning of authority

Megarry's ruling remains troubling to some constitutional theorists who deal with English law because it has implications for the meaning of the 'rule of law' in relation to governmental power generally.[656] The debate has recently been framed via two alternative readings of the 1765 case of *Entick v Carrington*, which since the late nineteenth century has been mobilised as a common law resource for legally constraining executive political decisions where they infringe upon civil liberties.

In *Entick v Carrington*, the Secretary of State issued general warrants ordering the King's Messengers to search for and seize any papers belonging to anyone suspected of involvement in the printing of seditious libel. The warrants were 'general' in that they named only the crime, not the suspects, and provided no peremptory reason for targeting them. Anyone suspected by the Messengers was rounded up and their homes searched for papers. As we saw in chapter four, Hale had previously written about the legal requirements for Justices of the Peace to issue search warrants; he explicitly stated general warrants were illegal.[657]

Lord Camden, the presiding judge in *Entick v Carrington*, found that there was no legal source of authority in common law or statute for a Secretary of State to issue general search warrants. It could not be justified by the royal prerogative because committing trespass was a legal wrong, and under the prerogative the King could do no wrong. Rather, he found the general warrants illegal, having no authority whatsoever. In an often-cited maxim, the judgment says: "If it is law it will be found in our books. If it is not to be found there it is not law." The Messengers and their superior officers were trespassing when they broke into and searched private premises, and as the general warrant had no authority in law it could not excuse them. Damages were awarded accordingly.

[656] Note that this particular debate does not exhaust the concept of rule of law, see Martin Loughlin, ***Sword and Scales: An Examination of the Relationship Between Law and Politics*** (Oxford: Hart, 2000), 65–75.

[657] See 4.2.3.

Recent interpretations of the case's significance argue that *Entick v Carrington* is authority for the proposition that no public authority can do anything unless they can point to a positive legal authorisation to do it. A positive legal basis must be found in at least one of three possible sources: the royal prerogative, common law precedents, or legislation. Otherwise, any exercise of governmental power is unlawful, regardless of its consequences.[658] This broad interpretation assumes, a priori, a difference between public and private subjects. Private subjects are free to do anything except what is explicitly prohibited. But public subjects occupy public personae, and in that capacity exercise powers that are defined by their office – powers which private citizens do not have. Public powers must be rooted in positive law. Law is positioned as the only legitimate medium of political power.[659]

Alternatively, *Entick v Carrington* simply means that no one can infringe on the legally protected rights of anyone else unless they have some positive lawful authority to do so. The consequence of this older understanding of the case is that everyone is free to exercise their powers and capacities as they see fit, so long as no one else's rights are infringed. This implies a negative conception of freedom that applies equally to public and private subjects. On this view, there is nothing inherently special about governmental actions. The critical issue in *Entick v Carrington* was that the Messengers had trespassed on private property without lawful authority. Consequences arose not from the absence of a power to make warrants, but from the absence of a justification for the trespass.[660] This reading underpins long-standing criticism of the common law as a resource for protecting human rights. Relying only on common law, as advocated by some opponents of human rights legislation, leaves rights open to abuse in any situations where they do not coincide with conservative property rights, such as the tort of trespass.[661]

[658] This is the view of Tomkins, 'The Authority of Entick v Carrington', 164.

[659] Ibid., 161–84.

[660] See Timothy Endicott, 'Was Entick v Carrington a Landmark?', in ***Entick v Carrington: 250 Years of the Rule of Law***, ed. Adam Tomkins and Paul Scott (Oxford: Hart Publishing, 2015), 109–30.

[661] Ewing and Gearty, ***The Struggle for Civil Liberties***, 14.

In the *Malone* case, Megarry was presented with the argument that the Secretary of State required some positive legal basis on which to make interception warrants. He therefore had to explicitly favour the narrow reading of *Entick v Carrington* and differentiate the cases from one another in the factual domain.[662] Hence, whereas Entick had suffered trespass in his home, the technical interception of phone calls by the Post Office 'happens' somewhere else:

> The subscriber speaks into his telephone, and the process of tapping appears to be carried out by Post Office officials making recordings, with Post Office apparatus on Post Office premises, of the electrical impulses on Post Office wires provided by Post Office electricity. There is no question of there being any trespass on the plaintiff's premises for the purpose of attaching anything either to the premises themselves or to anything on them: all that is done is done within the Post Office's own domain.[663]

Only by including this controversial element could Megarry reach the outcome he did.

5.3 Birkett and prerogative

When the Committee of Privy Councillors led by Norman Birkett reported on the legality of telephone tapping in 1957, they had taken a very different view of the question of legality:

> 49. … it was submitted that, so far as the interception of telephone messages is concerned, reliance could be placed on the doctrine followed until 1937 that the Post Office was entitled to intercept and that it was not unlawful to do so …
>
> 50. We should not be happy to feel that so important a power as the power to intercept telephone messages rested on either of the grounds set out in paragraphs 44-49. We favour the view that it rests upon the power plainly recognised by the Post Office statutes as existing before the enactment of the statutes, by whatever name the power is described.[664]

[662] *Malone v MPC* [1979] 344 Ch., 368–69; see also Paul Scott, 'Entick v Carrington and the Legal Protection of Property', in *Entick v Carrington: 250 Years of the Rule of Law*, ed. Adam Tomkins and Paul Scott (Oxford: Hart Publishing, 2015), 131–60.

[663] *Malone v MPC* [1979] 344 Ch., 369.

[664] Birkett, 'Birkett Report'.

On this account, there was a positive source of power to intercept communication in general. In this respect, Birkett reiterated the findings of the 1844 Secret Committee, which found that letter interception was an emanation of the royal prerogative, the same power that had first established the Post Office. Birkett summarised the Secret Committee's position on the legality of interception as follows:

> (a) The power to intercept letters and postal packets and to disclose their contents and otherwise to make use of them had been used and frequently used through many centuries.
>
> (b) Such a power existed and was exercised widely and publicly known as the debates in the House of Commons and the House of Lords plainly showed.
>
> (c) At no time had it been suggested with any authority that the exercise of the power was unlawful.[665]

But it was not clear whether or how this analysis applied to telegrams and, more especially, to telephone communications. Birkett, like Megarry a senior member of the judiciary as well as a Privy Councillor, was unable to identify any legal authority for the interception of communication in general. There appears to be a degree of deliberate ambiguity in the report's conclusion; the phrase "if there is a lawful power" and "by whatever name the power is described" at paragraph 51(c), cited above, indicate uncertainty.

The view that interception was grounded in the royal prerogative was the long-standing view of lawyers within the Home Office. While various statutes concerning the Post Office had been made over the years that prohibited intercepting or interfering with the mail or telegrams, except where authorised to do so by a warrant, these legislative clauses did not explicitly grant a power of interception to the Secretary of State. Rather, they implicitly suggested that such a power already existed under the royal prerogative. Legislation was drafted to criminalise anyone who tried to interfere with the post without a warrant. Such provisions were, in effect, part of

[665] Ibid., para. 39.

the consolidation of the monopoly over the transmission and interception of correspondence.

The major problem, as Birkett saw it, was new technology. Postal correspondence and telegrams were addressed in legislation mentioning warrants, however obliquely, but telephones were not. It was put to the Privy Councillors that perhaps there was a prerogative power to intercept "any messages", rather than specific media. But Birkett found difficulty with this argument. There was no legal record of a prerogative power over communication in general, and since the Glorious Revolution of 1689, no new prerogative powers could be created. Various constitutional writers had published works listing the various residual prerogative powers of the Crown that had survived the rise of Parliamentary sovereignty after 1689 – no general intereception power existed.

> 23. The opponents of the view that the power to intercept is a prerogative power emphasise the fact that no constitutional writer when dealing with the Royal Prerogative, mentions this particular power as being a prerogative power. In Chitty's *Prerogatives of the Crown* published in 1820, the learned author states that he has attempted "to present a comprehensive and connected, yet compressed and logical, view of every prerogative and corresponding right of the subject"; but nowhere is any reference made to a prerogative power of detaining and opening communications.

That interception was a long-standing government practice was not in itself legally persuasive. That argument was explicitly rejected, along with arguments of state necessity, in the case of *Entick v Carrington*. Just because successive Secretaries of State had assumed the power to intercept communication did not make it lawful. If ministers had issued warrants without authority, it meant only that they *had been* acting unlawfully. The law's past perfect progressive tense indicates that, where the authorities turn a blind eye to legality in the service of other goals, the legal status of their actions is not inherently legal, rather, it is risky. The risk is that the question will have to be determined in the future, and it is that risk which must be evaluated.[666]

[666] Luhmann, *Law as a Social System*, 179.

The ambiguity of Birkett's report may have influenced the government's legal strategy in 1979, which avoided the assertion that interception was a prerogative power. In his judgment Megarry does not dwell on the prerogative, or on the Birkett report's analysis of the law. He says only that he will not rule one way or the other on the existence of a prerogative power to intercept communication. This does not mean that the issue was not argued in court. Given that Malone's case was that no such power existed, only the police or Home Office would have raised it. If they did so, then they dropped the argument by the time argumentation ended. Common law judges are not required to perform an exhaustive investigation of the law, only to assemble and respond to the arguments that are put before them. Megarry could ignore the issue in his judgment only because no one asserted it.

5.3.1 The instrumental past in print

Common law involves using the past in a particular manner that has no regard for hermeneutical strategies or historical context. It means reading legally-valid texts of any age as if they co-exist on a plane of immanence. In Lord Camden's words, it means finding law "in our books" and treating it with complete indifference to the "pastness of the past", an a-temporal horizon, or eternal present.[667]

Stepping away from legal techniques and towards legal-historical techniques, the explanation for the contradiction between Megarry and Birkett is clearer. The doctrine that there should be a statement of all prerogatives had emerged within the common law during the nineteenth century, as it drew up textual lists of prerogative powers in order to ensure no 'new' ones could be claimed by representatives of the Crown. In structural terms, when the Post Office was founded the law did not consider that the *arcana* had to be presented as *arcana*, and therefore no secrecy-effect (*secretum*) was generated that required legal determination. The law did not have any firm rules about the prerogative. It occupied an important but thinly-defined element in the resources then available to the law. Martin Loughlin points out three features of the prerogative as it was described by legal theorists of the seventeenth century:

[667] Murphy, *The Oldest Social Science?* 95.

> First, that the existence of the absolute prerogative, one which derives from the distinction that the medieval scholastics made in theology between God's *potentia absoluta* and *potentia ordinata*, in no way suggests that such powers are unbounded. The absolute prerogative refers to an autonomous power of the king to govern, not arbitrarily to undermine the established legal order. It is a power assigned to the king—by fundamental law—to determine according to "reason of state". Secondly, that it is in the nature of this governmental function that aspects of it must remain secret and be conducted free from public gaze. And, thirdly, that these "mysteries of state" have always been connected to—and also impose limits on—the legal order.[668]

Around 1760, Blackstone, the most famous compiler of legal codes of his era, noted that seventeenth-century monarchs had thought their prerogative powers "too delicate and sacred to be profaned by the pen of a subject". It was considered a forbidden topic for any kind of legal writing. The royal prerogative could not be assigned a place within the legal order as it was not subject to the legal order. It was outside the law and superior to it. The prerogative, says Blackstone, was held to be "among the *arcana imperii*".[669] Royal assertions about the prerogative were contrary to already existing traditions in English law, and so they were viewed by many as an abuse of power. The prerogative thus provided the political backdrop to the English Revolution and to the classic contractual theories of government that followed.

According to Blackstone, things definitively changed after 1689 when the prerogative became decisively subject to law, via a legislative instrument known as the Bill of Rights.[670] If a King attacked the sovereignty of Parliament, that is, if a King tried to rule by proclamation, he would be legally deemed to have abdicated his throne. *De facto* abdication was the only formula that fit, because it was otherwise accepted that

[668] Loughlin, *Foundations of Public Law*, 380.

[669] William Blackstone, *The Oxford Edition of Blackstone's: Commentaries on the Laws of England: Book I: Of the Rights of Persons* (Oxford: Oxford University Press, 2016), 291.

[670] 'Bill of Rights 1689', *UK Parliament*, accessed 20 September 2014, https://www.parliament.uk/about/living-heritage/evolutionofparliament/parliamentaryauthority/revolution/collections1/collections-glorious-revolution/billofrights/.

the King governed in the "public good", that he could "do no wrong", and that the general interests of Parliament and Crown were therefore aligned. In practice, the Crown retained most of its pre-existing powers, and the King was rarely challenged in terms of how he or his ministers exercised them. The crucial difference was that the King could not break the 'contract' upon which his rule relied by acting against the 'constitution'. Writing contemporaneously to the events that led to *Entick v Carrington*, Blackstone's prerogative thus remains a special type of power, existing "out of the ordinary course of the common law", which "must be in its nature singular and eccentrical; that it can only be applied to those rights and capacities which the King enjoys alone, in contradistinction to others".[671] Secret powers were fully compatible with the prerogative.

It was under the symbol of the prerogative that the administrative organisation of governmental institutions took shape. European juridical and political theorists were not blind to the developments in governmental practices and the spread of disciplinary institutions. On the contrary, their task was to invent juridical theories to account for them. In such discourse they were described, generally, as 'police' or 'policy' matters. The concept of 'police' became more developed in French and German theories of state than in England, but it was recognised in England. In 1760, Adam Smith addressed a lecture to the need to enhance the growth and prosperity of the nation. For Smith, trade, security, and infrastructure were critically important matters in need of governmental regulation. Regulation, as a mode of jurisprudence to be distinguished from adjudicating disputes between private persons, he described as a police matter.[672] Blackstone, for his part, related "the public police and œconomy" to the King's powers, amounting to

> the due regulation and domestic order of the kingdom: whereby the individuals of the state, like members of a well-governed family, are bound to conform their general behaviour to the rules of propriety, good

[671] Blackstone, *Commentaries I*, 292.

[672] Loughlin, *Foundations of Public Law*, 424.

> neighbourhood, and good manners; and to be decent, industrious, and inoffensive in their respective stations.[673]

The administrative tasks of the 'police' developed complexity through legislation, but remained matters for the secretaryship. During the twentieth century, the number of Secretaries of State multiplied as the administrative welfare state grew in size, in turn provoking the development of judicial review, and the kind of critical public legal theory that is exemplified by demands for a clear conceptual distinction between public and private jurisprudence and a categorical definition of public power in the UK, which remains ambiguous.[674] Of course, this in no way affects the daily administration of things, which are attributed to the 'public power' of the state only through symbolic references that are constantly regenerated via cultural techniques of ascription. The technical reproduction of 'state' activities in no way depends on the internal coherence of legal theory.[675]

In the eighteenth century, general powers of security were subsumed under prerogative power, and therefore not subject to question by the law. By the twentieth century, when *Entick v Carrington* was unearthed as a constitutionally significant case, the legal understanding of the prerogative had altered completely. Political decisions to wield executive powers were more tightly coupled to the legal system. Judges were notoriously deferential to the executive, but nonetheless that deference had to be expressed in legal terms, whereas under the eighteenth century model, there was rarely any call to review political decisions of the executive.[676] The courts did not review how the prerogative was exercised until 1984 – coincidentally, the substance of prerogative decisions was first judicially reviewed in a case involving strike action

[673] Ibid., 425; citing volume 4 of Blackstone's Commentaries.

[674] Loughlin elaborates on this debate, and on the contemporary questions it continues to pose, in Martin Loughlin, 'The State, the Crown and the Law', in ***The Nature of the Crown: A Legal and Political Analysis***, ed. Maurice Sunkin and Sebastian Payne (Oxford: Oxford University Press, 1999), 33–76.

[675] This is, of course, the basic juridical point that Foucault made by displacing the figure of 'classical' sovereignty, Foucault, 'Governmentality' the point could equally be articulated by reference to the work of Tim Murphy, Niklas Luhmann, Bruno Latour, and others.

[676] This is not to say there were no such cases. See Thomas Poole, ***Reason of State*** (Cambridge: Cambridge University Press, 2015).

by civil servants working at GCHQ[677] – but before that, it was necessary to know what the prerogative powers claimed by government under the symbol of the Crown actually were, in order to be certain that executive decisions all fitted within a legally prescribed list. For the Home Office, the interception of communication was rooted in a continuation of a valid practice established in the seventeenth and eighteenth centuries. Applying the criteria of validity that had evolved in the legal system by the late twentieth century, it was rooted in nothing at all.

5.4 Law and publicity

Knowledge of the legally ambiguous status of interception power circulated within the files of the Home Office for a long time. So long as warrants continued to be made and the Post Office continued to recognise their authority, interception continued regardless. Problems of legal theory did not impact at all on the technical operations of interception. Legal incoherence did not matter, unless and until it was publicised, at which point it became politically dangerous. In short, the legality or illegality of certain practices could be used against the government, and could generate publicity that would in turn damage the effectiveness of the practices. Publicity is mobilised via the application of certain political techniques, which developed alongside the rise of the mass newspaper industry (spurred by the economics of the Post Office itself, as we saw).[678] When legal questions are used this way, the aim is not to achieve legal outcomes for their own sake, but to use law to mobilise the mass media, and thereby generate publicity.

The importance of publicity in relation to the political uses of law can be illustrated by returning to the case of *Entick v Carrington*. While the judgment later became used as a textual resource with which the common law could make decisions about public power, it originally came before the law as part of a tactical move to mobilise the courts themselves as weapons in an ongoing 'propaganda war'. What was at stake,

[677] Council for Civil Service Unions v Minister for the Civil Service (HL 22 22 November 1984); for a full account of the strike at GCHQ, see Lanning and Norton-Taylor, ***A Conflict of Loyalties***; Conor Gearty, 'The Courts and Recent Exercises of the Prerogative', ***The Cambridge Law Journal*** 46, no. 3 (1987): 372–74.

[678] See Section 2.3.

politically, was the ability to use or to suppress the medium of the printing press to political effect.[679]

5.4.1 Wilkes takes the stage

The celebrated *Entick v Carrington* judgment was the culmination of a series of cases and a longer series of events. In November 1762, *The Monitor* and *North Briton* newspapers. In 1762 general warrants were issued, targeting anyone connected to eight editions of *The Monitor*, and in 1763, targeting anyone connected to issued No.45 of *The North Briton* for publishing an article criticising the King over the terms of his peace treaty with France, which concluded the Seven Years' War.[680] The King's Messengers, under warrants of the Secretary of State and Under-Secretaries, seized papers and arrested men. They did not actually charge them: the aim was to intimidate them into self-censorship.[681] The crime of seditious libel was useful for the task as it was very broad. First, the truth or untruth of the libel against the sovereign was irrelevant; second, one could seditiously libel even a dead King, and third, seditious libel did not require publication. Merely passing the information to a third party sufficed.[682]

In response, the printers and journalists sought writs against the Secretaries and Messengers who had harassed them, on the basis of trespass and false imprisonment. On 6th December 1763, the case of *Wilkes v Wood* came before Pratt J, who had already ruled in favour of two printers who had been arrested under the general warrants. Wood was an Under-Secretary of State who had attended John Wilkes' house, knowing him to be a backer of the *The North Briton*, but had not seized anything. Wilkes, an outspoken and popular Member of Parliament, sought to claim that as he had not been personally named in the general warrant, Wood had trespassed on his

[679] Jacob Rowbottom, 'The Propaganda Wars and Liberty of the Press', in ***Entick v Carrington: 250 Years of the Rule of Law***, ed. Adam Tomkins and Paul Scott (Oxford: Hart Publishing, 2015), 85–107.

[680] Ibid., 89–95.

[681] Ibid., 88.

[682] Tom Hickman, 'Revisiting Entick v Carrington: Seditious Libel and State Security Laws in Eighteenth-Century England', in Entick v Carrington: 250 Years of the Rule of Law, ed. Adam Tomkins and Paul Scott (Oxford: Hart Publishing, 2015), 47.

property. Wilkes did not challenge the legality of the general warrant that directed the search and seizure of his property, which would have raised a technical matter for the judge alone to decide on. Instead he sought a trial of the facts, which meant a jury would be assembled. That way, Wilkes could call witnesses and question ministers. His strategy was to win the case by having a jury pass judgment on the situation. The procedures of the trial would give him the theatre of the courtroom in which to perform the role of champion of freedom, to publicly query "whether English liberty be a reality or a shadow".[683] The strategy was not to change the law, but to generate publicity.

As it happened, Pratt J made clear in his judgment that he felt the general warrant was unlawful, a "discretionary power given to messengers to search wherever their suspicions may chance to fall", but as that was not how Wilkes had put his case, the legality of general warrants could not arise and Pratt's comment was no more than *obiter dicta*.[684] On 27th November 1765, when Entick's case was determined, Pratt J, who had by then become Lord Camden, went through the legal issues in an explicit analysis. It may be summarised in three points: a defence of the absolute protection of private property from the tort of trespass in the absence of lawful justification; second, a specific rejection of state necessity, or reason of state, as a factor in English common law; and third, the famous insistence on positive "in our books" authority for actions carried out by the state.[685] To view the case as a triumph for English liberty would be misplaced: Wilkes anonymously sent threatening letters his jury, and published their names in newspapers to apply political pressure. Pratt, the judge, was a friend of Pitt, then in opposition to the government, whose own close associates financed *The Monitor* and the *North Briton.*

The important point is that for the printers, journalists, and radicals of London's political milieu, the law was a publicity device to be used for political ends. Conversely, Lord Camden's famous rhetorical statement that law is what is "in the

[683] Rowbottom, 'Revisiting Entick v Carrington', 100; Wilkes subsequently fled England to France for four years.

[684] Hickman, 'Revisiting Entick v Carrington', 66.

[685] Ibid., 82–84.

books" points to the media-dependency of a law that, under the scrutiny of others, must assemble decisions from the resources found in printed matter. Printed books enabled recorded judgments to be reproduced as texts, disseminated widely in a form that gives certainty to the particular formulations of words in each case. Only then could such texts be decontextualised and reassembled systematically as precedent and collated into a series of analyses and commentaries.[686] Law and media exchanged competencies. The legal system, rather than simply being a way of generating publicity, unexpectedly ruled that the integrity of a man's personal papers had to be legally protected. Printed matter was confirmed as the guarantor of what law is, its media-technical substrate "in our books". When Lord Camden rejected the argument in *Entick v Carrington* that general warrants were justified by reason of state, he showed that the idea that political necessity could generate novel rules or exception would not fit within a system that had attained stability through rearranging texts. The coupling of law and media coincided with a rejection of the mythical power of reason of state.[687] *Entick v Carrington* can be read as a confluence of law, power, and media. From that point on, both publicity and law have been regarded as different elements that can be mobilised towards different ends.

5.4.2 Neither confirm nor deny

When the Mazzini interception scandal occurred in 1844, the English press erupted in a "paroxysm of national anger".[688] The Post Office monitored the anger. During the currency of the scandal, all relevant news reports, commentaries, magazine articles, and letters to editors were all carefully cut out and glued into an entry book for ten months, between 14th June 1844 and 4th April 1845. The Post Office observed itself being publicly observed by the 'public', apprehended via the tenor of reporting in the mass media.[689]

[686] Murphy, *The Oldest Social Science?* 72–74.

[687] Here, we can recall the problems it caused Secretary Coventry, see 4.3.1.

[688] David Vincent, 'Surveillance, Privacy & History', History & Policy, 1 October 2013, http://www.historyandpolicy.org/index.php/policy-papers/papers/surveillance-privacy-and-history.

[689] 'POST 23/7'.

In response to the scandal, Parliament convened a Secret Committee. Their report, as we have seen, was the first historical and legal analysis of English interception power. Hansard, the official record of parliamentary proceedings that began publishing transcripts of debates and speeches around the turn of the nineteenth century, records that the constitution of the Secret Committee on the Post Office was viewed with suspicion by members of the opposition. In a departure from normal procedure, the Committee did not feature any legally-qualified MPs from the House of Commons. Meanwhile, the unelected members of the House of Lords contributed three ex-Ministers and two ex-Chancellors, men both loyal to the government and "accustomed to the most skilful mode of examination either for suppressing or for eliciting information."[690] This information was relayed in a speech from Thomas Duncombe, the Liberal MP who first raised Mazzini's case in Parliament, who claimed to have witnesses willing to testify about the details of interception practices. Hansard records that he unsuccessfully raised a motion in the Commons on 18th July 1844 seeking a vote to alter the constitution of the Committees. During the debate, Duncombe demanded to know if his own letters were being targeted by the Post Office. The Home Secretary, Sir James Graham, replied that he was unable to answer publicly,[691] saying,

> [Duncombe] has put to me a question to which he knows it is not consistent with my own sense of duty to attempt an answer. I have already stated to the House, respectfully and firmly, that consistently with my sense of duty, and bound by the obligation by which I am bound—and I am the judge of that sense of duty—I cannot answer, and will not answer this question.[692]

This appears to be the first recorded occasion on which a government minister refused to answer a question in Parliament. To neither confirm nor deny the premise of the question is to end the discussion. It is a barrier to further communication. It was the only way to give a public response and simultaneously maintain secrecy. The limit of

[690] 'POST OFFICE—OPENING LETTERS. (Hansard, 18 July 1844)', accessed 22 August 2017, http://hansard.millbanksystems.com/commons/1844/jul/18/post-office-opening-letters.

[691] Vincent, *The Culture of Secrecy*, 6 in his replies in Parliament Graham implicitly rebukes them for hypocrisy, but cannot spell this out publicly.

[692] 'POST OFFICE—OPENING LETTERS. (Hansard, 18 July 1844)'.

publicity was publicly drawn by publicly issuing a non-answer. The alternative would be to set a precedent for answering such questions. The formal 'neither confirm nor deny' response marks the limit of governmental publicity and secrecy today.[693] The abbreviated form, NCND, is shorthand for official UK government policy on responding to questions about official secrets.[694]

The Report of the Secret Committee, which of course was unavailable to the press, posits public opinion as a critical factor in its concluding recommendations. Prefiguring the problems that Birkett and Megarry later addressed, the report points out that although letter interception had been recognised as a prerogative power of the Crown by successive statutes, it was not based on any positive statement of law.[695] This was not a problem in itself, but the report does consider whether or not the government should legislate on the topic. In that respect, the question is publicity. The public would probably tolerate letter interception if they knew it was done only under a warrant, rather than via "extraordinary powers".[696] But while the public would probably tolerate interception for policing purposes, the Secret Committee suggests that the political uses of interception warrants risked inducing stronger "moral feeling which exists against the practice of opening of letters, with its accompaniments of mystery and concealment".[697] Ultimately, legislation would only attract unwanted attention:

> it must not be forgotten that, after the publicity given to the fact, that the Secretary of State has occasionally recourse to the opening of letters as a means of defence in dangerous and difficult times, few who hereafter may engage in

[693] In the United States, it is known as the 'Glomar response', Nicholas Wade, 'Glomar Explorer: CIA's Salvage Ship a Giant Leap in Ocean Engineering', ***Science*** 192, no. 4246 (1976): 1313–1315; N. Wade, 'Glomar Explorer Said Successful after All', ***Science (New York, N.Y.)*** 194, no. 4270 (1976): 1142 - NCND was the reply given to journalists who made Freedom of Information Requests about the Glomar Explorer, a secret CIA attempt to raise a sunken Soviet nuclear submarine.

[694] The Information Commissioner's guidance is instructive, see 'When to Refuse to Confirm or Deny Information Is Held' (Information Commissioners Office, 2013), https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf.

[695] This is stated briefly. ***Report from the Secret Committee on the Post-Office, Together with the Appendix***, 3.

[696] Ibid., 19.

[697] Ibid., 18.

> dangerous designs, will venture to communicate their intentions by the medium of the Post; and the importance of retaining the power, as a measure of detective police, will consequently be greatly diminished.[698]

Therefore, "it may appear to some that to leave it a mystery whether or not this power is ever exercised is the way best calculated to deter the evil-minded". In the final analysis, the Committee recommended maintaining the status quo.[699] The issue of whether or not to clarify the law was not decided by reference to justice or legal coherence, but by measuring the certainty of legislation against the effects of publicity.[700] To return to the distinction between forms of secrecy, in order to protect the *arcanum*, the secrecy effect created simply by signalling through legislation that a secret existed had to be minimised.

On 18th February 1845, when the affair was no longer a pressing news story, the Home Secretary, "telling the truth in carefully chosen words",[701] announced that the Post Office department maintained by the "Foreign Secretary of the Post Office" had been abolished. Meanwhile, interception of inland communication continued as before, soon expanding to include the telegraph.[702] The Post Office continued collecting news cuttings for two more months, presumably making sure that press attention had moved on.

5.4.3 Policies of secrecy

Secrecy within the administration of government had long been "embedded in administrative structures, regulations, and *mentalités*",[703] with silence being an inherent expectation of a gentlemanly civil servant. The historian of state secrecy, Christopher Moran, links the switch to legislative control under the Official Secrets Act, the first iteration of which was passed in 1889, directly to the growth in bureaucracy of the late nineteenth century. As government increasingly organised

[698] Ibid., 19.

[699] Ibid.

[700] Vincent, *The Culture of Secrecy*, 1–25.

[701] Ellis, *Post Office in the Eighteenth Century*, 141–42.

[702] Ibid.

[703] Moran, *Classified*, 25.

itself through the constant updating of registries, memos and filing catalogues, more and more bodies were required to service the movement and copying of files. This opened up government to men of lower standing, who were felt by senior civil servants to lack the moral cohesion of the elite, and to be vulnerable to the temptation to sell secrets.[704] Criminalisation was the inevitable outcome after a series of high-profile leaks during the second half of the nineteenth century, as secrecy was transposed into legal rules.

In media-technical terms, publicity-management is a procedural inflection on file-management. The circulation of information to and from files could only be permitted via closed, secure channels. A 'leak' was the name given to any information that escaped the closely prescribed circuits that files prescribed. To take effect on files, policies had to be placed in files. Policies became indexed as 'precedents' that could be stored and recalled as needed in the processing operations of the filing system itself. They operated reflexively, telling the users of files how to use them as and when the question of choosing between publicity or secrecy arose.

As explained previously, there are relatively few examples of files and materials concerning interception in the National Archives, which is probably a consequence of the excision of files on the topic. As Birkett discovered in 1957, the simplest approach to maintaining the secrecy of documents was to destroy them.[705] Yet there are several files in the National Archives that are indicative of the secrecy policy in respect of interception, and how it was maintained and used.

The particular prohibition on interception warrants entering courtrooms was clearly articulated in a file generated in 1929 in connection with the Meerut Conspiracy trial in India, in which a group of English and Indian trade unionists were prosecuted for conspiring to organise a railway workers' strike.[706] The prosecution wanted to include

[704] One Fleet Street newspaper advertised a rate of £5 for minor news and £100 for 'great secrets' ibid., 33.

[705] Section 4.6.

[706] The trial was commemorated in a 1932 play by the Manchester group Red Megaphones, see 'The Meerut Conspiracy Trial', accessed 25 May 2017,

intercepted material as evidence of the conspiracy. However, under Indian law the prosecution had to include interception warrants as evidence, in order to show that the intercepted material was lawfully obtained. In correspondence with Indian prosecutors, the Home Office indicated that this "would be very undesirable", and refused to provide the warrants despite the consequences for the prosecution. A letter to the Indian prosecutors again referred to precedent and explained that, as of September 1929, no interception warrant had ever been produced in court and this was policy not about to change.[707]

The press was kept under observation. Between 1926 and 1932 the Security Service, MI5, maintained a file dedicated to monitoring breaches of secrecy around interception powers. Left-wing newspapers occasionally reported on "The Black Cabinet in the Post Office", as the headline in a clipping from the *Workers Weekly* of 10th December 1926 puts it. On one occasion, a registry slip from MI5 accidentally ended up enclosed in an envelope delivered to one interception target, which was duly reported in *The Daily Worker* on the 12th December 1931.[708] Interest in interception was not limited to left-wing journalists. In 1935, the Postmaster General's office received a letter from a journalist working for the conservative magazine *John Bull*, proposing a feature on the interception of illicit and communist material in the postal system. The Post Office wrote to the Home Office, who responded with a letter making clear their prohibition on co-operation with mass media discussions of interception. The Home Office quoted a statement from Sir William Harcourt made in 1882, when he was Home Secretary:

> 'The very essence of the power is that no account can be rendered. To render an account would be to defeat the very object for which the power was granted.'

Harcourt's statement had become a policy maxim. The letter to the Post Office continued:

https://web.archive.org/web/20080303235605/http://www.wcml.org.uk/internat/meerut.htm; 'Cases of Leakage of Information about Interception of Mail 1926-1932 KV 4/221' 1932, National Archives.

[707] In the trial of Ernst prior to WW1, intercepted letters were produced, but the warrant was not. Section 2.5.

[708] 'KV 4/221'.

> Accordingly, while Parliament is aware of the existence and exercise of the power, it has been the invariable practice to decline, in the public interest, to furnish any information, even to Parliament, as to details …. If articles are published it is perhaps better on the whole that they should be inaccurate, and capable of denial, if questions should be asked in Parliament.[709]

Even Parliament was subject to the ban on communication about interception and in fact, Parliamentarians could be fair game for deliberate misinformation strategies.

During the early twentieth century, the Post Office was charged with identifying and intercepting postal packets thought to contain 'indecent material' and solicitations to enter illegal lotteries.[710] In 1920, a general warrant was signed for the interception of any letter suspected of containing solicitations to enter lotteries, a memo stating that it would be 'troublesome' to seek a specific warrant on each occasion that lottery correspondence was suspected. In 1934, it was decided that the general lotteries warrant should be replaced by individual specific warrants. Citing precedent legal advice obtained and stored in 1866,[711] the memorandum of 1934 discusses section 56(2) of the Post Office Act 1908, which said no one could open, delay or detain a postal packet, except "in obedience to an express warrant in writing under the hand of a Secretary of State".[712] This legislative formulation could not justify general warrants. Although it would be costly in terms of time and resources, the Home Office lawyers felt this to be the correct reading of the law, confirming that their lawyers did take law seriously even in the absence of judicial scrutiny. The alternative was to legislate for general powers of interception in respect of lotteries and indecent material. A lotteries bill was passing through parliament at the time, but it was decided that to amend the bill in order to allow for general interception of lottery material was too risky, despite the administrative benefits. Legislation would,

[709] '"John Bull" Article on Working of Postal Warrants HO 45/25960' 1935, National Archives.

[710] Including novels. See 'PUBLICATIONS: Interception in Mail of Copies of Poetry Book Pansies by D H Lawrence HO 144/20642' 1929, National Archives; 'HO 144/1837'; 'HO 45/25958', 259.

[711] As cited in chapter three, 'HO 144/164/A42354', 164.

[712] 'Post Office Act 1908', accessed 25 May 2017, http://www.legislation.gov.uk/ukpga/1908/48/section/56/enacted.

> … give rise to the most acute controversy and indeed might throw a doubt on the legality of actions taken in the past, and might also have far reaching consequences on the exercise of the prerogative power generally.[713]

The protection of secrecy thus took precedence over administrative convenience. The file includes a recent newspaper clipping of an article about Post Office interception. The uncertainty of the law in the absence of legislation was a problem, but the constant threat of publicity was more important.

5.4.4 Publicity trumps law

While the Home Office's filing system maintained and reiterated the imperative of non-publicity in respect of interception, it also began to signal that interception might be legally unsound. Perhaps prompted by the need in 1934 to consult precedent legal advice dating from 1866 in respect of lotteries, the legality of postal interception was reviewed in updated legal advice obtained from a government legal advisor in 1935. First, registry files were reviewed and a series of precedent examples noted and collated in a single reference file.[714] Then the prerogative, as a legal form of authority for intercepting letters and packets, was analysed in a detailed eighteen-page memorandum stored in a separate file.[715] It concluded that the prerogative form was ambiguous, but ultimately the interception of letters and packets was lawful.

However, telephone interception was different. In 1937, telephone interception warrants were introduced for the first time as a matter of policy.[716] Legal advice obtained from government lawyers as part of the process, however, strongly suggested that no lawful power of telephone interception existed. On the question of letters and telegrams, the government lawyer cited section 20 of the Telegraph Act 1868, which made it an offence for a clerk to disclose the contents of any telegram in circumstances "contrary to his duty". The Post Office Act 1908 criminalised any interference with a "postal packet", except "in obedience to an express warrant in

[713] 'HO 45/25958', 259.

[714] 'HO 45/25961'.

[715] 'HO 45/25962', note that the precedents file and the legal advice file have sequential index numbers.

[716] See 4.5.2.

writing under the hand of a Secretary of State".[717] Section 89 of the Post Office Act 1908 held that a "telegram" was included in the definition of a "postal packet". The prohibition on disclosure of a telegram in section 20 of the Telegraph Act 1968 could therefore be overridden by a warrant. But no analogous law regarding telephone warrants existed. When the Post Office had been awarded the right to issue licenses to telephone companies, it had successfully argued in the case of *Attorney General v Edison Telephone Company* that a telephone call and telegram were the same thing in law.[718] An individual clerk would be acting in line with his 'duty' if ordered to disclose a telephone call's contents by the Postmaster General, but there was nothing that suggested the Postmaster General would not then be liable to prosecution for making such an order. This analysis was far more pointed than anything later discussed by Birkett or Megarry. In short, the Home Office lawyer who drafted telephone interception warrants felt that telephone interception was illegal.[719]

It was generally assumed that legislation would resolve any ambiguity as to the legality of interception. In 1957, the Birkett report stated that if legislation were desirable, "it would be for Parliament to consider what steps ought to be taken to remove all uncertainty if the practice is to continue".[720] However, when the Birkett report was published, the leaders of both the Conservative and Labour parties ensured that their Members of Parliament remained silent. No questions were asked in Parliament concerning the report, and no subsequent questions were raised about the implementation of its recommendations.[721] Similarly, there was little coverage in the press of the Birkett report, despite large amount of sensational reporting when the phone-tapping 'scandal' that triggered the report first occurred. Journalists Fitzgerald and Leopold attribute this to a political agreement between editors and government officials to minimise the coverage.[722] This is plausible; by the 1950s the British

[717] Section 56, 'Post Office Act 1908'.

[718] 'Telegraph Act 1868'; ***Attorney-General v Edison Telephone Co of London*** 6 QBD 244. See fn. 336.

[719] 'HO 144/20619'.

[720] Birkett, 'Birkett Report', paras 51–52.

[721] Fitzgerald and Leopold, ***Stranger on the Line***, 124–26.

[722] Ibid.

government had established an effective system of voluntary press censorship based on the so-called 'D-Notice' system.[723]

5.4.5 Publicising secrets

For over a century, the Home Office and successive governments had been warned that the legal consistency of the prerogative in relation to interception was increasingly doubtful and that legislation would have provided a solution. Only when Malone finally brought the matter into court did change become a necessity rather than an option. In the immediate aftermath of Megarry's decision in *Malone*, the Home Office convened a Working Party on Interception in March 1979 to consider the judgment and assess the options for legislation, and to ask whether it would indeed be necessary. The Working Party's correspondence, partly redacted, was obtained under a Freedom of Information request for this thesis.[724]

It opens with two press cuttings, an article from the *New Scientist* and another from the *New Law Journal*, both dated 8th March 1979, and both critical of the state of the law after the judgment. In general, the correspondence involves different agencies such as the police, Post Office, customs, and the prison service informing the Home Office of the utility of interception for their roles and their current practices and internal procedures for seeking and granting authorisation to use it. On the whole, the Home Office was satisfied that the existing practices "strike an appropriate balance" between "the need to preserve the value and efficacy of interception and […] the protection of the liberty of the subject". However, "we could not in fairness say that the public knows this to be so." Noting that "since the Birkett Report the climate of opinion has become more critical", it continues:

> … any more vigorous defence of the present arrangements confronts the classic dilemma that, in delicate matters of crime and security, as little as possible

[723] A Privy Councillors' report was commissioned into the D-Notice system after Chapman Pincher revealed international cable interception, as discussed at 3.5.4. The aim of the report was to better suppress reporting of secret materials, see 'Report of the Committee of Privy Counsellors Appointed to Inquire into "D" Notice Matters'; see also Moran, ***Classified***; Nicholas Wilkinson, ***Secrecy and the Media: The Official History of the United Kingdom's D-Notice System***, (London, New York: Routledge, 2009).

[724] It is now accessible in the National Archives. 'HO 325/536'.

> should be said publicly to avoid compromising the very value of the operations on wishes to justify. Some foreign countries have responded to this problem by setting their interception arrangements in the context of a detailed law … We have been informed, and have no reason to doubt, that the law enforcement and intelligence agencies in those countries have been severely handicapped in their capacity to obtain advance intelligence via interception, and the greater openness of the arrangements has often removed useful sources of information.[725]

The report anticipated, correctly, that the European Court of Human Rights would insist on legislation. Therefore,

> In the Working Party's view "legislating Birkett" would be the least objectionable course, but it would be best framed in such a way as to avoid cases becoming justiciable as a result. Our legal advice is that this cannot be done with certainty.

One concrete means of doing this prefigures current arrangements, discussed below:

> In order to provide a limited form of independent appeal, we also recommend the appointment of three advisers to the Secretary of State to whom aggrieved persons could appeal. These advisers would have access to the files on the case in question. They would not be able to tell the individual whether or not his telephone had been tapped; but they would be able to assure him that if it had been tapped this had been done for good reason and the proper procedures followed.

The Malone case took place against the backdrop of a wider change in government strategy concerning secrecy. During the 1970s, faced with leaks, spies, and the publication of memoirs, the British government gradually accepted that it was unable to constrain publications about controversial aspects of its national security and foreign intelligence agencies. There was simply too much information accumulating, and too many people to effectively censor. Instead, the strategy shifted to embracing "a public relations-infused approach to information control, based on experiments

[725] Final report, 9th July 1979, ibid.

with opinion-forming".[726] Rather than suppressing information about the arcana of state power, they would be framed for consumption by the mass media.

The strategy involves a wide range of measures in a number of fields, not least of which is what Aldrich calls "policing the past": carefully vetting and censoring secret documents and then releasing them to the National Archives.[727] That strategy includes material used in this thesis. Other changes include publicly advertising jobs in the intelligence and security services, allowing public appearances by named directors of the services, and commissioning new buildings by postmodern architects to give the agencies a distinct visual identity in relation to the city and the countryside, with MI6's "Babylon on Thames" and GCHQ's "doughnut", typically photographed from above as if it were only to be seen from a satellite, just the most famous instances.[728]

The turn to publicity informed the making of legislation to bring the intelligence and security services onto a public legal footing. The Security Services Act 1989 and the Intelligence Services Act 1994 assigned MI5, GCHQ, and MI6 formally defined legal roles. Malone taking his case to Strasbourg may have forced the timing of the Interception of Communication Act 1985 upon the government, but it coincided with a broader shift in strategy that saw legislation as a tool for proactively determining the frame of public discourse about formerly secret agencies, rather than a triumph of the rule of law.

5.5 Mediated reality

In Foucault's account of the rise of nineteenth century liberalism out of eighteenth century absolutism, government does not create or promote 'freedom' so much as generate it and feed from it. 'Freedoms' are always relationally defined, and evaluated as binary distinctions that can be evaluated according to the achievement or hindrance

[726] Moran, *Classified*, 347.

[727] Richard J. Aldrich, 'Policing the Past: Official History, Secrecy and British Intelligence Since 1945', *The English Historical Review* 119, no. 483 (2004): 922–53.

[728] Moran, *Classified*; Aldrich, 'Policing the Past: Official History, Secrecy and British Intelligence Since 1945'; Andrew, *The Defence of the Realm*; Keith Jeffery, *MI6. The History of the Secret Intelligence Service 1909-1949.* (London: Bloomsbury Publishing Ltd, 2011).

of other governmental ends.[729] Publicity management is one such governmental practice amongst others. Viewed strategically, government mobilises and manages the 'freedom of the press' through selective practices designed for withholding information.

Publicity as a governmental resource is particularly significant because more than any other technique or governmental practice, it is the means by which government describes itself to itself and others. The unity of the 'state' is not an ontological given, as implied by most legal and political theories, nor is it simply the agglomerate effect that emerges from an assemblage of different instrumental governing strategies. The notion of 'state' as an emergent effect of ascription, and the circumstances under which the meaning of the state is formed, can be understood by focusing on the structural coupling of legal and political communication to the reality that is recursively generated by the dissemination of information through mass media operations, as described by Niklas Luhmann. We must here suspend a close reading of the agency of technical media and deploy instead a theory based on observation.

5.5.1 Theory of the mass media

To understand mass media and publicity, we begin with the "addictive and generative power of 'information'",[730] as perceived by an observer. 'Information' is used here in the phenomenological sense articulated by Gregory Bateson, that is, as a "difference that makes a difference" to an observer, rather than information as physical order distinguished from entropic disorder.[731] For information to make a difference in this sense presupposes an observer. Where the observer is capable of second-order observation, meaning the capacity to observe oneself in the act of observation and thus shift between *what* is observed and *how* it is observed, the observer can observe other possible modes of observation that were open to them but not actualised. To do so, the observer requires time. The present is the vanishing instant of observation,

[729] Foucault, *Birth of Biopolitics*, 63–65.

[730] Alain Pottage, 'Our Geological Contemporary', in In Search of Contemporary Legal Thought, by Desautels-Stein and Tomlins (Cambridge: Cambridge University Press, 2017), 182.

[731] See Gleick, *The Information*; César Hidalgo, *Why Information Grows: The Evolution of Order, from Atoms to Economies* (Allen Lane, 2015).

connecting the past and future. The observer is perpetually in the present of observation.

According to systems theory, neither the creator nor the addressee of a given piece of information can experience the other's role in communication. Hence the informational aspects of each 'utterance' are determined by whatever each observer considers to be significant. The utterance, which means the selection of how the information is mediated, is also an attribute ascribed to the information by each party. For each observer, any piece of information that can be observed as such presents a horizon of possible understandings. The world is produced differently for each observer or observing system as a broad and unpredictable horizon of possibility. Readers, writers, listeners, viewers, and users of mass media must all select and reconnect for themselves the 'information' and 'utterance' of each item in radically different ways, using techniques of second-order observation.

The role of a medium is to provide some stability by narrowing the possible selections. By the repeated use of recognised forms of presentation, media function to constrain the range of possible understandings so that communication can become relatively consistent and reliable, even where millions of different people are watching, listening, or reading along. While technical conditions determine the possible scope of observation, they do not determine the meaning that observers ultimately attribute to each statement. Communication occurs only at the moment that an observer assigns meaning to a statement, which is not necessarily the same instant that a technical medium performs its digital, electric, or physical operations.

The mass media in this sense includes any system for disseminating information that uses copying technology to reproduce information, and which does not pre-determine or particularise its addressees. Luhmann argues that modern society has come to anticipate a certain mode of second-order observation that structures how mass media are understood. This includes scepticism about the truth of information. It has long been agreed, for instance, that advertising is designed to manipulate, that entertainment is formulaic, and that newspapers have political agendas. The point is that all such observations about the mass media presuppose the capacity to alternate between first and second-order observation, and thereby consume information while filtering it through the difference between what is said and how it is delivered. Knowing how observations are manufactured is built into the observation of what is communicated. This way, everyone is expected to keep up with the world, allowing complete strangers to communicate on the assumption that everyone is more or less aware of what is 'going on', and what is important at the moment. As Alain Pottage puts it, "dealing with the mass media is in itself an education in second-order observation."[732]

The notion of constantly knowing what important things are 'publicly' unfolding in the world through the media implies that society is informed about topics via a temporal dynamic that constantly substitutes old information for new information. The process of disseminating 'new' information instantly transforms it into 'old' information. The mass media system itself feeds on its own product. It seeks out new information only to immediately transform it into redundancy simply by processing it.

> Information cannot be repeated; as soon as it becomes an event, it becomes non-information. A news item run twice might still have its meaning, but it loses its information value. If information is used as a code value, this means that the operations in the system are constantly and inevitably transforming information into non-information. The crossing of the boundary from value to opposing value occurs within the very autopoiesis of the system. The system is constantly feeding back its own output, that is, knowledge of certain facts, back into the system on the negative side of the code, as non-information; and in doing so it forces itself constantly to provide new information.[733]

When a news item is broadcast, it cannot be repeated, at least not the following day. If a story has been 'broken' elsewhere, then a news organisation must assume that observers are already informed and the story has to be abandoned, or presented with

[732] Pottage, 'Our Geological Contemporary', 184.

[733] Niklas Luhmann, The Reality of the Mass Media, trans. Kathleen Cross (Cambridge: Polity, 2000), 20.

a novel twist. After producing news, the next task for the editor or the journalist is to find a new angle. This might mean adding more information to the story, or deepening it by finding connections elsewhere, or correcting it because new facts have emerged, or employing a commentator from the senior echelons of the profession, or perhaps even from academia, to add an opinionated 'perspective'. What is 'new' is actively manufactured, and folded into the operations of the news organisation, simultaneously setting the departure point for more news to come.

The cumulative effect is that contemporary social reality is structured by the operations of the mass media. In classical and ancient societies, it was the priests who informed society about itself. For a period of time, philosophers believed that they alone had the tools to correctly interpret the world and give it meaning. Today, one switches on the television or logs onto so-called 'social' media. As Luhmann puts it,

> Every morning and every evening, an inexorable web of news settles over the earth and sets out what has happened and what one has to be ready for.[734]

Some events are not subjects for the mass media, and they are ignored except insofar as society is described as a turbulent place where unexpected things happen all the time. Other events occur specifically in the expectation that they will be picked up in the mass media. Mass media do not invent the topics they report on, but when they select information they present it in a way neither determined nor explained by the priorities of other functional social systems. The dynamics of mass media always depend on generating information about society and, at the same time, determine the horizon of possibilities for other social systems when it comes to interacting with the 'public' or 'society' at large. Mass media therefore have a "retroactive effect upon communication in the environment of the mass media".[735]

This means that law, too, must respond to the imperatives of the mass media when deciding whether or not to discuss state *arcana* – put figuratively, the issue is whether or not to open the envelope and peer inside. Luhmann's theory of the mass media

[734] Luhmann, *Theory of Society*, 2:315.

[735] Luhmann, *The Reality of the Mass Media*, 12.

serves to confirm that secrecy has no mysterious valence or metaphysical quality in the modern age. It simply requires preventing information from being reproduced and disseminated through the mass media. Whatever knowledge can be attributed to the 'public' is generated via the mass media. There is no other system that can disseminate information to undefined recipients in a generalised and widespread manner. The protection of the *arcana* of state, which must not be communicated about in order for their techniques to remain unobserved and thus effective, is particularly attuned to the dynamics of the mass media. Few things attract mass media attention like the disclosure of secret information. This is not because secrets are politically important or intellectually interesting, but because they are always novel. As such, the "secrecy effect" that Horn discussed is always materialised as a media effect:

> Instead of being part of the sphere of political rationality, the secret today is relegated to the domain of slip-ups and indiscretions. It can come to light only in the form of scandal – or fiction.[736]

Paradoxically, mass media both demand full transparency and, at the same time, renew their operations each day on the basis that there is always something hidden, and therefore something more to know. The secrecy effect – the knowledge of the unknown – is the presupposition of believing there is something 'new' to say on a 'rolling basis'.

In 1844, when the Secret Committee set the tone for future discussions about interception and legislation, they referred to the 'public mind' and anticipated it would respond to more information about interception badly. The point was not about whether or not interception was felt to be justified: it was. The point was that the mass media would make much of the story and thereby information about interception practices would be used by potential targets to evade detection. The engine of publicity, motivated by 'public opinion', would have unacceptable strategic consequences. The leaking of secrets to the mass media, therefore, is a tactical problem more than a democratic problem. The utility of secrecy aims at ensuring the ongoing reproducibility of interception operations as effective sources of intelligence, rather

[736] Horn, 'Political Secrecy', 118.

than a concern that 'public opinion' will lead to a change in the law towards a more 'transparent' regime. This is not to say that such outcomes are impossible. The myth, however, is the assumption that the 'public' is a pre-existing collective of willing individuals with political agency, who will rise up and demand change from the government if only they were better informed.

Public opinion itself is a fiction of the mass media. It can never be consulted in advance of reporting on it, rather it is projected onto the position of the spectator, the imaginary consumer of mass media who is at once affected by social changes, takes part in them, and at the same time feels anxious about their consequences. Media producers must project an idea of the 'public' as the sum of segmented stereotypes and audience typologies, which have been produced by and for the mass media's own operations.

> It therefore makes little sense to ask whether and how the mass media *distort* reality; they *generate* a description of reality, a world construction, and this *is* the reality on which society orients itself. Information is disseminated in large quantities and day by day. This produces immense redundancy, which obviates having to investigate what individuals really think and know.[737]

Media determine what they presuppose, and the rest of society has to adapt, including political decision-makers.[738] Public opinion "is the 'Holy Spirit' of the system, the communicative availability of the results of communication."[739]

For those in opposition to government, it is also understood that the mass media determine public opinion. Consider the way in which the Snowden story was reported. Edward Snowden chose to give his cache of leaked material to journalists Glenn Greenwald and Laura Poitras because he knew from their published work that they had adopted political positions critical of the US government's secret intelligence activities. In order to process the information into the public domain, Snowden, Greenwald and Poitras devised a strategy of working with different news

[737] Luhmann, *Theory of Society*, 2:318.

[738] Luhmann, *The Reality of the Mass Media*, 21.

[739] Luhmann, *Theory of Society*, 2:322.

organisations in different countries. Each news organisation was assigned particular types of 'revelation', and a schedule was devised so that information would emerge incrementally, "so as to enable an enduring public debate with real consequences, rather than achieve a one-off scoop that would accomplish nothing beyond accolades for the reporters."[740]

5.5.2 Consequences of mass media

The symbolic fictional collective of the 'public', generated via the mass media, plays a central role in the law. When the European Court of Human Rights found the UK to be in breach of Article 8 of the Convention in *Malone*, it was on the basis that no public law existed indicating the rules and procedures governing interception powers. A secret governmental practice that, by its nature, interfered with privacy must be 'foreseeable', and this foreseeability must take the form of law. It does not mean that operational secrecy must be sacrificed, but it does require that the general circumstances in which interception powers may be authorised must be indicated to the 'public'. This connects legality to democratic legitimacy, via the symbolic status of legislation as the highest form of valid law – even if in reality only lawyers ever read it.

The legal expertise required to cognitively understand legislation is totally irrelevant to the legal question of 'foreseeability'. What matters is that there is 'public' law, in the sense of legislation that is publicly disseminated. The technical methodologies of interception are not required to be published, as that would defeat their ends, but detailed guidance codes that explain the general requirements are necessary. The inscription of secrecy and publicity within the law recently led to unusual decisions in the specialised forum designed for hearing such cases. In other words, the normativity of legislation is determined not by any normative content about practices of interception, but by the standards of mass media. Law self-assesses its own capacity to disseminate information.

[740] Greenwald, *No Place to Hide*, 56.

5.5.3 Below the waterline with the IPT

In order to facilitate complaints, the Investigatory Powers Tribunal (IPT) was established by the Regulation of Investigatory Powers Act 2000 (RIPA). The IPT was legislatively constituted to have exclusive jurisdiction over complaints from individuals who believe themselves to be subject to unlawful violations of RIPA, or related unlawful infringements on rights protected by the European Convention on Human Rights (ECHR). The Tribunal was specifically designed to maintain the secrecy of individual cases while conducting its work.

Members of the Tribunal, all security-vetted lawyers or judges, are empowered to compel the police, intelligence services, or other relevant agencies to disclose to them all information relevant to any complaint. Working secretly with the agencies, the Tribunal must, in each case, independently arrive at a decision from a prescribed list of possible decisions. Where a complainant has in fact not been the object of interception at all, they receive the determination: 'Complaint Not Upheld'. Precisely the same answer is issued to any complainant who is in fact under communications surveillance, provided the agencies concerned have operated in accordance with the law. The response 'Complaint Not Upheld' is deliberately ambiguous so that a network of complainants cannot use the Tribunal to establish who is and who is not under investigation. The government's policy of 'neither confirm nor deny' remains intact. Only where the Tribunal finds unlawful interception of communication occurred is a complaint 'upheld'. If that happens the IPT must report the details directly to the Prime Minister, while providing the complainant with general information about the finding, but no details that would compromise operational secrecy in general. There are no rights of appeal from the IPT under RIPA (although this is to change under the Investigatory Powers Act 2016).[741]

[741] Sections 65-70, 'Regulation of Investigatory Powers Act 2000', accessed 19 June 2017, http://www.legislation.gov.uk/ukpga/2000/23/contents; 'Investigatory Powers Act 2016', accessed 25 January 2017, http://www.legislation.gov.uk/ukpga/2016/25/section/261/enacted; Anderson, 'A Question of Trust', 121–23.

However, in 2003 the Tribunal altered its procedures to enable open hearings in certain circumstances. A complaint brought by an individual, with support from a civil liberties NGO, sought to address not only the legality or illegality of the alleged interception of his communication but also challenged the legality of the Tribunal's procedural rules.[742] Under section 68 of RIPA, the Tribunal was empowered to modify its own procedures so as to be able to assess matters flexibly. The Tribunal found that section 68 gave it authority to judicially review the procedural rules made for it by the Home Office, and then ruled that maintaining absolute secrecy in each situation interfered with the right to a fair trial.

Since then, echoing Megarry's strategy in *Malone*, the Tribunal has conducted open hearings on preliminary questions of law where the law is unclear. The government is party to such cases but formally holds a position of 'neither confirm nor deny' in respect of the alleged facts. The law is assessed on the basis of 'assumed facts', a fictional hypothecation that allows a generic legal argument to unfold, addressing whether or not the claimant's allegations would be legal or illegal. Once the legal question has been determined by the Tribunal, consideration of the specific facts of the complaint take place in closed proceedings without the complainant or his lawyers present, a phase that the Tribunal has come to refer to as 'going below the waterline'.

After the Snowden revelations, a number of NGOs petitioned the IPT, notably an organisation called Privacy International, which organised a series of challenges to the legality of different aspects of UK interception powers as described in the published material. Here, we shall address the two instances in which the Tribunal ruled that hypothetical powers were unlawful when measured against the requirements of Convention rights. The critical issue in both instances concerned the 'foreseeability' of potential violations of privacy by the government under the law.

In the first case, Privacy International and Liberty, a civil rights organisation, led a coalition of international NGOs in arguing that regardless of the UK's legal

[742] 'Summary in the Matter of IPT/01/62 and IPT/01//77', Case summary (Investigatory Powers Tribunal, 22 January 2003), http://www.ipt-uk.com/docs/Summary_IPT0162_0177.pdf.

framework as it applied to UK agencies, there was no publicly available legal framework that governed the transfer of data obtained under RIPA powers to foreign governments. Given that the Snowden documents demonstrated close co-operation and extensive data transfers between GCHQ and the NSA, amongst others, the lack of any publicly available legal framework meant that transfers and sharing of private data governed by RIPA was not 'foreseeable' to the public, and therefore unlawful under Article 8 of the ECHR.[743]

In the second case, the issue concerned the collection and use of bulk datasets containing various aggregated digital databases of personal information, and communication records from telecommunications companies. The latter were compelled to provide records of users and their communications not under RIPA powers, but under section 94 of the Telecommunications Act 1984, legislation for regulating the telecommunications market upon the privatisation of British Telecom. Section 94 enables the Home Secretary to issue any 'directions' to a telecommunications company that she deems necessary for the purposes of national security, and binds the addressees of such directions to secrecy. The acquisition of personal data in this manner was held to be unlawful due to lack of foreseeability.[744]

In both instances, the Tribunal ruled that the unlawfulness caused by the lack of foreseeability had been remedied by the time of the publication of the Tribunal's decision. During the course of the hearings in relation to bulk datasets, the government publicised draft Codes of Practice offering rules on how the intelligence and security agencies collected and processed bulk data, and how these processes were made subject to oversight. Bulk data practices were described in a report issued by the Intelligence and Security Committee,[745] a Parliamentary oversight body, and

[743] Liberty & Others v The Secretary of State for Foreign and Commonwealth Affairs & Others, IPT/13/77/H (2015).

[744] Privacy Internation v Secretary of State for Foreign and Commonwealth Affairs & Others, IPT/15/110/CH (2016), there have been subsequent developments in this case, following on from this legal determination, which are not relevant for present purposes.

[745] 'Privacy and Security: A Modern and Transparent Framework' (Intelligence and Security Committee, 2015), http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf.

by the government's 'terror law watchdog', David Anderson QC.[746] These disclosures and reports were sufficient to make the collection and analysis of bulk datasets sufficiently 'foreseeable'.

In relation to sharing intercepted data with other governments, the IPT also ruled that any such activity had hypothetically been unlawful, but had been made lawful on the day of the first determination in the case, which addressed the legality issue. It was remedied not because of the publication of governmental information, but because of the Tribunal's own decision, the same one in which it formally found that the practice had been unlawful. The judgment explicitly referred to itself as the vessel by which information on intelligence-sharing, and the procedures governing it, came to public attention. Intelligence-sharing was unlawful until the moment that the IPT found it unlawful. The text was both the medium of legal review and the medium of legal remedy, both a normative assessment of the situation and a factual intervention into the situation. The law altered its informational environment in the process of assessing it. Here, the line between secrecy and publicity was mobilised and redrawn through its assessment. The distinction that the IPT had to draw in order to consider the law in the first place re-entered the process as information, in the sense of a "difference that made a difference".[747] The legal distinction between publicity and secrecy was both the condition of making a decision and altered by the decision.[748]
The IPT determined that it had been illegal and in doing so, paradoxically, made it legal.

What shifted was the line of the secrecy-relationship inscribed within the legal system itself. The device of 'assumed facts' effectively insulates interception practices from consideration. There will never be another interception warrant sealed in an envelope on the bench, on the cusp of revealing its secrets. Even a finding of illegality is enough

[746] Anderson, 'A Question of Trust'.

[747] This is Gregory Bateson's definition of information, see Luhmann, *Social Systems*, 40.

[748] Bernard Keenan, 'Going "Below the Waterline": The Paradoxical Regulation of Secret Surveillance in the UK', SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 1 March 2015), http://papers.ssrn.com/abstract=2583806.

to erase any pathologies that may emerge. All such legal processing operations are hermetically sealed within the law itself, which assesses itself in terms of the information it transfers to the public domain. Law assesses itself by standards derived from the function of the mass media.

As the IPT has made clear, the question of 'foreseeability' is measured by the fact of publication of information about legal rules and processes. Legislation, Codes of Practice, official guidance notes – the processing of these media converted illegality into legality before the IPT. They produced foreseeability – which has nothing to do with cognitive foresight, but is entirely determined by the availability of information in the 'public domain'. This confirms the fictitious status of the 'public' as constructed by the law which, simply through the publication of a judgment by a tribunal, suddenly achieved foresight previously lacking. If one were to seek out cognitive foresight and measure its sources, it is perhaps more likely to have arisen as a result of the mass media reporting of Edward Snowden's disclosures than any documents promulgated by the Home Office or the IPT.

5.6. Conclusion: legislating against surprises

Transforming legislation from a source of risk into a publicity-management device inevitably meant producing a secrecy-effect in the law, to insulate legal attention from arcane techniques. Both the Interception of Communications Act 1985 and the Regulation of Investigatory Powers Act 2000 were deliberately drafted to obfuscate the practicalities of the interception of communication; they provide a legal framework composed in an abstract and complex manner, and which reveals almost nothing about the powers they supposedly govern.[749] They reveal nothing about the materiality of interception techniques but simply abstract the issue by specifying requirements and protocols for the production of interception warrants. The warrant, as it was before Megarry, marks the distinction between legal process and interception

[749] A list of quotes from senior judges describing the difficulty of understanding RIPA can be found in, Graham Smith, 'Future-Proofing the Investigatory Powers Bill', accessed 28 January 2017, http://www.cyberleagle.com/2016/04/future-proofing-investigatory-powers.html.

techniques and at the same time couples them together. Where the warrant has been manufactured according to the prescribed formulae, all that follows shall be lawful.

Snowden succeeded in terms of transforming the parameters of 'public' discussion about interception powers. They ultimately caused a rapid increase in the amount of publicly available information regarding interception. In the UK, more information was released as legal challenges were brought before the IPT. During some proceedings, government lawyers stated that some 'assumed facts' were to be formally 'avowed'. Occasionally they issued previously-classified documents, with some redactions. Over three years, there was an unpredictable and unplanned amount of information passing from "below the waterline" into publication. This line of cases is not discussed in detail here, but must be reserved for another article.

In 2015, the government proposed legislation to replace RIPA. The Home Secretary has called the Investigatory Powers Act 2016 "world-leading legislation that provides unprecedented transparency and substantial privacy protection".[750] She may have in mind the detail of the legislation, which contains 272 sections divided into nine parts, each of which deals with a separate topic. In this respect, it is the antithesis of the legislation it replaces. Privacy campaigners disagree. Where government promotes the structure of the legislation itself, they focus on the political implications of the techniques that the Act authorises, which include all of the practices that Snowden revealed. There is nothing in the Act that curtails the technical capacities reserved for the government.[751]

Viewed through the lens of mass media, however, the debate about whether the legislation is 'transparent' or 'repressive' is beside the point. Snowden's disclosures unfolded in the mass media. There is a documentary, *Citizenfour*, directed and filmed

[750] Amber Rudd, cited in Burgess, 'What Is the IP Act and How Will It Affect You?'

[751] Ibid.; 'UK Parliament Passes Most Extreme Surveillance Law in UK History'; Liberty are challenging the legality of the Act itself in relation to European Data Protection Laws, see Armour, 'Liberty Gets Go-Ahead to Challenge Snoopers' Charter in the High Court'; Alan Travis, 'Tribunal Says EU Judges Should Rule on Legality of UK Surveillance Powers', *The Guardian*, 8 September 2017, sec. World news, http://www.theguardian.com/world/2017/sep/08/snoopers-charter-tribunal-eu-judges-mass-data-surveillance.

by Laura Poitras, the first journalist Snowden contacted about his planned disclosures. It captures the moment she first met him.[752] His delivery of material to her and the journalist Glenn Greenwald, and his subsequent escape from Hong Kong to Russia, self-consciously unfolded under the observation of the mass media. Whereas Malone's High Court case began with an accidental disclosure of evidence before a criminal court, the fictionalised 'assumed facts' based on Snowden's disclosures before the IPT emerged through the mass media. For the campaigning groups involved in litigation before the IPT, the Tribunal was as much a place to generate publicity, force further disclosures, and thus compel legislative change as it was a place to seek justice – which, in any event, could only be delivered hypothetically.[753]

It is therefore unsurprising that the outcome of this strategy is equally attuned to the observations of the mass media. The Investigatory Powers Act 2016 (IPA) can most clearly be differentiated from the Regulation of Investigatory Powers Act 2000 (RIPA) by its textual redundancy. Both pieces of legislation translate the data transfer operations of digital media into the symbolic order of the law. But whereas the textual interface provided by RIPA, when it addressed itself to the 'public' at large was enigmatic and ambiguous, its replacement is demonstratively clear. Where RIPA was drafted in a deliberately abstract and minimalist form, the IPA lists categories of different technical operations available: interception of communication in transit, acquisition of stored communication data, the use of bulk datasets, and so on. Whereas RIPA authorised powers according to minimally-stated, abstract formulations, positioning clauses regarding 'safeguards' in different parts of the text to the powers they 'safeguarded', and so on, the IPA has a large degree of textual redundancy, repetitively restating the same procedural qualifications for each type of operation.

[752] *Citizenfour*. (2014). [DVD] Directed by Laura Poitras. Germany: Praxis Films

[753] This is based on personal observations during the period concerned – a formal research project is planned.

Snowden's revelations were highly informative in the sense that they were highly surprising. For the mass media, information is by definition surprising.[754] Once information has been processed by the mass media, it is no longer surprising. It is already known, and thus redundant. Information (surprise) is transformed into redundancy simply by entering the 'public' domain. Many paragraphs of the IPT's judgments in its post-Snowden determinations are devoted to explaining how the 'assumed facts' derived from the Snowden archive were indeed authorised by RIPA's enigmatic formulations. Only where the legal technique of analogy could not succeed in explaining assumed facts by reference to existing legislation did the IPT rule that such hypothetical scenarios had been unlawful – at least until, via the IPT's own process that put 'Codes of Practice' and 'arrangements' into the public domain, more surprising information (but not particularly interesting information) was disclosed, thereby making the practices referred to hypothetically lawful. The surprises had to be made non-surprising to be made lawful.

Despite naming the various categories of techniques that Snowden revealed and enfolding each category into a framework of authorisations, time-limits, and other prescriptions, the Investigatory Powers Act 2016 is not informative. It discloses no information that Snowden had not already addressed to the mass media, and that the mass media in turn disseminated, transforming unknown and unforeseeable secrets into cognitively foreseeable knowledge with each publication. Once published and disseminated, the classified information entered the 'public domain'. The Investigatory Powers Act converts what mass media made cognitively foreseeable into legislation, thus making it legally foreseeable. Its content is derived not from any normative standards about privacy, but from information provided by the mass media.

This allows us to assess RIPA by reference to the distinction between *variety* and *redundancy*. RIPA contained little information about the processes of interception that

[754] This equation applies to Luhmann's model of social systems generally, Luhmann, *Theory of Society*, 2: 44-48; the observer-dependency implicit in this definition of 'information' is indicative of what makes Luhmann and Kitter difficult to theoretically reconcile.

it authorised in law. In systems theoretical terms, we can say it was high in variety. Redundancy and variety are opposed, in that:

> redundancy involves the information that is available for the processing of information, and variety is the information that is as yet missing. The greater the variety of a system, the more difficult it becomes to use one operation about which there is little information to draw conclusions about other operations [...] and the more surprises there are to be generated.[755]

RIPA was high in variety, the IPA is high in redundancy. The legislation's high level of textual redundancy serves to close down the possibility of being surprised by more information in the future. RIPA had a surprisingly large variety of meanings 'below the waterline'. The effect of the legislation is not to create 'world-leading legislation', in the Home Secretary's media-minded, legally meaningless formulation. It functions as publicity management, forming a shield against the risks of further disclosures and thus the publicity effect generated by surprises and secrets. It does this by narrowing the possible variance of future meanings latent in the law.

Paradoxically, by making more legal rules, the legislation narrows the potential for future legal action. Legislating for interception powers neither constrains operations nor makes them 'accountable'. Ultimately, it serves to reiterate a much older fiction – that interception is attributable to subjects. In so doing, law makes them redundant as factual categories in order to safeguard their operational unknowability. Secrecy of the *arcana* as they operate in practice depends on constraining surprises, which are akin to the *secretus* – the knowledge that there are secrets. Today, the *arcana* of state are not protected through absolute prohibitions on speaking about them, but through speaking about them in great detail, via legislation. Law is thus determined by the reality of the mass media, which it has come to equate with foresight.

If the legislation functions, we shall not hear much more about interception beyond what the law already makes public: that the Secretary of State remains in charge, and that audited statistics are available on governmental websites. If the law fails, we shall

[755] Luhmann, *Law as a Social System*, 320.

not know in advance. We can only wait until we are surprised by the next unexpected leak of arcane information, which will necessarily refer to new interception techniques that are presently unforeseeable.

6. Conclusion: Silicon Sovereignty

6.1 Digital warrantry

The Snowden archive of leaked documents include a set of PowerPoint slides on 'warrantry', created in November 2008 by GCHQ's 'Operational Legalities' team to deliver training to intelligence officers.[756] The team exists to "enable SIGINT" by providing guidance and assistance with warrant applications; developing policy; taking decisions regarding the disclosure of secret files and documents; and 'implementing' legal processes.

As of 2008 when the slides were created, there were four pieces of UK legislation that directly affected the so-called 'warrantry' associated with GCHQ's operations. They were the Intelligence Services Act 1994, the Human Rights Act 1998, The Regulation of Investigatory Powers Act 2000 (RIPA), and the Wireless Telegraphy Act 2006. The Intelligence Services Act 1994 placed the UK's existing foreign intelligence agencies, GCHQ and the Secret Intelligence Service (MI6), onto a legal footing. It states that their function is to serve the following three purposes: the protection of national security, the maintenance of the economic well-being of the UK, and the prevention or detection of serious crime. These purposes are identified and formalised in practice by the Joint Intelligence Committee (JIC).[757] The Intelligence Services Act 1994 also provides warrants and certificates authorising 'interference' with property in the UK or overseas, which secretly formed the basis for tactics such as 'equipment interference' and 'computer network exploitation' (CNE). These are more commonly known as 'hacking' computer systems and networks, essentially to make them perform operations that are imperceptible to their immediate users. The Human Rights Act 1998 gives direct legal effect to the European Convention on Human Rights

[756] The slides date from November 2008 and were first published in June 2015, 'Operational Legalities - GCHQ' *Snowden Doc Search*, https://search.edwardsnowden.com/docs/ContentorMetadata%3F2015-09-25nsadocs.

[757] 'Joint Intelligence Committee - GOV.UK', accessed 12 September 2017, https://www.gov.uk/government/groups/joint-intelligence-committee one of the Committee's stated purposes is: 'to contribute to the formulation of statements of the requirements and priorities for intelligence gathering and other tasks to be conducted by the intelligence agencies.'

(ECHR), meaning that any interference with the right to respect for private life has to be in accordance with law, must be necessary within a democratic society, and must only involve action that is proportionate to the particular ends. The Wireless Telegraphy Act concerns intercepting or interfering with radio transmissions, while RIPA provides the main legal footing spelling out the circumstances and conditions under which interference with private communications can be authorised, via an interception warrant or analogue form of authorisation. To take effect, these legislative enactments have to be translated into processes.

There are a wide range of legal descriptions of various technical operations that GCHQ's legal experts must be aware of. However, we shall focus on the interception warrants available under RIPA, which serve as useful examples. There are two types of interception warrant available, determined by the territorial dimensions of targeted communications. Under section 8(4) warrants, 'external' communications may be intercepted. External communications are those in which the sender or receiver is located somewhere outside the British islands. A section 8(4) warrant's function is to provide "an intelligence gathering capability".[758] As such, it need not specify a human target. In fact, the warrant's targets are specified pieces of communication media, described in technical terms as 'communications bearers'. Bearers that may be targeted include submarine fibre optic cables, earth stations for sending and receiving satellite transmissions, or wireless relay masts.

Using a section 8(4) warrant means that all 'external' communications, including both the content and metadata, can lawfully be collected in their entirety from a targeted bearer. However, intercepted material can only be subject to 'human examination' provided an element of its semantic content matches against a 'selector' term. Selectors are, by analogy, a reconfiguration of the list of targets formerly provided to human interceptors. All selectors must be listed on a certificate that must accompany each section 8(4) warrant in order to validate it. The certificate contains the list. It provides "descriptions of intercepted material the examination of which [the Secretary of State]

[758] 'Report of the Interception of Communications Commissioner: Annual Report for 2015' (IOCCO, 8 September 2016), 31, http://iocco-uk.info/docs/56850%20HC%20255%20ICCO%20Web%20only.pdf.

considers necessary".[759] The certificate and the warrant both must be signed by the Secretary of State in order to be validated.

By contrast, a section 8(1) warrant is required for all communications 'internal' to the British islands. The warrant must name a particular person or particular premises as a target, and it must also provide details as to the background of the case, how it connects to the target, the methodologies to be employed, why the operation is both necessary and proportionate to its ends, any 'collateral' intrusion into the privacy of others that may result, any particularly 'sensitive' factors involved such as medical, religious, journalistic, or legal confidentiality; and any particularly urgent factors. The applicant must also provide written assurances that all collected data will be lawfully handled and disposed of.[760] While the warrant itself, and any renewal, must be signed by a Secretary of State, each warrant made under section 8(1) must include a 'schedule' that provides granular operational details. Schedules can be modified without requiring the Secretary to re-authorise the warrant, for instance where a target changes his mobile phone for another.

When commercial communication service providers are served with a warrant and any relevant parts of the schedule needed to implement it, they are required to enable the interception to proceed. GCHQ can in turn be served by schedules requiring it to facilitate interception on behalf of other government or police agencies, and the legal department advises staff to insist on seeing the full schedule before taking any action; otherwise the Interception of Communication Commissioner has to be informed of a breach of the law. As one slide emphasises, "Say: No schedule No targeting!"

Section 8(1) warrants therefore require detailed prior knowledge of the target. Whereas section 8(4) warrants are about gathering intelligence overseas on an open-ended basis, section 8(1) warrants are investigatory tools. The two types of warrant therefore inscribe different temporalities into technical interception operations in relationship to the information they produce. Furthermore, the difference between the

[759] Regulation of Investigatory Powers Act 2000, Section 8 (4)(b)(i).

[760] 'IOCCO Annual Report 2015', 24–25.

warrants must also take effect on a material lever. The architecture of the internet is such that data packets are routed by TCP/IP protocol between servers on a heuristic basis. National borders do not determine the transmission decisions made by servers in the ordinary course of operations. Online communication that is both sent and received within the UK, therefore, could be routed via overseas servers, and therefore packets of data pertaining to 'internal' communications are inevitably collected as they transit bearers targeted by section 8(4) external warrants. The law holds that such data cannot be examined only on the basis of it containing selectors. It is protected by the territorial location of the sender and receiver, which are machines, not people, located within the British islands. Any such communications pertaining to 'internal' individuals must be specifically targeted, or the material cannot be examined.[761] But in order to operationalise this distinction, the difference between 'internal' and 'external' packets of data must be established by examination. The IP addresses of sender and receiver, provided they are not disguised, indicate the country within which communicating devices are located.[762] All communications on a bearer must be collected in the first instance, and algorithmically sorted so as to eliminate packets that cannot lawfully be examined. In physical terms, interception is a reductive process of elimination from a 'buffered' total collection. This is not simply a legal protocol but an inflexion upon an operationally necessary process, as the totality of data collected is full of irrelevant or redundant data and must undergo a 'Massive Volume Reduction' process to be made useful.[763]

All warrants are formally addressed to the person who makes the application to the Home Secretary. There is a prescribed list of possible applicants; for each agency, it is the most senior official in that agency. For GCHQ, then, only the Director formally 'makes' a warrant application. The warrant symbolically couples the office-holder of an agency with the office-holder of a ministry. All warrants must be signed

[761] This is the effect of section 16, Regulation of Investigatory Powers Act 2000.

[762] IP addresses are assigned within certain 'ranges' for each country, see IP2Location, 'IP Address Ranges by Country', *IP2Location*, accessed 26 September 2017, http://lite.ip2location.com/ip-address-ranges-by-country; the coupling of protocological standards to nation states has been addressed, in a somewhat dialectical fashion, by Galloway, *Protocol*, 121.

[763] 'GCHQ Problem Book', 10.

‘personally’ by a Secretary of State, although there are no rules specifying the media to be used to personally constitute her signature.[764] Interception warrants are signed by the Home Secretary for domestic purposes, and the Foreign Secretary for oversees purposes, but the Defence Secretary, the Secretary of State for Northern Ireland, and the Cabinet Secretary for Justice in Scotland may also sign interception warrants.[765]

Legal authorisation has three functions, according to the Operational Legalities presentation slides. First, it ensures compliance with the positive obligations of human rights law, such that any interference with privacy is carried out lawfully. Second, it is necessary because interception and other GCHQ activities, such as hacking into computer systems, is straightforwardly a criminal offence otherwise, and “civil servants are not immune from prosecution”. Finally, authorisation “gives visibility of operational activities to GCHQ seniors and [the Secretary of State]”, meaning that all operations can be referred to official governmental policy and can be reviewed accordingly by management for efficacy. Everything GCHQ does in pursuit of its functions has to be “authorised, necessary, and proportionate”; with the latter described as the “most challenging” part of each application. Rather than a full legislative exposition, the aim of this section is to highlight how these elements of legislation are folded into the production of warrants.

6.1.1 External warrants

The computer software used to interface with intercepted material in 2008 was, and perhaps still is, referred to as Corinth/UDAQ (Unified Data Access and Query tool). It is a portal, it controls access. In passing through the portal, an intelligence analyst passes through the law. If one cannot pass through the portal, one cannot enter the privileged position of interception.[766] The interface contains fields that are specifically

[764] ‘IOCCO Annual Report 2015’, 17–18; ‘Interception of Communications Code of Practice’ (Home Office, January 2016), 24, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf.

[765] ‘IOCCO Annual Report 2015’, 18.

[766] A GCHQ presentation on interception concludes by reminding analysts that they are in an ‘enviable’ and ‘privileged’ position – ‘you have access to a lot of sensitive data… have fun and make the most of it’ ‘Access to

set up “for legal compliance reasons”.[767] They cannot be avoided, and are a necessary precondition for carrying out any operation that accesses intercepted data, or that initiates interception.

To gather data for ‘external’ section 8(4) purposes, an intelligence analyst adds selector terms to the lists that must be appended to a warrant’s certificate, or set of certificates. Because no individual or premises need be known in advance, they can add selectors on the basis of thematic topics. The list of selectors on each certificate is updated on a rolling basis, while the warrant covering the communications bearer itself remains in force. In 2008, when the training slides were made, there were ten certificates in effect, including one ‘global’ certificate for all GCHQ signal processing operations around the world. The rest are assigned individually to particular “special source access” sites. This seems to indicate that the certificates function on an administrative logic, rather than legal: a ‘global’ certificate legalises operations universally, but not all selectors are useful in all locations. As such, local certificates are used to differentiate locally interesting topics.

Apparently, a sample certificate was passed around during the session, which further suggests that analysts do not normally see the certificates. In other words, while certificates must contain a formal list of terms that describe the themes being searched for, they exist as an element in the formal legal paperwork, a nexus of legal media that couples the Operational Legalities team to GCHQ’s senior management, and on to government ministers. The certificate is a legal document that draws lines between elements in a complex organisational hierarchy. Analysts, however, do not normally use the certificate as such. They interact with selector terms not on paper, but through the UDAQ interface. According to the training notes, this procedure ensures that “individuals’ ECHR rights are protected on a world-wide basis” by tying them back to the legal framework encoded into the portal.

the Future’, *Snowden Doc Search*, 21 June 2013, https://search.edwardsnowden.com/docs/Accesstothefuture2013-06-21_nsadocs_snowden_doc.

[767] ‘Operational Legalities - GCHQ’.

6.1.2 The portal

The image in figure 17 is a screenshot of the UDAQ interface, taken from the training slides (the resolution is less than ideal). We can discern some instructive features. First, the interface has been accessed via Microsoft Internet Explorer, "provided by GCHQ", and the browser address bar is directed to a redacted website using the encrypted 'https' protocol (Hyper Text Transfer Protocol Secure). This protocol is commonly used for web-based financial services and other sites that require secure encryption of traffic. One of the systems used to generate encryption keys for such services was compromised by the NSA, as discussed in the introductory chapter.[768]

The secure web address suggests that gaining access to the portal to work with intercepted material via UDAQ is possible via the internet. Provided that Internet Explorer is configured correctly and the user has logged in securely, it appears that analysts can access GCHQ's internal network from any internet connection, making the delivery of intercepted data subject to the same protocols that enabled the interception of that data. However, it could equally be the case that access is limited to fixed terminals within GCHQ and allied states' installations.

The 'Source' tab on the interface offers two options, 'intercept' and 'opensource'. On the screenshot in figure 17, 'intercept' is selected. Presumably, 'opensource' data is less interesting for training purposes, as it likely refers to information that has been gathered from websites and other 'open' sources of published information rather than interception, and therefore no warrant is required to access it. The interception tab offers three checkboxes, which seem to correspond to codenames for sources of intercepted data.[769] Below, the 'Search Terms' tab offers a textbox for entering keywords and drop-down menus for setting the parameters within which the search is to be conducted. Presumably, results would be offered in the unmarked space below, which offers either 'structured' or 'freeform' views.

[768] Landau, 'Highlights from Making Sense of Snowden, Part II', 63; see 1.1.

[769] A 'counterveillance' blog (my ascription) containing a useful 'opensource' list of such codewords is available at 'GCHQ Codewords and Abbreviations', accessed 20 September 2017, http://electrospaces.blogspot.com/p/gchq-nicknames-and-codewords.html.

On the right of the screen is the ‘Properties’ tab, which we shall return to below. Below ‘Properties’ is the HRA (Human Rights Act) justification section, which requires entry of a ‘Miranda’ number, with the label ‘JIC priority’ next to it. According to the training slides, the Miranda number “equates to [an] intelligence requirement”. The number refers to a centralised list of political priorities for the UK’s intelligence services as a whole, set by the Joint Intelligence Committee of the UK Government.[770] This, then, is what makes a given query qualify as ‘necessary’ for the purposes of human rights law, which stipulates requires that all intrusions into privacy must be “necessary in a democratic society”. The Miranda number includes such standards in every operation; it addresses itself to the legally-mandated question of ‘necessity’. Individual GCHQ intelligence analysts are neither qualified nor required to make necessity judgements, they just need to include a valid and relevant Miranda number.

To enter a valid selector term, the analyst must provide a short ‘justification’. According to the training materials, the intended target of a particular selector term may be human or non-human. For instance, it could be aimed at detecting the communications produced by a software-based ‘bot’. But because the data that is returned does not discriminate between human users except according to location, the analyst will inevitably see data attributable in some sense to humans. As such, the human rights justification box must be populated with some semantic textual explanation as to why that is to be so. This entry, the trainers emphasise in their slides, cannot simply repeat other factors entered elsewhere, but should connect the selector term to a wider justificatory strategy. Each selector has to be justified by the analyst using it.[771]

Certificated selectors take effect by populating a database called ‘Broad Oak’. Broad Oak is a ‘strategic target’ database. The database is distributed, meaning that it is copied to memory systems at all GCHQ sites where any ‘external’ communication bearers are intercepted. As described above, the technical effect of a section 8(4)

[770] ‘Joint Intelligence Committee - GOV.UK’.

[771] ‘Operational Legalities - GCHQ’.

warrant is that all data packets passing through the targeted bearer are lawfully copied to a temporary memory system, known as a 'buffer'.[772] Once the data has been purged of uninteresting types of data packet, the packets are reassembled into communications, referred to as 'sessions', and semantic content of each communication is inspected with reference to the active selector terms in the Broad Oak database. If data packets contain content that matches an active selector, that content is collected for processing and analysis. 'Selection', paradoxically, is realised by selective forgetting. The legal act of 'selecting' is performed in a subtractive process of elimination; everything that has not been authorised to be retained is deleted. However, this only applies to packets of semantic content. All collected 'traffic' data is universally collected and stored, compiling a map of all 'external' communication links observed in the system.

From thematically defined 'seed' selectors that are generally applied across the buffer, information thus emerges and offers itself as the basis for further enquiries.[773] The training notes state that the selectors listed on a certificate need not be precisely the same as the selectors an analyst enters into Broad Oak. The certificates do not require the same granularity used in actual operations, but need only list "general categories of material" that "broadly mirror" the intelligence priorities set by the Joint Intelligence Committee. In practice, analysts can go beyond those legally certificated terms when actually implementing selectors, which means there is a distinction between the formal entries on the certificate and the operational entries that may follow. Despite being coded into one interface, law and intelligence analysts still obey different logics, and thus remain elements in two different registers even as they are co-produced.

[772] Technical details have been leaked and published independently of the Snowden archive, see Ryan Gallagher, 'The Little-Known Company That Enables Worldwide Mass Surveillance', ***The Intercept***, accessed 23 October 2016, https://theintercept.com/2016/10/23/endace-mass-surveillance-gchq-governments/.

[773] The process summarised here is more complex and requires patient analysis of Snowden documents to understand, see generally 'Tempora - GCWiki Entry'; 'GCHQ Problem Book'; 'Special Source Access (Supporting Internet Operations) - GCHQ Presentation', 2010, ***Snowden Doc Search,*** https://search.edwardsnowden.com/docs/SupportingInternetOperations2015-09-25nsadocs; 'XKeyScore - NSA Presentation'; for a summary, see Greenwald, ***No Place to Hide***.

Figure 18 shows the results: a screenshot of UDAQ, displaying the features of an active selector. The HRA justification entry states: "SUSPECTED OF PRCOCURING ARMS FROM IRAN IN CONTRAVENTION OF UN SANCTIONS". This second screenshot is an example taken from the Broad Oak database, the logo appearing in the top left of the image. This particular selector, the semantic content of which is blanked out in the slideshow, was to be applied only to email traffic, thereby narrowing the processing requirements. On the completed selector screen in figure 18, there is a visible Miranda number, a JIC 'priority code' in a separate box, and a date set for 'HRA review' (that is, presumably, a Human Rights Act-mandated review). Furthermore, there is a reference code specifying the 'Legal Authorization for Target'. This code number is most likely the reference number against which the term appears on all relevant certificates and warrants, bearing in mind that it could be applied on any of the ten active certificates that were then in force. At the bottom, the list shows the interception locations where the selector is active.

Where the justifications for a selector term no longer apply, the reasons for removing it from the list of active selectors must be recorded and the selector deactivated in the Broad Oak network. If an overseas target enters the UK, there is a five-day window in which interception can continue while the analyst obtains a section 8(1) warrant that will subsequently authorise the continuing process, superseding the section 8(4) authorisations used while the target was abroad.[774] The Operational Legalities team advise that they are available to help convert any ambiguous cases into an "appropriate format". For instance, where no specific information is known about a topic, such as any specific names, devices, or locations, GCHQ bulk databases can be analytically mined to produce targets, but doing so requires senior official approval. The slides stress that the 'belief' element required of analysts – for instance, where they believe the target to be located, what they believe the situation to be that justifies interception – does mean "100% knowledge with hindsight". While operatives should not "turn a blind eye" to inconvenient data, they should nonetheless always be

[774] The legislation is complex, but see also section 16(3) Regulation of Investigatory Powers Act 2000.

confident in proceeding on the basis of available knowledge at the time. What matters most, the training says, is always recording the reasons for doing something. Even if an assumption is later proved incorrect, the interface generates a trail of evidence to demonstrate to the "good faith" reasons for the initial "judgement call".

6.1.3 Internal warrants

For any interception operation targeting persons or premises located within the British islands, a RIPA section 8(1) warrant must be in place. The unified system for lawful interception within the UK is called the Preston system. In a 2007 document describing its architecture and functions, it is described as follows:

> PRESTON collection is the warranted intercept of all UK line access. It covers fixed and mobile communications; and voice and data. Each target must be covered by a RIPA 8(1) warrant. GCHQ is one of eight intelligence and law enforcement agencies involved in this type of collection.[775]

The document provides details of the logical architecture of the system's ability to intercept, process, and store communications via 'streams' that are copied via a one-way link from commercial 'communication service providers' in the UK, all of whom must, by law, co-operate with section 8(1) warrants. Here we shall briefly review the "Use-Case view" section of the document, which describes how intelligence analysts, rather than systems engineers, interact with the architectural environment of Preston. It describes

> how the actors apply a formal process to achieve the interception. In short, the process covers preparing a case for interception, application for a warrant, warrant review, and (if successful) the provisioning of communication intercept.[776]

[775] 'Preston Architecture - GCHQ' (The Intercept, 5 July 2007), 5, https://theintercept.com/document/2016/06/07/preston-architecture/.

[776] Ibid., 11.

To enable interception, both an "intelligence analyst" and an "interception authority" must be in place. As the document explains,

> the process is compliant with RIPA, as no communication interception can occur without a warrant in place. The RIPA requirements ensure compliance with HRA, in particular, the case for interception must be strong for the warrant to be obtained.[777]

The approval of a warrant is the result of the procedural confirmation of its lawfulness. The procedure is graphically rendered in figure 19**.** The so-called "business process" does not only ensure lawfulness, it also integrates the technical process of "stream routing" into "collection or survey" systems. A collection system is used where a data stream requires no technical analysis before it is presented to an intelligence analyst; for instance, the recording of a voice call. A survey system is one that disentangles a complex data stream into component elements, where the initial structure of the data is not already understood. After all; "the internet is flexible, and supports a myriad of protocols, so a more complex process is used".[778] Working in tandem, the intelligence analyst and the tasking manager ensure that all streams operationalised by GCHQ are confirmed to be of value, and so are kept 'on stream' only for so long as operationally necessary (figure 20**)**. This way, the technical application of interception processes and the intelligence analysis are coupled together via the medium of the warrant, which at the same time confirms the legality of all such collaborative operations.

The Corinth/UDAQ interface shown in figures 17 and 18 is, or at least was, used for adding 'selectors' to Preston.[779] As with external communications, the routines were coded to ensure the intelligence analyst, as the functional 'user' of the interface, can only interact with the Preston system in accordance with the law. But, as the Preston Architecture document makes clear, this alone does not describe how the data is

[777] Ibid.

[778] Ibid., 12–13.

[779] Ibid., 15.

intercepted, parsed, or made available for analysis.[780] There are more complex processes involving systems administrators and collection managers, but these do not concern the legalities that centre on the intelligence analyst.[781] The arrangement is summarised in the chart shown in figure 21.

6.1.4 Legalities table

It should be emphasised again that we have dealt with the interception of the 'content' of communication here, rather than also including the position in respect of 'communications data', more commonly referred to as 'metadata'. A document from 2007 provides a simplified breakdown of the legal situation under RIPA regarding the content and metadata of intercepted communications as determined by the location of the target. As can be seen, RIPA permits the collection of all metadata without warrant (figure 22).

The table refers to a second distinction, that of 'Second Party' locations or nationals. Second party nations are the members of the 'Five Eyes' alliance: the UK, US, Australia, Canada and New Zealand. To intercept material covered by the legal systems of those states, no warrant is required, but 'STA' is.[782] STA stands for 'Sensitive Targeting Authorisation'.[783] It has subsequently been replaced by COPA (Combined Policy Authorisation), through which the close SIGINT allies coordinate their activities.[784] This can involve different operational distinctions. For instance, unlike the UK's legal system which legally differentiates data according to its

[780] For the technical side of the Preston system, see ibid., 21–40 the codewords are, of course, difficult to decipher without further resources in the Snowden archive.

[781] 'Preston Business Processes - GCHQ' ***Snowden Doc Search***, 18, https://search.edwardsnowden.com/docs/PRESTONBusinessProcesses2016-06-07_nsadocs_snowden_doc.

[782] 'Legalities Table - GCHQ' ***Snowden Doc Search***, https://search.edwardsnowden.com/docs/Legalities2015-09-25_nsadocs_snowden_doc; An operational flowchart of the warrantry regime summarises the overall position, see 'Legal Authorisation Flowchart - GCHQ', ***Snowden Doc Search***, https://search.edwardsnowden.com/docs/LegalAuthorisationFlowchartsTARGETINGandCOLLECTION2015-06-22_nsadocs_snowden_doc.

[783] 'GCHQ Codewords and Abbreviations'.

[784] Ryan Gallagher, 'From Radio to Porn, British Spies Track Web Users' Online Identities', ***The Intercept***, accessed 10 October 2016, https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.

territorial points of transmission and reception, the US legal system attaches rights to individual citizens. US citizens must therefore be eliminated from intercepted datasets in a subtractive process. While on a semantic level this indicates a higher degree of legal protection for US citizens, conversely, it requires some prior set of stored and reliable connections between the IP address of a given device and the nationality of its user. To avoid surveillance under these conditions, a US citizen's electronic devices must already be known, stored, and indexed to their identity in internationally distributed government databases.

Returning to figure 17, in the 'Properties' tab of UDAQ, the analyst must name their specific query and indicate its classification status. There are options on a menu in which one can specify a particular country in the 'Five-Eyes' alliance. This indicates that other nation's analysts may interface with and use UDAQ. The 'Properties' tab appears to be designed for producing a 'Targeting Protection Security Label', an example of which is seen near the bottom of the interface in the following image of a completed selector. The label indicates to anyone within the 'Five-Eyes' alliance the classification status of the selector and, perhaps, whether or not they are permitted to access material generated by it. Within the global network of shared interception systems, each nation can still keep some things from its partners.

The five national agencies all make data available to one another, with the caveat that they all respect one another's legal arrangements. For instance, in order to access NSA databases, GCHQ operatives require a special license with 'STA' approval. According to the training slides, such a license is easy to obtain. In 2008 at least, it involved an "open-book exam" with multiple-choice questions, presumably on the basic application of US constitutional law and rules derived from the Foreign Intelligence Surveillance Act 1978 (FISA), or rather, the interfaces through which the NSA operationalises those rules. Only the category of 'other', that is, everyone else in the world, can freely be targeted under the broad range of generalised selectors added to Broad Oak through the medium of a section 8(4) warrant and certificate.

6.1.5 Dissemination and audit

The dissemination of intelligence produced from intercepted material must be channelled via the National Technical Assistance Centre (NTAC), part of GCHQ.[785] The Operational Legalities notes state that a single interface system is in place for "passing intelligence to customers", that is, to anyone outside GCHQ. The training emphasises that emailing someone with classified intelligence is a bad idea; doing so can lead to prosecution. Deciding on the content of an intelligence report requires a separate legally-mandated proportionality assessment, in addition to the one that generated the intercepted material in the first place. There is a proportionality assessment when deciding what data to examine, and another when deciding what observations derived from intercepted data can be disclosed. Data no longer required for operational purposes must be destroyed, and data use must be minimised; the guiding principle is that private data is looked at, copied and disseminated as little as possible. Errors leading to breaches of law or policy have to be immediately reported, and in any case, it would be much worse should mistakes covered up later emerge on audit. The analyst thus interfaces with the world via another closed system, that imposes a different set of legal requirements.[786]

All activities carried out in this digital environment are subject to audit. Each year, a percentage of all entries are randomly selected and checked by the Interception of Communication Commissioner's Office (IOCCO). Each domestic section 8(1) warrant entry is checked individually, alongside a random selection of the more numerous 'externals'. The inspectors sample all data sets and can personally observe the use of interfaces and data by various agencies.[787] There is an ongoing audit process, conducted on all agencies that utilise any of the powers granted in RIPA, and generalised results are published annually. Every operation carried out is fully recorded and attributable. As each operative in GCHQ is constructed as a user of an

[785] 'The National Technical Assistance Centre | GCHQ Site', accessed 8 July 2017, https://www.gchq.gov.uk/features/national-technical-assistance-centre NTAC 'manages the delivery of intercepted communications to the agencies that have a lawful authorisation in place to acquire them'.

[786] 'Interception COP', 41.

[787] 'IOCCO Annual Report 2015', 26–31.

interface, their persona is attached to every action they perform in the network. Every application for authority to act generates a unique reference ID that connects it to subsequent actions under the same warrant, making it possible to recombine data for legal compliance purposes. The inspection regime operates not only by inspecting individual warrants but by sampling data and running various mathematical analyses on it, looking for patterns that may indicate poor practice or insufficient consideration of legalities.

As Marilyn Strathern puts it, with auditing processes, reflexivity "sustains a judgmental and thus an ethical self."[788] We can, with audits, see auditing as an independent subsystem that reproduces itself through the accounts that it elicits from organisations. Auditees are "turned into ethical self-auditors – typically they do their own audit on themselves before the experts come in."[789] In order to do this, the complexity of the organisation itself has to be reduced to a few simplified critical differences that can capture the ethical moments – here defined by legislation – which can assure the auditors that all is, statistically speaking, carrying on in accordance with the law. Audits take effect via disciplining the correct application of procedures, rather than engaging substantively in retrospective assessments of normative decisions to intercept communication. Bluntly, it is about form and not content. In what sense has this enhanced the role of law? Strathern again:

> Now what makes audit virtuous is its power to purify the principles of (good) organization as such. Audit does not just produce auditees and auditors; it is an organization that produces trust in organization(s). Its own self becomes recognizable in the efforts others make to come up to standard… The practitioners (auditors) are ethical arbiters with guidelines to implement rather than social observers with a job of analysis to do. Audit keeps its own virtue through its own self-description as (the phrase is mine) an enabling technology.[790]

[788] Marilyn Strathern, 'Bullet-Proofing: A Tale from the United Kingdom', in ***Documents: Artifacts of Modern Knowledge***, ed. Annelise Riles (Ann Arbour: University of Michigan Press, 2006), 191.

[789] Ibid.

[790] Ibid., 192.

Strathern's notion of audit as an "enabling technology" is useful. Recall that in order to be legal under contemporary human rights law, any interference with personal privacy must be in accordance with the law, necessary, and proportionate. The interface itself is designed so that the only operations possible are in accordance with the law; the law is encoded into its architecture. Necessity is a political determination which is controlled by the use of JIC priority codes.

For an individual analyst, the legal variable that they must generate concerns the 'proportionality' of the particular operation. From a legal perspective, the key legal elements of the assessment are already in place: first, the legitimacy of interception in general is established by legislation; second, the necessity of the operation is confirmed by inserting the JIC priority code; third, the suitability of interception is inherent in the fact that it is the only way to access private communications. The interface, holding all other elements together, requires only the entry of a fourth element, the 'balancing' of the interest in the data against the interference with privacy that is presumed to follow.[791] It requires a statement that accounts for the contingency of the future anterior operation by assigning a normative value to the anticipated difference between the state of the situation before interception and the situation after; that is, to explain the anticipated outcome in normative terms.

The warrantry processes outlined above posit warrants as technologies that link together and enable a number of other processes. Not least, they designate and differentiate the symbolic roles of the Secretary of State and the requirements of the legal system, making possible the attribution of legal responsibility to her in the form of a decision to sign a warrant. However, what is presented to the Secretary of State to sign has already passed through the portal: her scope for 'decision' is intentionally narrow, given that she has no basis for second-guessing the applications presented to her. As the Interception of Communications Commissioner's latest report confirms, very few applications are refused because inadequate applications are corrected,

[791] These four elements are taken from a doctrinal overview of the concept of proportionality in constitutional law, see Kai Möller, 'Proportionality: Challenging the Critics', *International Journal of Constitutional Law* 10, no. 3 (1 July 2012): 711.

filtered out within the agencies before reaching the Secretary of State.[792] By the time it reaches her desk, the decisive elements are already in place.

Her authorisation validates the creation of an indexed reference number, in reference to which authorised operations are automatically recorded as digital 'files' for auditing. Data access, data retention periods, and intelligence dissemination are all similarly coded into the system. Making a warrant is impossible without entering data in a form that is already coded to these purposes, or, put the other way around, it is, as the annual statistics confirm, almost impossible to make an illegal warrant.

As Luhmann points out, the binary difference between legal and illegal is easy to institutionalise, provided one knows what is legal and what is illegal.[793] An institution that establishes its own procedures for interfacing with the world outside can in turn observe how those procedures appear when considered through the law; this is the self-auditing logic that Strathern describes. But to actualise this reality, so-called warrantry must be ascribable to the decisions made by GCHQ operatives and their political masters. Digital media, which can simulate and perform the operations of any other medium, transcribe the requirements of the law into media-technical procedures that control access to the privileged position media assign to interceptors.

Interception is a privileged position assigned by technical media. The warrantry process works not to restrain action but to legalise it.

6.2 Conclusion

To return to the founding question: can technical literacy produce laws that control interception? The answer is no, because interception has already superseded the law. Both interception and the law are symbolic ascriptions given to media-technical operations. Digital media, which can simulate all others, are capable of performing both interception and legal operations at the same time. The challenge is designing a

[792] 'IOCCO Annual Report 2015', para. 6.12, 7.5.

[793] Luhmann, *Law as a Social System*, 180.

suitable interface that directs the operations of the analyst, and allows them to occupy the position of 'user' who sees themselves as in control.

Technical literacy is no answer, because literacy is always already an effect of technical operations. As long as government actions were performed on paper, it was possible to believe that law could direct them. As Vismann and Krajewski show, this position is no longer sustainable. Interfaces were first designed by the NSA in 1971,[794] since then, access to intercepted data has been determined by the rules of computer architecture, not legislature.[795] Digital operations supersede legal operations.

Increasingly, as experiments in machine learning indicate, the reasons for adding selectors to the growing lists of interception targets are generated by machine-learning processes that filter and interrogate the agglomerated data derived from interception and related techniques.[796] Whether or not such processes are 'effective' is beside the point. The criticism that intelligence agencies collect 'too much' data to be functionally effective is weak criticism.[797] It only justifies further experiments in improving the efficiency of learning algorithms; which by definition requires more data than can be 'useful' for a prescribed end. The point is that the algorithm must learn to identify everything that is not useful.[798]

Moreover, arguments based on the empirical effectiveness of how intercepted data is used seek to ascribe a temporal process based on law to operations determined by media. Intelligence agencies cannot only collect the data that they will use, because it is humanly impossible to know ascribe meaning to data after it has been collected and inspected. Hence legal distinctions can only be applied to data after it has been collected. The fiction that the human analyst who, in adding a new selector term to

[794] Section 3.5.3

[795] Vismann and Krajewski, 'Computer Juridisms', 91–92.

[796] 'GCHQ Problem Book'.

[797] Glyn Moody, 'MI5 Collecting "significantly More" Data than It Can Use, New Snowden Docs Reveal', ***Ars Technica UK***, 7 June 2016, https://arstechnica.co.uk/tech-policy/2016/06/mi5-too-much-data-preston-milkwhite-analysis/.

[798] Ethem Alpaydin, ***Machine Learning: The New AI*** (Cambridge, Mass.: MIT Press, 2016), 166.

the database, is responsible for generating the reasons for adding that selector is sustainable so long as human analysts remain in the position assigned to users, who enter semantic search terms that digital media operationalise through selection operations applied to the distributed stores of intercepted data. Yet as machines increasingly come to determine the selection of data for intelligence purposes, the legally generated notion of an a priori justificatory reason for intercepting data will lose its place in the order of things. Machines supplant their users.

Learning machines cannot account for their decisions in semantic terms, any more than studying the brain can give an account of consciousness.[799] Justificatory reasons emerge from the interception and analysis of data, not before. They will continue to exist only so long as the law maintains the fiction that the results of recursive computerised pattern recognition can be attributed to the Secretary of State through her signature.[800]

Already, the analyst's job is simply to semantically translate the output of past interception operations into input for the next; already, the post-facto analysis of intercepted data generates 'justifications' for intercepting more. The law disguises this process by attributing action to human intentions, but in linking abnormal patterns of intercepted data to abnormal human behaviour, machines are learning to do this too. Without the function assigned to them by the law, humans have no grounds on which to second-guess machines.[801] At the point when the law is finally confirmed to have lost its ability to assign meaning to media-technical operations, it may become possible to glimpse the real locus of power today.

[799] Ibid., 22.

[800] On law's fictions and computers, see Vismann and Krajewski, 'Computer Juridisms', 92.

[801] Elena Esposito has elegantly compared the human position in this situation to the position of the priests in ritual forms of divination, see Elena Esposito, 'Digital Prophecies and Web Intelligence', in ***Privacy, Due Process and the Computational Turn***, ed. Mireille Hildebrandt and Katja de Vries (London New York: Routledge, 2013), 121–42.

Bibliography

Books and Scholarly Articles

Aldrich, Richard. *GCHQ*. London: Harper Press, 2011.

Aldrich, Richard J. 'Policing the Past: Official History, Secrecy and British Intelligence Since 1945'. *The English Historical Review* 119, no. 483 (2004): 922–53.

Allen, E. J. B. *Post and Courier Service in the Diplomacy of Early Modern Europe*. The Hague: Martinus Nijhoff, 1972.

Alpaydin, Ethem. *Machine Learning: The New AI*. Cambridge, Massachusetts: MIT Press, 2016.

Amoore, Louise. *The Politics of Possibility: Risk and Security Beyond Probability*. Durham: Duke University Press, 2013.

Andrew, Christopher. *The Defence of the Realm: The Authorized History of MI5*. London: Penguin, 2010.

Andrew, Christopher, and Keith Neilson. 'Tsarist Codebreakers and British Codes'. In *Codebreaking and Signals Intelligence*, edited by Christopher Andrew, 6–12. London: Frank Cass, 1986.

Audibert, Lucie C., and Andrew D. Murray. 'A Principled Approach to Network Neutrality'. *SCRIPTed* 13, no. 2 (2016): 118–43.

Bakir, Vian. *Torture, Intelligence and Sousveillance in the War on Terror: Agenda-Building Struggles*. Farnham, Surrey: Ashgate Publishing Limited, 2013.

Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency*. New York: Penguin, 1983.

———. *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America*. Doubleday, 2008.

Barker, Elaine, and John Kelsey. 'Recommendation for Random Number Generation Using Deterministic Random Bit Generators'. Computer Security Resource Center, 2012. https://csrc.nist.gov/publications/detail/sp/800-90a/archive/2012-01-23.

Barnard, H. C. 'The Messageries of the University of Paris'. *British Journal of Educational Studies* 4, no. 1 (1955): 49–56.

Barty-King, Hugh. *Girdle Round the Earth: The Story of Cable and Wireless and Its Predecessors to Mark the Group's Jubilee, 1929-1979*. London: Heinemann, 1979.

Bauer, Friedrich L. *Decrypted Secrets: Methods and Maxims of Cryptology*. Third Edition. Berlin: Springer, 2002.

Beale, P. O. *A History of the Post in England from the Romans to the Stuarts*. Brookfield, VT: Ashgate, 1998.

Beattie, J. M. *Crime and the Courts in England, 1660-1800*. Oxford: Clarendon Press, 1986.

Bedos-Rezak, Brigitte. *When Ego Was Imago: Signs of Identity in the Middle Ages*. Leiden; Boston: Brill, 2011.

Bellamy, J. G. *The Law of Treason in England in the Later Middle Ages*. Cambridge: Cambridge University Press, 1970. http://ebooks.cambridge.org/ref/id/CBO9780511522369.

Blackstone, William. *The Oxford Edition of Blackstone's: Commentaries on the Laws of England: Book I: Of the Rights of Persons*. Oxford: Oxford University Press, 2016.

Bratton, Benjamin H. *The Stack: On Software and Sovereignty*. Software Studies. Cambridge, Massachusetts: MIT Press, 2015.

Brown, A. L. 'The Authorization of Letters under the Great Seal'. *Historical Research* 37, no. 96 (1 November 1964): 125–56.

Campaigne, Howard H. 'Lightning'. *NSA Technical Journal* 4, no. 3 (July 1959): 63–67.

Campbell-Smith, Duncan. *Masters of the Post: The Authorized History of the Royal Mail*. London: Penguin, 2012.

Carruthers, Mary J. *The Book of Memory: A Study of Memory in Medieval Culture*. Cambridge: Cambridge University Press, 1993.

Chester, Sir Daniel Norman. *The English Administrative System 1780-1870*. Oxford: Clarendon Press, 1981.

Chrimes, S. B. *An Introduction to the Administrative History of Mediaeval England*. Third Edition. Studies in Mediaeval History. Oxford: Blackwell, 1966.

Clanchy, M. T. *From Memory to Written Record: England 1066-1307*. Second Edition. Oxford: Blackwell, 1993.

Clarke, Arthur C. *How the World Was One: Beyond the Global Village*. London: Gollancz, 1992.

Cohen, Julie E. *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven: Yale University Press, 2012.

Corera, Gordon. *Intercept: The Secret History of Computers and Spies*. W&N, 2015.

Couldry, Nick, and Alison Powell. 'Big Data From the Bottom Up'. *Big Data & Society* 1, no. 2 (2014).

Daunton, M.J. *Royal Mail: The Post Office Since 1840*. London: The Athlone Press, 1985.

'Defence Requirements for Cable Landing Sites', 1910. BT Archives.

Deleuze, Gilles. 'Postscript on the Societies of Control'. *October* 59 (1992): 3–7.

Delgado, Alan. *The Enormous File: A Social History of the Office*. London: John Murray Publishers Ltd, 1979.

Denniston, A. G. 'The Government Code and Cypher School Between the Wars'. In *Codebreaking and Signals Intelligence*, edited by Christopher Andrew, 48–70. London: Frank Cass, 1986.

Diffie, Whitfield, and Susan Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Updated Edition, Cambridge, Massachusetts: MIT Press, 2007.

Dickens, Charles. *The Signalman: A Ghost Story*. London: Profile Books, 2015.

Eachus, Joseph, Walter W. Hagedorn, Samuel S. Snyder, and Howard H. Campaigne. 'Growing Up with Computers at NSA'. *NSA Technical Journal*, no. Special Issue (1972): 3–14.

Ellis, Kenneth. *The Post Office in the Eighteenth Century: A Study in Administrative History.* Oxford: Oxford University Press, 1958.

Endicott, Timothy. 'Was Entick v Carrington a Landmark?' In *Entick v Carrington: 250 Years of the Rule of Law*, edited by Adam Tomkins and Paul Scott, 109–30. Oxford: Hart Publishing, 2015.

Engstrom, Edward T. 'Science and Cryptology'. *NSA Technical Journal* 3, no. 3 (July 1958): 1–6.

Esposito, Elena. 'Digital Prophecies and Web Intelligence'. In *Privacy, Due Process and the Computational Turn*, edited by Mireille Hildebrandt and Katja de Vries, 121–42. London, New York: Routledge, 2013.

Evans, Florence Greir. *The Principal Secretary of State: A Survey of the Office from 1558 to 1680.* Manchester: Manchester University Press, 1923.

Ewing, Keith, and Conor Gearty. *The Struggle for Civil Liberties: Political Freedom and the Rule of Law in Britain, 1914-1945*. Oxford: Oxford University Press, 2001.

Fari, Simone. *Victorian Telegraphy Before Nationalization*. Basingstoke, Hampshire: Palgrave Macmillan, 2015.

Firth, C. H. 'Thurloe and the Post Office'. *English Historical Review* 13 (1 January 1898): 527–533.

Fisher, John H. 'Chancery and the Emergence of Standard Written English in the Fifteenth Century'. *Speculum* 52, no. 4 (1977): 870–99.

Fitzgerald, Patrick, and Mark Leopold. *Stranger on the Line: The Secret History of Phone Tapping*. London: The Bodley Head, 1987.

Foucault, Michel. *Discipline and Punish: The Birth of the Prison*. Translated by Alan Sheridan. London: Penguin, 1991.

———. 'Governmentality'. In *Power*, by James D. Faubion, 201–22. translated by Robert Hurley & Ors. Essential Works of Foucault 1954 - 1984. London: Penguin, 2002.

———. *Security, Territory, Population.* Edited by Arnold I. Davidson. Translated by Graham Burchell. Basingstoke; New York: Palgrave Macmillan, 2007.

———. *Society Must Be Defended*. Translated by David Macey. London: Penguin, 2003.

———. *The Archaeology of Knowledge*. Translated by A.M. Sheridan Smith. 2nd edition. London ; New York: Routledge, 2002.

———. *The Birth of Biopolitics*. Edited by Arnold I. Davidson. Translated by Graham Burchell. Basingstoke; New York: Palgrave Macmillan, 2008.

———. *The Order of Things: An Archaeology of the Human Sciences*. London: Tavistock, 1970.

———. 'Truth and Juridical Forms'. In *Power*, by James D. Faubion, 1–89. translated by Robert Hurley & Ors. Essential Works of Foucault 1954 - 1984. London: Penguin, 2002.

———. 'What Is an Author?' In *The Art of Art History*, edited by Donald Preziosi, 299–314. Oxford: Oxford University Press, 1998.

Fraser, Peter. *The Intelligence of the Secretaries of State and Their Monopoly of Licensed News, 1660-1688*. Cambridge: Cambridge University Press, 1956.

Fuchs, Christian. *Critical Theory of Communication: New Readings of Lukács, Adorno, Marcuse, Honneth and Habermas in the Age of the Internet*. London: University of Westminster Press, 2016.

———. 'Surveillance and Critical Theory'. *Media and Communication* 3, no. 2 (30 September 2015): 6–9.

Galloway, Alexander R. *Protocol: How Control Exists After Decentralization*. Cambridge, Massachusetts: MIT Press, 2006.

Gearty, Conor. 'The Courts and Recent Exercises of the Prerogative'. *The Cambridge Law Journal* 46, no. 3 (1987): 372–74.

Gleick, James. *The Information*. London: Fourth Estate, 2012.

Goodman, Dena. 'Epistolary Property: Michel de Servan and the Plight of Letters on the Eve of the French Revolution'. In *Early Modern Conceptions of Property*, edited by John Brewer and Susan Staves, 339–64. London, New York: Routledge, 1995.

Grant, J. Kerry. *A Companion to The Crying of Lot 49*. Athens: University of Georgia Press, 1994.

Greenwald, Glenn. *No Place to Hide*. New York: Macmillan US, 2014.

Gumbrecht, Hans Ulrich. 'Media History as the Event of Truth: On the Singularity of Friedrich A. Kittler's Works'. In *The Truth of the Technological World*, translated by Erik Butler, 307–29. Stanford: Stanford University Press, 2013.

———. 'Second Order Observation Historicized - An Epistemological Frame Narrative'. Stuttgart: Akademie Schloss Solitude, 2010. http://www.design-in-human.de/lectures/gumbrecht.html.

Habermas, Jürgen. *The Structural Transformation of the Public Sphere: Inquiry into a Category of Bourgeois Society*. Translated by Thomas Burger. New Ed edition. Cambridge: Polity Press, 1992.

Haggerty, Kevin D., and Richard V. Ericson. 'The Surveillant Assemblage'. *British Journal of Sociology* 51, no. 4 (2000): 605–22.

Hale, Sir Matthew. *The History of the Pleas of the Crown (Published from His Lordship's Original Manuscript, and the Several References to the Records Examined by the Originals)*. Reproduction from British Library. Vol. 2. London: Gyles, Woodward, and Davis, 1736.

Harding, Alan. *Medieval Law and the Foundations of the State*. Oxford: Oxford University Press, 2002.

Hardt, Michael, and Antonio Negri. *Empire*. Cambridge, Massachusetts: Harvard University Press, 2000.

Harvey, P. D. A., and Andrew McGuiness. *A Guide to British Medieval Seals*. London: British Library and Public Record Office, 1996.

Headrick, Daniel R. *The Invisible Weapon: Telecommunications and International Politics, 1851-1945*. New York: Oxford University Press, 1991.

Hemmeon, J. C. *History of the British Post Office*. Cambridge, Massachusetts: Harvard University Press, 1912.

Herman, Michael. *Intelligence Power in Peace and War*. Cambridge University Press, 1996.

Hickman, Tom. 'Revisiting Entick v Carrington: Seditious Libel and State Security Laws in Eighteenth-Century England'. In *Entick v Carrington: 250 Years of the Rule of Law*, edited by Adam Tomkins and Paul Scott, 43–84. Oxford: Hart Publishing, 2015.

Hidalgo, César. *Why Information Grows: The Evolution of Order, from Atoms to Economies*. London: Allen Lane, 2015.

Hildebrandt, Mireille. 'Profile Transparency by Design?' In *Privacy, Due Process and the Computational Turn*, edited by Mireille Hildebrandt and Katja de Vries, 221–46. London, New York: Routledge, 2013.

Hill, Christopher. *Intellectual Origins of the English Revolution Revisited*. Oxford: Oxford University Press, 1997.

Hodges, Andrew. *Alan Turing: The Enigma*. London: Vintage, 1992.

Hong, Sungook. *Wireless: From Marconi's Black-Box to the Audion*. Cambridge, Massachusetts: MIT Press, 2001.

Horn, Eva. 'Logics of Political Secrecy'. *Theory, Culture & Society* 28, no. 7–8 (2011): 103–22.

Housden, J. A. J. 'The Merchant Strangers' Post in the Sixteenth Century'. *The English Historical Review* 21, no. 84 (1906): 739–742.

Hu, Tung-Hui. *A Prehistory of the Cloud*. Cambridge, Massachusetts: MIT Press, 2015.

Innis, Harold Adams. *Empire and Communications*. 2nd ed. Toronto: University of Toronto Press, 1972.

Jagodzinski, Cecile M. *Privacy and Print: Reading and Writing in Seventeenth-Century England*. Charlottesville: University of Virginia Press, 1999.

James, Henry. 'In the Cage'. In *In the Cage and Other Stories*. London: Penguin, 1972.

Jeffery, Keith. *MI6. The History of the Secret Intelligence Service 1909-1949.* London: Bloomsbury Publishing Ltd, 2011.

Johnson, Thomas R. *American Cryptology During the Cold War, 1945-1989, Book II: Centralization Wins, 1960-1972*. Excised & Declassified 2013. National Security Agency: Center for Cryptological History, 1998. https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/cold_war_iii.pdf.

———. *American Cryptology During the Cold War, 1945-1989, Book III: Retrenchment and Reform, 1972-1980*. Excised & Declassified 2007. National Security Agency: Center for Cryptological History, 1998. https://www.nsa.gov/news-features/declassified-documents/cryptologic-histories/assets/files/cold_war_iii.pdf.

Joyce, Patrick. *The State of Freedom: A Social History of the British State since 1800.* Cambridge: Cambridge University Press, 2013.

Kahn, David. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. 2nd ed. New York: Scribner, 1996.

Kantorowicz, Ernst H. *The King's Two Bodies*. Princeton, New Jersey: Princeton University Press, 1957.

Kennedy, Paul M. 'Imperial Cable Communications and Strategy, 1870-1914'. *The English Historical Review* 86, no. 341 (1971): 728–752.

Kittler, Friedrich. 'Authorship and Love'. *Theory, Culture & Society* 32, no. 3 (2015): 15–47.

———. *Optical Media*. Translated by Anthony Enns. Cambridge: Polity, 2010.

———. 'Towards an Ontology of Media'. *Theory, Culture & Society* 26, no. 2–3 (1 March 2009): 23–31.

Kittler, Friedrich A. *Discourse Networks 1800/1900*. Stanford: Stanford University Press, 1992.

———. *Gramophone, Film, Typewriter*. Translated by Geoffrey Winthrop-Young. Stanford University Press, 1999.

———. 'Protected Mode'. In *The Truth of the Technological World*, translated by Erik Butler, 209–18. Stanford: Stanford University Press, 2013.

———. 'The Artificial Intelligence of World War: Alan Turing'. In *The Truth of the Technological World*, translated by Erik Butler, 178–218. Stanford: Stanford University Press, 2013.

Krajewski, Markus. 'Paper as Passion: Niklas Luhmann and His Card Index'. In *'Raw Data' is an Oxymoron*, edited by Lisa Gitelman, translated by Charles Macrum II, 103–20. Cambridge: MIT Press, 2013.

———. *Paper Machines: About Cards & Catalogs, 1548-1929*. Translated by Peter Krapp. Cambridge, Massachusetts: MIT Press, 2011.

———. *World Projects: Global Information Before World War I*. Translated by Charles Marcrum II. Minneapolis: University of Minnesota Press, 2014.

Kynaston, David. *The Secretary of State*. Lavenham, Suffolk: Terence Dalton, 1978.

Landau, Susan. 'Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations'. *IEEE Security Privacy* 12, no. 1 (January 2014): 62–64.

———. 'Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations'. *IEEE Security Privacy* 11, no. 4 (July 2013): 54–63.

Lang, A. 'The Bishop's Plot.' Edited by William III Blackwood. *Blackwood's Edinburgh Magazine* 161, no. 975 (January 1897): 90–99.

Lanning, Hugh, and Richard Norton-Taylor. *A Conflict of Loyalties: GCHQ 1984-1991*. New Clarion, 1991.

Lessig, Lawrence. *Code 2.0*. CC Online. Basic Books, 2006. http://codev2.cc/download+remix/Lessig-Codev2.pdf.

Lewins, William. *Her Majesty's Mails: A History of the Post Office and an Industrial Account of Its Present Condition.* London: S. Low, son, and Marston, 1864.

Lippert, Randy, and David Wood. 'The New Urban Surveillance: Technology, Mobility, and Diversity in 21st Century Cities'. *Surveillance & Society* 9, no. 3 (2012): 257–262.

Longley, Paul A., Michael F. Goodchild, David J. Maguire, and David W. Rhind. *Geographic Information Systems and Science*. 4th Edition. Hoboken, NJ: John Wiley & Sons, 2015.

Loughlin, Martin. *Foundations of Public Law*. Oxford: Oxford University Press, 2010.

———. *Sword and Scales : An Examination of the Relationship Between Law and Politics*. Oxford: Hart, 2000.

———. 'The State, the Crown and the Law'. In *The Nature of the Crown: A Legal and Political Analysis*, edited by Maurice Sunkin and Sebastian Payne, 33–76. Oxford: Oxford University Press, 1999.

Luhmann, Niklas. *Law as a Social System*. Translated by Klaus Ziegert. Oxford: Oxford University Press, 2004.

———. *Social Systems*. Translated by John Bednarz and Dirk Baecker. Stanford University Press, 1995.

———. *The Reality of the Mass Media*. Translated by Kathleen Cross. Cambridge: Polity, 2000.

———. *Theory of Society*. Translated by Rhodes Barrett. Vol. 1. 2 vols. Stanford, California: Stanford University Press, 2012.

———. *Theory of Society*. Translated by Rhodes Barrett. Vol. 2. 2 vols. Stanford, California: Stanford University Press, 2012.

Lustgarten, Laurence, and Ian Leigh. *In From the Cold: National Security and Parliamentary Democracy*. Oxford: Oxford University Press, 1994.

Lyon, David. 'Everyday Surveillance: Personal Data and Social Classifications'. *Information, Communication & Society* 5, no. 2 (January 2002): 242–57.

Mack Smith, Denis. *Mazzini*. New Haven: Yale University Press, 1996.

Marshall, Alan. *Intelligence and Espionage in the Reign of Charles II, 1660-1685*. Cambridge University Press, 2003.

———. 'Sir Samuel Morland and Stuart Espionage'. In *King Charles Lecture*. Bath Spa University College, 2003.

http://www.academia.edu/1557372/Sir_Samuel_Morland_and_Stuart_espionage.

McLuhan, Marshall. *Understanding Media: The Extensions of Man*. London: Routledge, 2001.

Menke, Richard. 'Telegraphic Realism: Henry James's In the Cage' 115, no. 5 (October 2000): 975–90.

Merkel, Miles A. 'A "Word Spotter"'. *NSA Technical Journal* 4, no. 4 (1959): 91–100.

Meyer, J.A. 'Computers: The Wailing Wall'. *NSA Technical Journal* 1, no. 3 (1956): 69–90.

Milsom, S. F. C. *Historical Foundations of the Common Law*. London: Butterworths, 1969.

Möller, Kai. 'Proportionality: Challenging the Critics'. *International Journal of Constitutional Law* 10, no. 3 (1 July 2012): 709–31.

Moody, Glyn. 'MI5 Collecting "significantly More" Data than It Can Use, New Snowden Docs Reveal'. *Ars Technica UK*, 7 June 2016. https://arstechnica.co.uk/tech-policy/2016/06/mi5-too-much-data-preston-milkwhite-analysis/.

Moran, Christopher. *Classified: Secrecy and the State in Modern Britain*. Cambridge: Cambridge University Press, 2012.

Morland, Samuel. 'A Brief Discourse Concerning the Nature and Reason of Intelligence'. Egmont Papers. Vol. CCXIV (ff. ii+276)., 1695. Add MS 47133. British Library, Western Manuscripts.

Murphy, W. T. *The Oldest Social Science? Configurations of Law and Modernity*. Oxford: Clarendon Press, 1997.

Nickels, David Paull. *Under the Wire: How the Telegraph Changed Diplomacy*. Cambridge: Harvard University Press, 2003.

NSA. 'The PLATFORM Network Evolution'. *Cryptologic Quarterly*, 1989. https://www.nsa.gov/news-features/declassified-documents/cryptologic-quarterly/assets/files/The_PLATFORM_Network_Evolution.pdf.

Ogilvie, A. M. 'A New History of the Post Office'. *The Economic Journal* 23, no. 89 (1913): 137–141.

Oldcorn, Benjamin David. ‘On the Wire: The Strategic and Tactical Role of Cable and Wireless during the Second World War’, 26 September 2013. https://ore.exeter.ac.uk/repository/handle/10871/14642.

Omand, David. *Securing the State*. London: C Hurst & Co Publishers Ltd, 2012.

Paget, Mary. *The King's Messengers, 1199-1377: A Contribution to the History of the Royal Household*. London: Arnold, 1961.

Palmås, Karl. ‘Inauthentically Intense: Coveillance and Consumer Culture among Speedsurfers’. *Surveillance & Society* 13, no. 3/4 (2015): 487–496.

Pascall, Stephen C., and David J. Withers. *Commercial Satellite Communication*. Oxford: Focal Press, 1997.

Paul Baran. *On Distributed Communications Networks*. Santa Monica, California: The RAND Coporation, 1962. https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf.

Peacey, Jason. *Politicians and Pamphleteers: Propaganda During the English Civil Wars and Interregnum*. Aldershot: Ashgate, 2004.

Pellew, Jill. *The Home Office 1848-1914: From Clerks to Bureaucrats*. London: Heinemann, 1982.

Perry, Charles R. ‘Frank Ives Scudamore and the Post Office Telegraphs’. *Albion: A Quarterly Journal Concerned with British Studies* 12, no. 4 (1980): 350–67.

Pollock, Sir Frederick, and Frederic William Maitland. *History of English Law Before the Time of Edward I*. Vol. 1. Liberty Fund Inc, 2009.

Poole, Thomas. *Reason of State*. Cambridge University Press, 2015.

Pottage, Alain. ‘Law after Anthropology: Object and Technique in Roman Law’. *Theory, Culture & Society* 31, no. 2–3 (1 March 2014): 147–66. doi:10.1177/0263276413502239.

———. ‘Our Geological Contemporary’. In *In Search of Contemporary Legal Thought*, by Desautels-Stein and Tomlins, 177–95. Cambridge: Cambridge University Press, 2017.

———. ‘Power as an Art of Contingency: Luhmann, Deleuze, Foucault’. *Economy and Society* 27, no. 1 (1998): 1–27.

———. ‘The Measure of Land’. *The Modern Law Review* 57, no. 3 (1994): 361–84.

Potter, Lois. *Secret Rites and Secret Writing: Royalist Literature 1641-1660*. Cambridge: Cambridge University Press, 1989.

Potter, Simon James. *News and the British World: The Emergence of an Imperial Press System, 1876-1922*. Oxford: Clarendon, 2003.

Price, Alfred. *Instruments of Darkness: The History of Electronic Warfare 1939-1945*. Revised. Barnsley: Frontline Books, 2017.

Renton, R. N. *Telegraphy*. London: Pitman Publishing, 1976.

Richardson, Malcolm. 'The Fading Influence of the Medieval Ars Dictaminis in England After 1400'. *Rhetorica: A Journal of the History of Rhetoric* 19, no. 2 (2001): 225–47.

Rosenzweig, Roy. 'Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet'. *The American Historical Review* 103, no. 5 (1998): 1530–52.

Rowbottom, Jacob. 'The Propaganda Wars and Liberty of the Press'. In *Entick v Carrington: 250 Years of the Rule of Law*, edited by Adam Tomkins and Paul Scott, 85–107. Oxford: Hart Publishing, 2015.

Schmitt, Carl. *Dictatorship*. Translated by Michael Hoelzl and Graham Ward. Cambridge: Polity, 2013.

Scott, Paul. 'Entick v Carrington and the Legal Protection of Property'. In *Entick v Carrington: 250 Years of the Rule of Law*, edited by Adam Tomkins and Paul Scott, 131–60. Oxford: Hart Publishing, 2015.

Sedley, Stephen. *Lions Under the Throne: Essays on the History of English Public Law*. Cambridge: Cambridge University Press, 2015.

Serres, Michel. *The Parasite*. Minneapolis: University of Minnesota Press, 2007.

Shannon, Claude E. 'A Mathematical Theory of Communication'. *The Bell System Technical Journal* 27, no. July (1948): 379–423.

Siegert, Bernhard. 'Media After Media'. In *Media After Kittler*, edited by Eleni Ikoniadou and Scott Wilson, 79–91. London, New York: Rowman & Littlefield International, 2015.

———. *Relays: Literature as an Epoch of the Postal System*. Translated by Kevin Repp. Stanford, California: Stanford University Press, 1999.

Smith, Graham. 'Future-Proofing the Investigatory Powers Bill'. Accessed 28 January 2017. http://www.cyberleagle.com/2016/04/future-proofing-investigatory-powers.html.

Sood, Gagan D. S. 'The Informational Fabric of Eighteenth-Century India and the Middle East: Couriers, Intermediaries and Postal Communication'. *Modern Asian Studies* 43, no. 5 (2009): 1085–1116.

Souden, David. *Voices Over the Horizon: Tales from Cable and Wireless*. Cambridge: Granta Editions, 1999.

Sprenger, Florian. *The Politics of Micro-Decisions*. Translated by Valentine A. Pakis. Lüneburg: meson press, Hybrid Publishing Lab, 2015. http://meson.press/books/the-politics-of-micro-decisions/.

Srnicek, Nick. *Platform Capitalism*. Cambridge: Polity Press, 2016.

Staff, Frank. *The Penny Post, 1680-1918.* London, Lutterworth Press, 1964.

Starosielski, Nicole. *The Undersea Network*. Durham: Duke University Press Books, 2015.

Strathern, Marilyn. 'Bullet-Proofing: A Tale from the United Kingdom'. In *Documents: Artifacts of Modern Knowledge*, edited by Annelise Riles, 181–205. University of Michigan Press, 2006.

Thomson, Mark A. *The Secretaries of State 1681-1782*. Oxford: Clarendon Press, 1932.

Tomkins, Adam. 'The Authority of Entick v Carrington'. In *Entick v Carrington: 250 Years of the Rule of Law*, edited by Adam Tomkins and Paul Scott, 161–84. Oxford: Hart Publishing, 2015.

Tout, T. F. *The Place of the Reign of Edward II in English History*. Manchester: University of Manchester, 1914.

Tuchman, Barbara W. *The Zimmerman Telegram*. London: Constable, 1959.

Turing, Alan Mathison. 'On Computable Numbers, with an Application to the Entscheidungsproblem'. *Journal of Math* 58, no. 345–363 (1936): 5.

Underdown, David. *Royalist Conspiracy in England, 1649-1660.* New Haven: Yale University Press, 1960.

Van Caenegem, Raoul. *The Birth of the English Common Law*. 2nd ed. Cambridge: Cambridge University Press, 1988.

Vincent, David. 'Surveillance, Privacy & History'. *History & Policy*, 1 October 2013. http://www.historyandpolicy.org/index.php/policy-papers/papers/surveillance-privacy-and-history.

———. *The Culture of Secrecy: Britain 1832-1998*. Oxford: Oxford University Press, 1999.

Vismann, Cornelia. 'Cultural Techniques and Sovereignty'. *Theory, Culture & Society* 30, no. 6 (1 November 2013): 83–93.

———. *Files: Law and Media Technology*. Translated by Geoffrey Winthrop-Young. Stanford: Stanford University Press, 2008.

———. 'Jurisprudence: A Transfer Science'. *Law and Critique* 10, no. 3 (October 1999): 279–86.

Vismann, Cornelia, and Markus Krajewski. 'Computer Juridisms'. *Grey Room* 29 (2008): 90–109.

Wade, Nicholas. 'Glomar Explorer Said Successful after All'. *Science (New York, N.Y.)* 194, no. 4270 (1976): 1142.

———. 'Glomar Explorer: CIA's Salvage Ship a Giant Leap in Ocean Engineering'. *Science* 192, no. 4246 (1976): 1313–1315.

Ward, John O. 'Rhetorical Theory and the Rise and Decline of Dictamen in the Middle Ages and Early Renaissance'. *Rhetorica: A Journal of the History of Rhetoric* 19, no. 2 (2001): 175–223.

'Warrant, n.1'. *OED Online*. Oxford University Press. Accessed 19 June 2017. http://www.oed.com/view/Entry/225837.

West, Nigel. *British Security Coordination: The Secret History of British Intelligence in the Americas 1940-1945*. London: Little Brown, 1998.

Whyman, Susan E. *The Pen and the People: English Letter Writers 1660-1800*. Oxford: Oxford University Press, 2009.

Wilkinson, Nicholas. *Secrecy and the Media: The Official History of the United Kingdom's D-Notice System*. London, New York: Routledge, 2009.

Winthrop-Young, Geoffrey. *Kittler and the Media*. 1 edition. Cambridge: Polity, 2013.

———. ‘Silicon Sociology, Or, Two Kings on Hegel’s Throne? Kittler, Luhmann, and the Posthuman Merger of German Media Theory’. *The Yale Journal of Criticism* 13, no. 2 (2000): 391–420.

Wright, Peter. *Spycatcher*. New York: Viking, 1987.

Wymer, Norman. *From Marconi to Telstar: The Story of Radio*. London: Longman’s, 1966.

Archival Materials

'"A Report to the Postmaster General, July 1866" HIC 0197/005/033', 1866. BT Archives.

'Cancellations of Postal Warrants: Practice HO 45/25957', 1933. National Archives.

'Cases of Leakage of Information about Interception of Mail 1926-1932 KV 4/221', 1932. National Archives.

'Censorship Warrants Which Should Be Revoked on Cessation of Hostilities in Europe HO 45/25973', 1946. National Archives.

'Central Criminal Court Deposition, Defendant: ERNST, Karl Gustav. Charge: Offences against the Official Secrets Act. Session: November 1914, CRIM 1/151/2', 1914. National Archives.

'Chancery: Warrants for the Great Seal, Series I, 1230 - 1485 C 81'. National Archives. Accessed 28 June 2017. http://discovery.nationalarchives.gov.uk/details/r/C3641.

'Code and Cypher School - Erection of Wireless Interception Stations and Staffing FO 366/1059', 1939. National Archives.

'Complete List of Radio Conferences'. *ITU*. Accessed 8 April 2017. http://www.itu.int:80/en/history/Pages/CompleteListOfRadioConferences.aspx

'Constitutional Authority to Stop Letters in the Post HO 45/25962', 1935. National Archives.

'Detection of Lottery Correspondence in the Post; Secretary of State's Warrant of 19 April 1920 HO 45/25958', 1934. National Archives.

'Devices for Recording Telephone Conversations POST 33/904', 1930. BT Archives.

'Disturbances: Warrant Issued for Production of Telegram Addressed to Anarchist Prisoner at Stafford from the "United Anarchist Groups, London" HO 144/242/A53582B', 1892. National Archives.

'Draft Report by the Metropolitan Board of Works, Including Post Office Proposals for New Street Names in Central London POST 17/120', 1856. Royal Mail Archive.

Electric and International Telegraph Company. *Government and the Telegraphs: Statement of the Case of the Electric and International Telegraph Company against the*

Government Bill for Acquiring the Telegraphs. London: E. Wilson, 1868. https//catalog.hathitrust.org/Record/006847104. BT **ARCHIVE check citation**

'Empiradio Beam Services: Method of Recording Received Signals POST 33/2227', 1930. BT Archives.

'Home Office: Post Office Correspondence 1787-1816 HO 33/1', 1816. National Archives.

'Home Office: Post Office Correspondence 1823-1837 HO 33/3', 1837. National Archives.

'Indecent Wares from Abroad: Warrants for the Detention of Illegal Postal Packets (1911-1923) HO 144/1837', 1923. National Archives.

'Interception of Postal and Telephone Communications: Interception Working Party Correspondence' HO 325/536', 1979. National Archives.

'Interception Service FO 366/2381', 1938. National Archives.

'International Radiotelegraph Convention of Washington, 1927 and General and Supplementary Regulations (Washington, 1927)'. Accessed 8 April 2017. http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.39.43.en.100.pdf.

'International Radiotelegraph Convention, Signed at London, July 5, 1912. (London, 1912)'. Accessed 8 April 2017. http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.37.43.en.100.pdf.

'Investigation of Espionage 1914-1919: Incomplete, Draft Summary KV 1/48', 1919. National Archives.

'"John Bull" Article on Working of Postal Warrants HO 45/25960', 1935. National Archives.

'Letters and Papers. Correspondence Relating to Post Office, Customs, Excise, Auditors' Office, College of Arms, Lord Chamberlain and the University of Oxford.' HO 42/208, 1792. National Archives.

'Marconi-Bellini-Tosi Apparatus for Directive Wireless Telegraphy POST 30/3139', 1914. BT Archives.

'Ministry of Economic Warfare', 1942. Cable and Wireless archive (redacted). http://discovery.nationalarchives.gov.uk/details/r/edf70107-39c9-4ba2-b750-68c7e2bb3b6f.

'Minutes of 23rd Meeting. (Home Defence; Possibility of Invasion; Use by Private Persons of Wireless Telegraph Stations in War-Time; Importance of Joint Naval and Military Manoeuvres.) CAB 38/3/72', 1903. National Archives.

'Monomarks: System of Identification: Instructions to the Commissioner's Office and the Position under the Official Secrets Act 1920 (1925 – 1978) MEPO 2/9582', 1978. National Archives.

'Newspaper Cuttings Relating to Letter Opening, 1844/1845 POST 23/7'. Newspaper cuttings relating to the Secretary of State's abolition of the board established at Post Office Headquarters to consider the policy on the opening of letters from persons suspected of treason against the UK and foreign governments, 4 April 1845. British Postal Museum and Archive: The Royal Mail Archive.

'Out Letters to the General Post Office Regarding the Interception of Telegrams and Letters (1887-1899) HO 151/7', n.d. The National Archives, Kew.

'Policy and Procedure for the Imposition of Home Office Warrants for the Interception of Mail and Telephone Communications in the UK 1939-1945 KV 4/222', 1944. National Archives.

'Policy with Regard to the Interception of Private Lines by Telephone Units without HOWs 1941-1944 KV 4/445', 1944. National Archives.

'POST 120 Series: Post Office Investigation Department 1836-1999'. Royal Mail Archive. Accessed 21 September 2017. http://catalogue.postalmuseum.org/index.php?

'Post Office Act 1908'. Accessed 25 May 2017. http://www.legislation.gov.uk/ukpga/1908/48/section/56/enacted.

Post Office (Revenues) Act 1710, 9 Anne I, c. 11 § (1710).

'POST OFFICE—OPENING LETTERS. (Hansard, 18 July 1844)'. Accessed 22 August 2017. http://hansard.millbanksystems.com/commons/1844/jul/18/post-office-opening-letters.

‘Postcodes’. *The Postal Museum*. Accessed 28 August 2017. https://www.postalmuseum.org/discover/explore-online/postal-history/postcodes/.

‘Precedents in Common Law for Opening Letters in the Post HO 45/25961’, 1935. National Archives.

‘Publications: Interception in Mail of Copies of Poetry Book Pansies by D H Lawrence HO 144/20642’, 1929. National Archives.

‘Radiotelegram Intercepted: Legislation to Enforce Secrecy POST 30/1904D’, 1908. BT Archives.

‘Radiotelegrams on Board Ships: Censorship Arrangements, Interceptions and Use of Radio-Telegrams by Salvage Vessels, Part 1 POST 30/2097’, 1928. BT Archives.

‘Radiotelegrams on Board Ships: Censorship Arrangements, Interceptions and Use of Radio-Telegrams by Salvage Vessels, Part 2 POST 30/2098’, 1933. BT Archives.

‘Reports on Directed Wireless Telegraphy Systems Including the Belini-Tosi System TCB 274/10’, 1915. BT Archives.

‘Sedition; Warrants: Warrants Authorising the Production of Letters and Telegrams to and from Russia for Inspection HO 144/1684/400430’, 1921. National Archives.

‘Signing Cancellations of Postal Warrants HO 45/25956’, 1928. National Archives.

‘Special Duties: General Post Office Investigation Branch MEPO 2/1500’, 1919. National Archives.

‘Strike of Telegraphists 1872, POST 30/215’, 1871. BT Archives.

‘Suppression of Experimental and Private Business Wireless Stations during the First World War, Part 1 POST 30/3501’, 1914. BT Archives.

‘Telegraphs: Interception of Letters in Criminal Case. L.O.O.797 as to Exercise of Power by Secretary of State HO 144/164/A42354’, 1886. National Archives.

‘Telegraphs: Mode of Transmitting Letters Intercepted under Warrant of Secretary of State HO 144/203/A47869’, 1887. National Archives.

‘The National Archive of the UK POST 114/1’. File(s), 1657. British Postal Museum and Archive: The Royal Mail Archive.

Thurloe, John. ‘Thurloe Papers, First Series. Collection of State Letters and Papers Relating to Events at Home and Abroad Chiefly in the Time of the Commonwealth - Add MS 4155-4159’, 1692. Western Manuscripts, British Library.

Wallis, John. ‘Letter-Book of John Wallis 1651-1701 - Add MS 32499’, 1701. Western Manuscripts, British Library.

‘Warrants: Listening-in to and Recording of Telephone Conversations under Written Authority of Home Secretary HO 144/20619’, 1937. National Archives.

‘Warrants: Post Office Warrant for Search of Private Correspondence HO 144/674/100653’, 1903. National Archives.

‘Wireless: Interception by Amateurs on Shortwave POST 33/2905D’, 1931. BT Archives.

Snowden Archive

‘Access to the Future’. *Snowden Doc Search*, 21 June 2013. https://search.edwardsnowden.com/docs/Accesstothefuture2013-06-21_nsadocs_snowden_doc.

‘HIMR Data Mining Research Problem Book’, 20 September 2011. https://search.edwardsnowden.com/docs/HIMRDataMiningResearchProblemBook2016-02-02nsadocs.

‘Operational Legalities - GCHQ’. Snowden Doc Search, 22 June 2015. https://search.edwardsnowden.com/docs/ContentorMetadata%3F2015-09-25nsadocs.

‘Preston Architecture - GCHQ’. The Intercept, 5 July 2007. https://theintercept.com/document/2016/06/07/preston-architecture/.

‘Preston Business Processes - GCHQ’. Snowden Doc Search, 8 May 2007. https://search.edwardsnowden.com/docs/PRESTONBusinessProcesses2016-06-07_nsadocs_snowden_doc.

SID today (NSA newsletter). ‘Chef’s Choice: SIGINT and the Question of Governance’. *The Intercept*, 5 May 2004. https://theintercept.com/snowden-sidtoday/.

———. ‘SIGINT Development: A Network of Discovery Networks’, 11 June 2003. https://search.edwardsnowden.com/docs/SIGINTDevelopmentANetworkofDiscoveryNetworks2016-05-16nsadocs.

‘Special Source Access (Supporting Internet Operations) - GCHQ Presentation’, 2010. https://search.edwardsnowden.com/docs/SupportingInternetOperations2015-09-25nsadocs.

‘Tempora - GCWiki Entry’. *Snowden Doc Search*, 21 May 2012. https://search.edwardsnowden.com/docs/TEMPORA2014-06-18nsadocs.

‘XKeyScore - NSA Presentation’. *Snowden Doc Search*, 25 February 2008. https://search.edwardsnowden.com/docs/XKeyScore2013-07-31nsadocs.

News reports, blogs, press releases, and websites

'ABC Case | DuncanCampbell.org'. Accessed 8 September 2017. http://www.duncancampbell.org/content/abc-case.

'After Legal Claim Filed against GCHQ Hacking, UK Government Rewrite Law to Permit GCHQ Hacking'. *Privacy International*, 15 May 2015. https://www.privacyinternational.org/node/584.

Armour, Sophie. 'Liberty Gets Go-Ahead to Challenge Snoopers' Charter in the High Court'. *Liberty Human Rights*, 30 June 2016. https://www.liberty-human-rights.org.uk/news/press-releases-and-statements/liberty-gets-go-ahead-challenge-snoopers%E2%80%99-charter-high-court.

Bowcott, Owen. 'Terrorism Act Incompatible with Human Rights, Court Rules in David Miranda Case'. *The Guardian*, 19 January 2016, sec. World news. http://www.theguardian.com/world/2016/jan/19/terrorism-act-incompatible-with-human-rights-court-rules-in-david-miranda-case.

Burgess, Matt. 'What Is the IP Act and How Will It Affect You?' *WIRED UK*. Accessed 19 September 2017. http://www.wired.co.uk/article/ip-bill-law-details-passed.

Campbell, Duncan. 'Big Buzby Is Watching You'. *New Statesman*, 1 February 1980.

'Edward Coleman'. *Catholic Online*. Accessed 16 September 2017. http://www.catholic.org/saints/saint.php?saint_id=3052.

'Everything You Need to Know about the "terrifying" Investigatory Powers Bill'. Accessed 25 September 2017. https://www.newstatesman.com/science-tech/2016/10/everything-you-need-know-about-terrifying-investigatory-powers-bill.

'Former GCHQ Legal Director: Journalists' Communications Not Considered in RIPA Drafting'. *The Bureau of Investigative Journalism*. Accessed 25 September 2017. https://www.thebureauinvestigates.com/stories/2015-02-09/former-gchq-legal-director-journalists-communications-not-considered-in-ripa-drafting.

Gallagher, Ryan. 'From Radio to Porn, British Spies Track Web Users' Online Identities'. *The Intercept*. Accessed 10 October 2016.

https://theintercept.com/2015/09/25/gchq-radio-porn-spies-track-web-users-online-identities/.

———. 'The Inside Story of How British Spies Hacked Belgium's Largest Telco'. *The Intercept*. Accessed 16 October 2016. https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/.

———. 'The Little-Known Company That Enables Worldwide Mass Surveillance'. *The Intercept*. Accessed 16 October 2016. https://theintercept.com/2016/10/23/endace-mass-surveillance-gchq-governments/.

'GCHQ Codewords and Abbreviations'. Accessed 10 October 2016. http://electrospaces.blogspot.com/p/gchq-nicknames-and-codewords.html.

Gellman, Barton, and Ashkan Soltani. 'NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say'. *Washington Post*, 30 October 2013, sec. National Security. https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

Harding, Luke. 'Footage Released of Guardian Editors Destroying Snowden Hard Drives'. *The Guardian*, 31 January 2014, sec. UK news. http://www.theguardian.com/uk-news/2014/jan/31/footage-released-guardian-editors-snowden-hard-drives-gchq.

'Hawklaw Intercept "Y" Listening Station (Former), Hawklaw | Buildings at Risk Register'. Accessed 4 November 2016. http://www.buildingsatrisk.org.uk/details/907213.

'How GCHQ Hacked Belgacom'. *Infosecurity Magazine*, 11 November 2013. http://www.infosecurity-magazine.com/news/how-gchq-hacked-belgacom/.

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. 'GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications'. *The Guardian*, 21 June 2013, sec. UK news. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

Reitman, rainey. '3 Years Later, the Snowden Leaks Have Changed How the World Sees NSA Surveillance'. *Electronic Frontier Foundation*, 5 June 2016.

https://www.eff.org/deeplinks/2016/06/3-years-later-snowden-leaks-have-changed-how-world-sees-nsa-surveillance.

Rusbridger, Alan, and Ewen MacAskill. 'Edward Snowden Interview - the Edited Transcript'. *The Guardian*, 18 July 2014, sec. World news. http://www.theguardian.com/world/2014/jul/18/-sp-edward-snowden-nsa-whistleblower-interview-transcript.

Scahill, Jeremy. 'Gemalto Doesn't Know What It Doesn't Know'. *The Intercept*, 25 February 2015. https://theintercept.com/2015/02/25/gemalto-doesnt-know-doesnt-know/.

Travis, Alan. 'Tribunal Says EU Judges Should Rule on Legality of UK Surveillance Powers'. *The Guardian*, 8 September 2017, sec. World news. http://www.theguardian.com/world/2017/sep/08/snoopers-charter-tribunal-eu-judges-mass-data-surveillance.

'UK Parliament Passes Most Extreme Surveillance Law in UK History'. *Privacy International*. Accessed 19 September 2017. https://www.privacyinternational.org/node/1005.

'We Defend Freedom - UK Spy Chiefs'. *BBC News*, 7 November 2013, sec. UK Politics. http://www.bbc.co.uk/news/uk-politics-24847399.

Cases, legislation, Codes of Practice

An Act for establishing a General Post Office for all her Majesty's Dominions, and for settling a weekly Sum out of the Revenues thereof, for the Service of the War, and other her Majesty's Occasions., (9 Ann.) C A P. X. (11) § (1710). Justis.com.

Attorney-General v Edison Telephone Co of London 6 QBD 244 (1880).

'Bill of Rights 1689'. *UK Parliament*. Accessed 26 September 2017. https://www.parliament.uk/about/living-heritage/evolutionofparliament/parliamentaryauthority/revolution/collections1/collections-glorious-revolution/billofrights/.

Council for Civil Service Unions v Minister for the Civil Service (HL 22 22 November 1984).

Draft Investigatory Powers Bill, CM 9152 § (2015). https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf.

'Interception of Communications Code of Practice'. Home Office, January 2016. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/496064/53659_CoP_Communications_Accessible.pdf.

'Investigatory Powers Act 2016'. Accessed 25 January 2017. http://www.legislation.gov.uk/ukpga/2016/25/section/261/enacted.

Liberty & Others v The Secretary of State for Foreign and Commonwealth Affairs & Others,

R v Secretary of State for Home Affairs ex p. Hosenball [1977] 1 WLR 766

Some Account of the Trial, &c. of Dr. Florence Hensey, Kimber, Edward (ed.) *London magazine, or, Gentleman's monthly intelligencer*, 1747-1783; London27 (Jun 1758): 304-305.

IPT/13/77/H (2015).

Malone v Commissioner for the Metropolitan Police (No.2) [1979] 344 Chancery Division.

Malone v. The United Kingdom (ECtHR 2 August 1984).

Official Secrets Act 1920. Accessed 19 October 2016. http://www.legislation.gov.uk/ukpga/Geo5/10-11/75/contents.

Privacy International v Secretary of State for Foreign and Commonwealth Affairs & Others, IPT/15/110/CH (2016).

R v Secretary of State for Home Affairs ex p. Hosenball [1977] (n.d.).

Regulation of Investigatory Powers Act 2000. Accessed 19 June 2017. http://www.legislation.gov.uk/ukpga/2000/23/contents.

'Summary in the Matter of IPT/01/62 and IPT/01//77'. Case summary. Investigatory Powers Tribunal, 22 January 2003. http://www.ipt-uk.com/docs/Summary_IPT0162_0177.pdf.

'Telegraph Act 1868'. Accessed 31 August 2017. http://www.legislation.gov.uk/ukpga/Vict/31-32/110/contents/enacted.

'When to Refuse to Confirm or Deny Information Is Held'. Information Commissioners Office, 2013. https://ico.org.uk/media/for-organisations/documents/1166/when_to_refuse_to_confirm_or_deny_section_1_foia.pdf.

'Serious Crime Act 2015'. Accessed 28 September 2017. http://www.legislation.gov.uk/ukpga/2015/9/section/44/enacted.

Reports and Press Releases

Anderson, David. 'A Question of Trust: Report of the Investigatory Powers Review'. Stationery Office, 2015.

'Report of the Committee of Privy Councillors Appointed to Inquire into the Interception of Communications (the Birkett Report)', 1957. http://www.fipr.org/rip/Birkett.htm.

Gardiner, Thomas. 'A General Survey of the Post Office - Add MS 62091', 1682. Western Manuscripts, British Library.

'Intercepted Letters'. In *Journal of the House of Commons: Volume 2, 1640-1643*, 2:883–84. London: His Majesty's Stationery Office, 1642. http://www.british-history.ac.uk/commons-jrnl/vol2/pp883-884.

Keenan, Bernard. 'Going "Below the Waterline": The Paradoxical Regulation of Secret Surveillance in the UK'. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 1 March 2015. http://papers.ssrn.com/abstract=2583806.

'Open Rights Group - Home Office Consultation: Investigatory Powers (Technical Capability) Regulations 2017'. *Open Rights Group*. Accessed 23 May 2017. https://www.openrightsgroup.org/ourwork/reports/home-office-consultation:-investigatory-powers-(technical-capability)-regulations-2017.

'Privacy and Security: A Modern and Transparent Framework'. Intelligence and Security Committee, 2015. http://isc.independent.gov.uk/files/20150312_ISC_P+S+Rpt(web).pdf.

'Report from the Secret Committee on the Post-Office'. Secret Committee on the Post Office, House of Commons, 1844. http://www.gbps.org.uk/information/downloads/files/official-documents/Report%20from%20the%20Secret%20Committee%20on%20the%20Post-Office%20(1844).pdf

'Report of the Committee of Privy Counsellors Appointed to Inquire into "D" Notice Matters'. London: UK Parliament Prime Minister's Office, 1967.

‘Report of the Interception of Communications Commissioner: Annual Report for 2015’. IOCCO, 8 September 2016. http://iocco-uk.info/docs/56850%20HC%20255%20ICCO%20Web%20only.pdf.

‘Report of the Second Computer Study Group’. *NSA Technical Journal* 19, no. 1 (1974): 21–63.

Report on Cable Censorship during the Great War (1914-1919). London: General Staff, War Office, 1920.

‘Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System) - Temporary Committee on the ECHELON Interception System - A5-0264/2001’. Accessed 17 October 2016. http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=EN.

Website references

'Interception, n.' *OED Online*. Oxford University Press. Accessed 22 June 2017. http://www.oed.com/view/Entry/97583.

IP2Location. 'IP Address Ranges by Country'. *IP2Location*. Accessed 26 September 2017. http://lite.ip2location.com/ip-address-ranges-by-country.

'Joint Intelligence Committee - GOV.UK'. Accessed 12 September 2017. https://www.gov.uk/government/groups/joint-intelligence-committee.

'Monument, n.' *OED Online*. Oxford University Press. Accessed 22 June 2017 Accessed 9 September 2017. http://www.oed.com/view/Entry/121852?rskey=wWf7oU&result=1#eid.

'The Meerut Conspiracy Trial'. Accessed 25 May 2017. https://web.archive.org/web/20080303235605/http://www.wcml.org.uk/internat/meerut.htm.

The National Archives. 'Home Office Correspondence 1782-1979'. *The National Archives*. Accessed 11 September 2017. http://www.nationalarchives.gov.uk/help-with-your-research/research-guides/home-office-correspondence-1782-1979/.

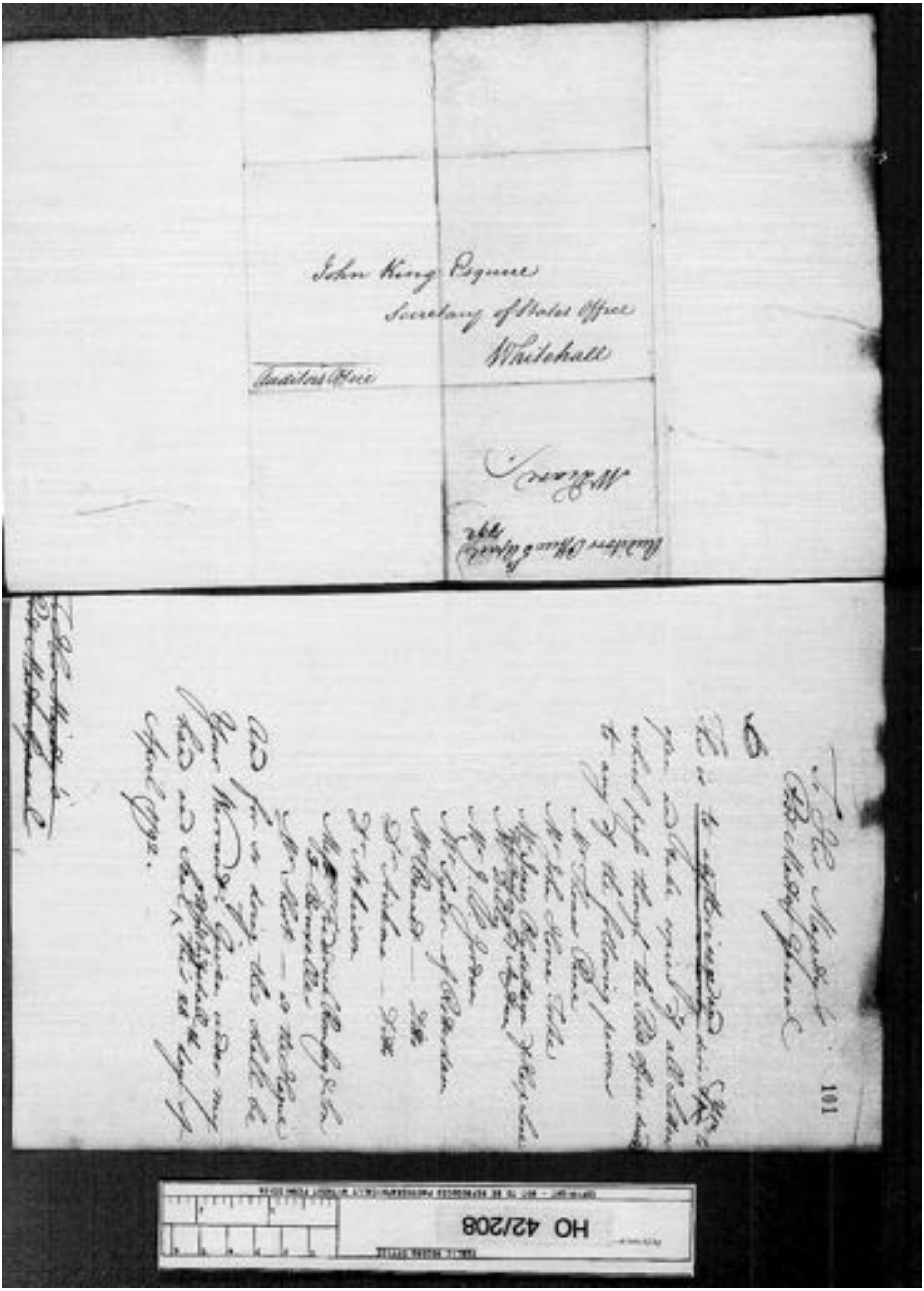
'The National Technical Assistance Centre | GCHQ Site'. Accessed 8 July 2017. https://www.gchq.gov.uk/features/national-technical-assistance-centre.

'When a Telephone Conversation Was Actually a Telegram in the Eyes of the Law'. *BT.com*. Accessed 25 May 2017. http://home.bt.com/tech-gadgets/when-a-telephone-conversation-was-actually-a-telegram-in-the-eyes-of-the-law-11364121187126.

Film

Citizenfour. (2014). [DVD] Directed by L. Poitras. Germany: Praxis Films

Images



John King Esquire
Secretary of States Office
Whitehall

Auditors Office

To His Majesty's
Post Master General

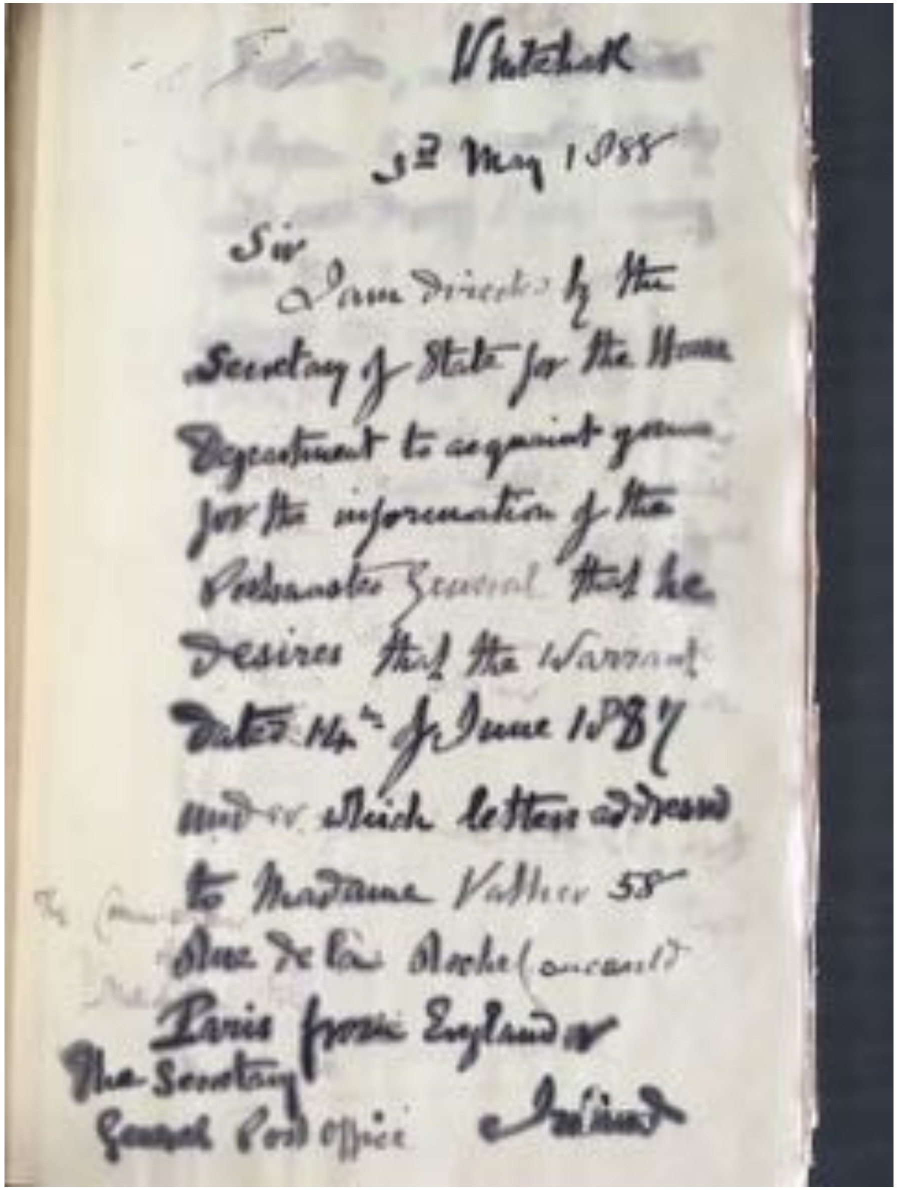
These are to ~~authorize and~~ direct you to open and take copies of all Letters which pass through the Post Office directed to any of the following persons
Mr Thomas Paine
Mr John Horne Tooke
Mr Isaac Blydesteyn of [illegible]
Mr [illegible] Dilly
Mr J. S. Jordan
Mr Sydow of Rotterdam
Mr Bennet — Ditto
Dr Aitkens — Ditto
Dr Atkinson
Messrs Frederick Romberg & Son of Brussells
Mr Hirt — at the Hague
And for so doing this shall be Your Warrant. Given under my hand and Seal at Whitehall this 28th day of April 1792.

~~To His Majesty's Post Master General~~

101

HO 42/208

Figure 1: Copy of an interception warrant. Home Office records, 28th April 1792.



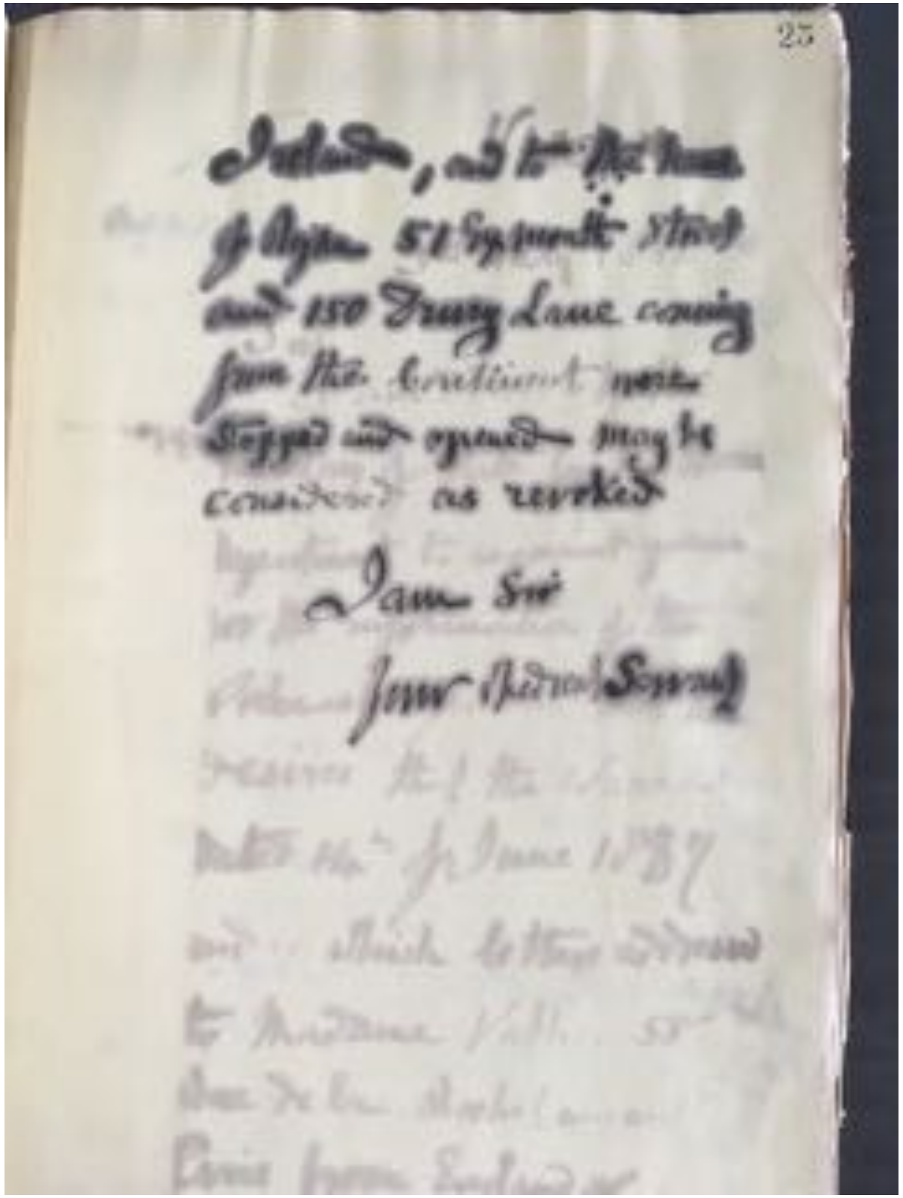
Whitehall

3rd May 1888

Sir

I am directed by the Secretary of State for the Home Department to acquaint you for the information of the Postmaster General that he desires that the Warrant dated 14th of June 1887 under which letters addressed to Madame Vallier 58 Rue de la Rochefoucauld Paris from England or Ireland

The Secretary
General Post Office

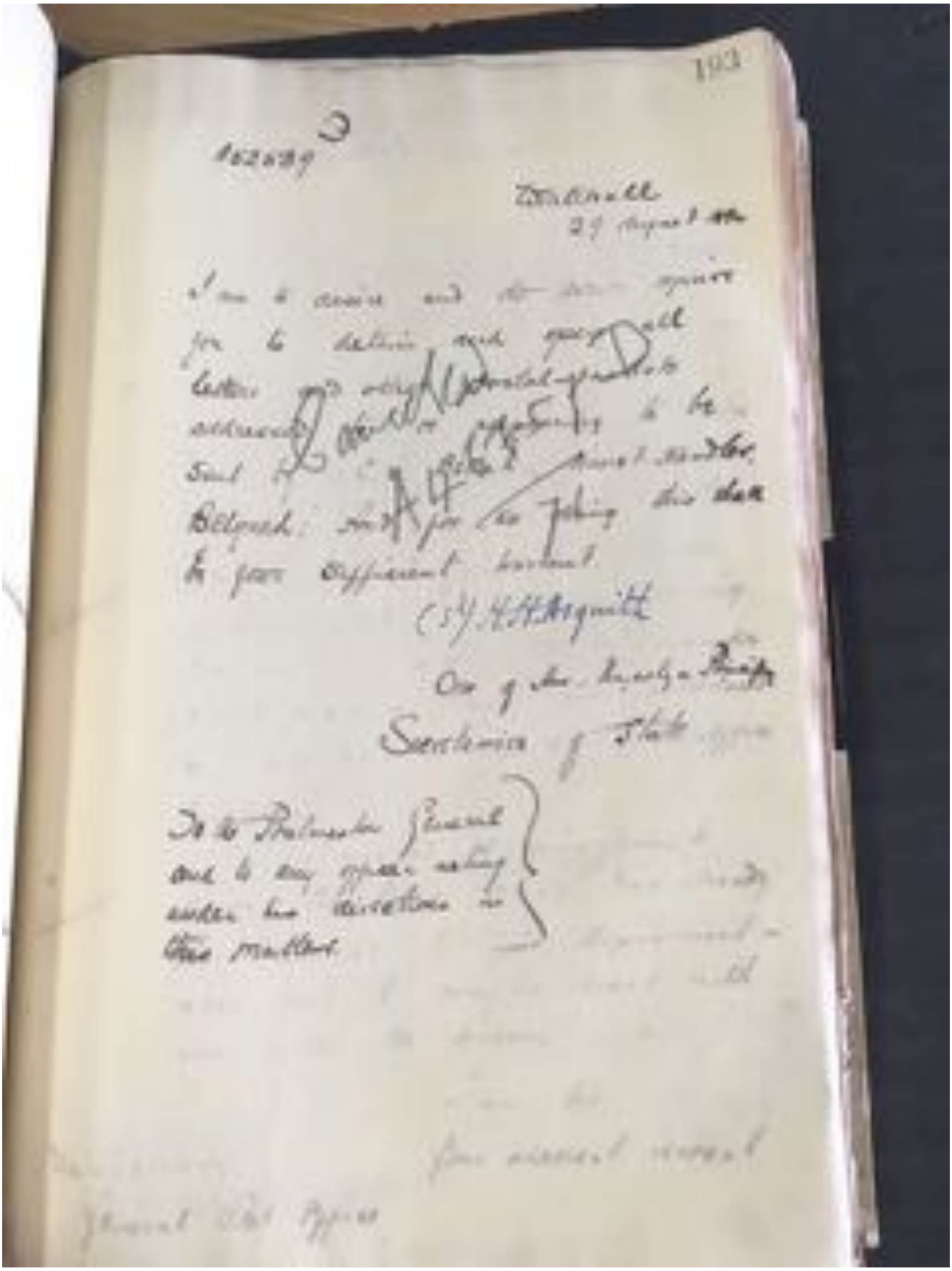


25

Ireland, and to the Name of [illegible] 51 Weymouth Street and 150 Drury Lane coming from the Continent were stopped and opened may be considered as revoked

I am Sir
Your obedient Servant

Figure 2: Pressed copy of a cancellation letter, May 1888, referring to warrant from 1887



193

3

162689

Whitehall
29 August [illegible]

I am to desire and do hereby require you to detain and open all letters [illegible] addressed [illegible] to be sent [illegible] Belgrade [illegible] this date [illegible] your obedient servant

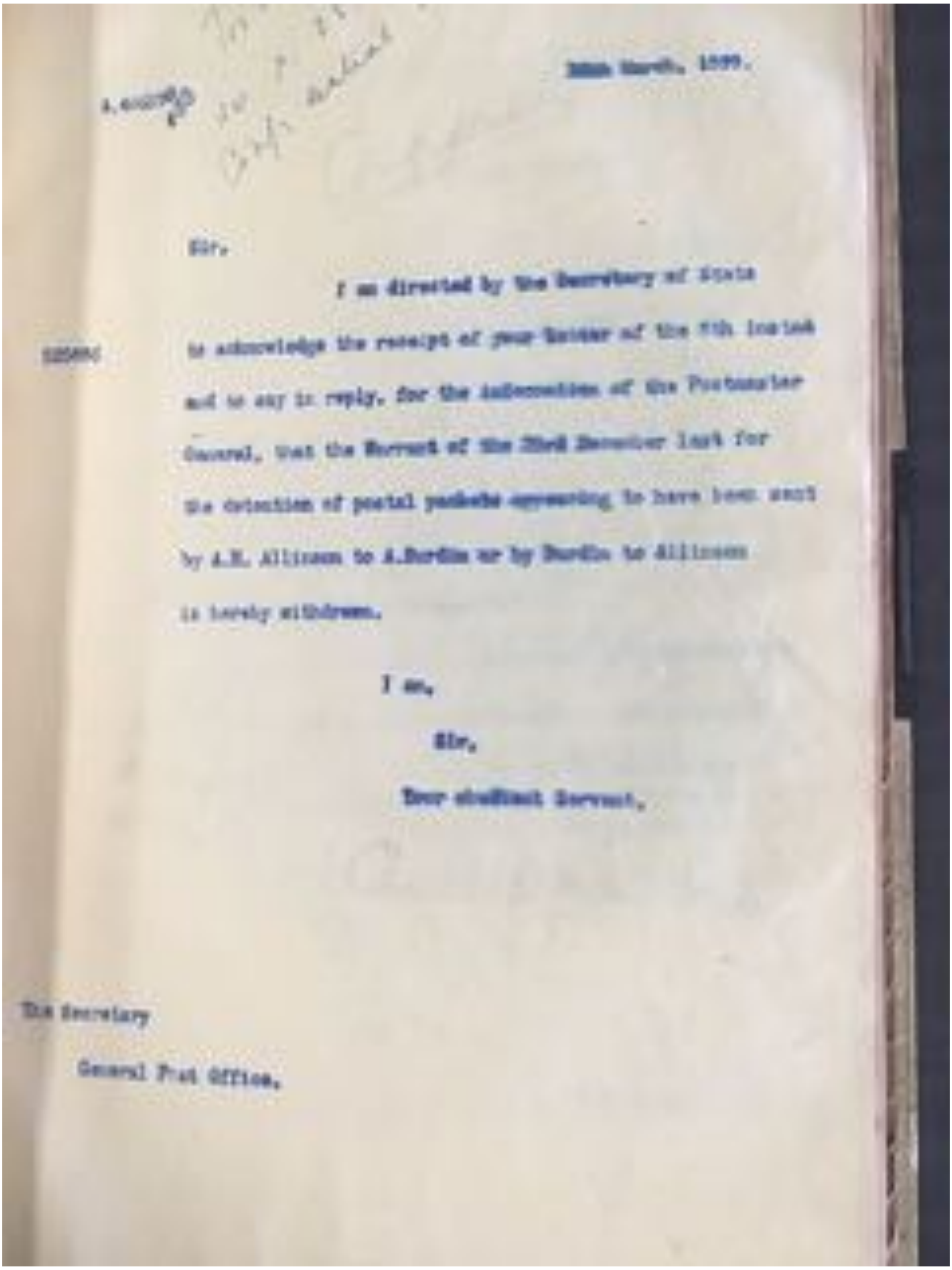
A4963

(Sd) H. H. Asquith

One of His Majesty's Principal Secretaries of State

To the Postmaster General and to any officer acting under his directions in this matter

Figure 3: Copy of a warrant signed by Asquith, later marked as cancelled, features alphanumeric reference number



[illegible] March, 1899.

A.[illegible]

Sir,

I am directed by the Secretary of State to acknowledge the receipt of your letter of the 5th instant

[illegible]

and to say in reply, for the information of the Postmaster General, that the Warrant of the 23rd December last for the detention of postal packets appearing to have been sent by A.H. Allison to A.Burdin or by Burdin to Allison is hereby withdrawn.

I am,

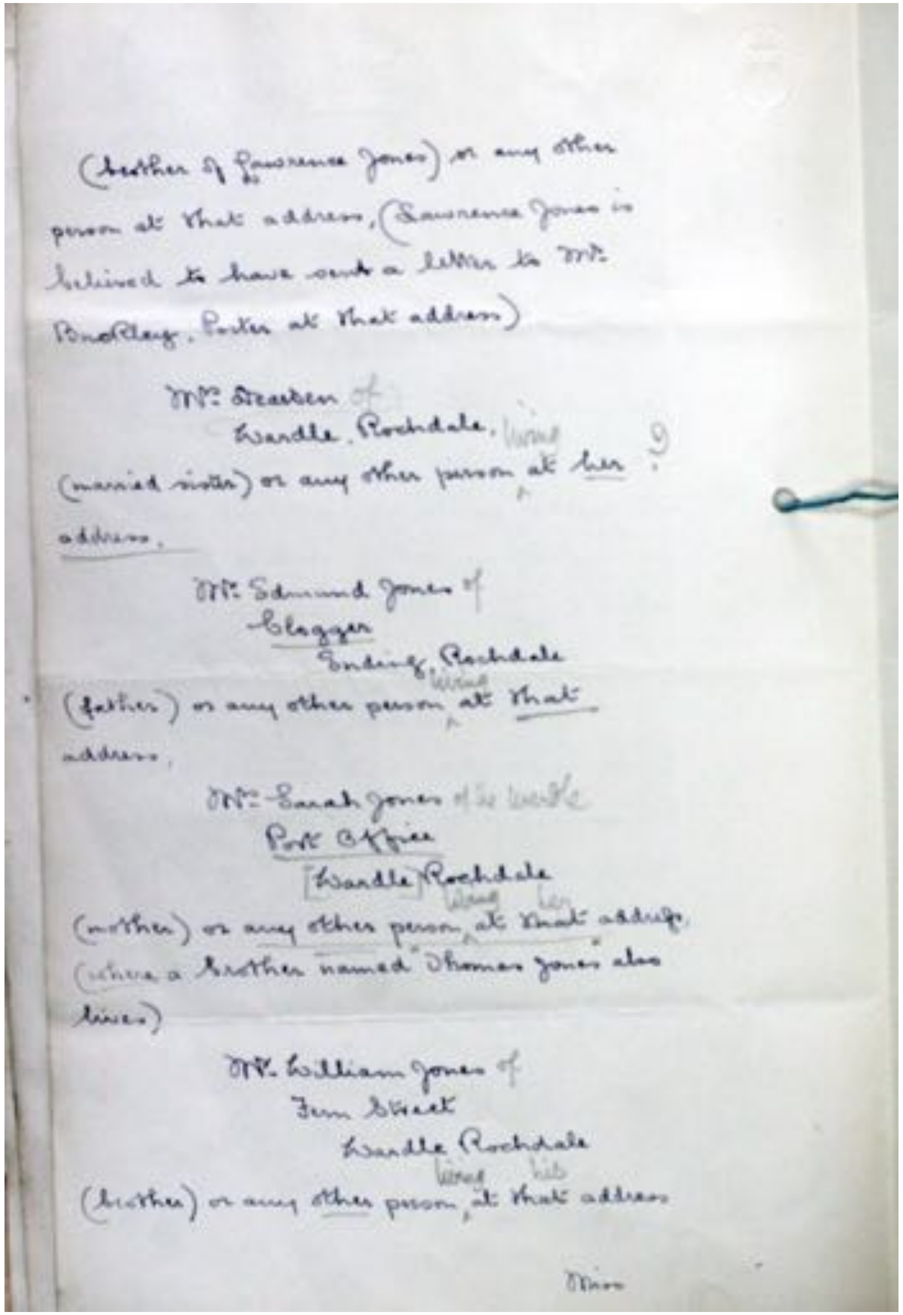
Sir,

Your obedient Servant,

The Secretary

General Post Office.

Figure 4: The typewriter makes the copybook redundant, March 1899.



(brother of Lawrence Jones) or any other person at that address, (Lawrence Jones is believed to have sent a letter to Mr Brockley, Porter at that address)

Mrs Dearden of
Wardle, Rochdale,

(married sister) or any other person living at her address.

Mr Edmund Jones of
Clogger
Ending, Rochdale

(father) or any other person living at that address,

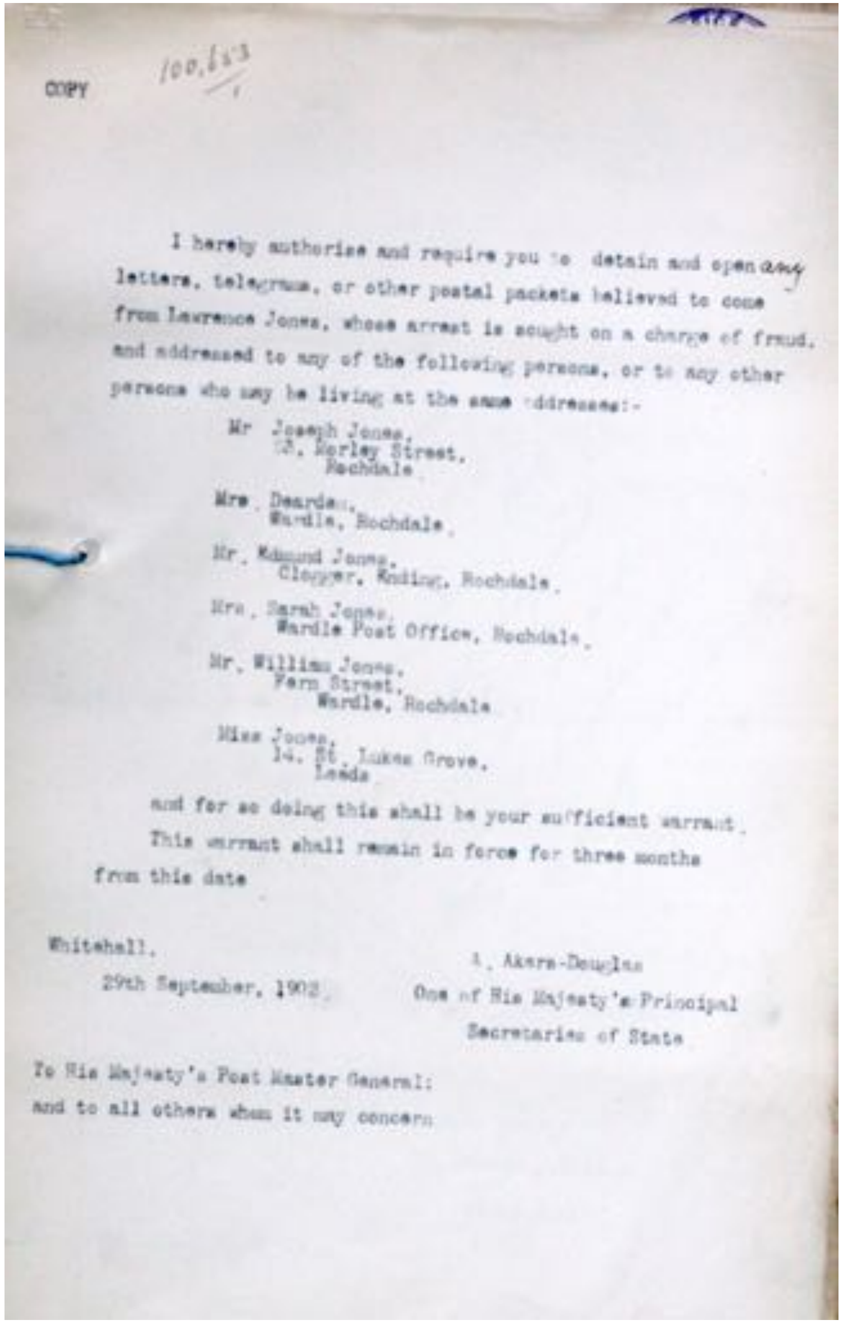
Mrs Sarah Jones of the Wardle
Post Office
Wardle Rochdale

(mother) or any other person living at her that address, (where a brother named "Thomas Jones" also lives)

Mr William Jones of
Fern Street
Wardle Rochdale

(brother) or any other person living at his that address

Mem



COPY 100,683/1

I hereby authorise and require you to detain and open any letters, telegrams, or other postal packets believed to come from Lawrence Jones, whose arrest is sought on a charge of fraud, and addressed to any of the following persons, or to any other persons who may be living at the same addresses:-

Mr Joseph Jones,
12, Morley Street,
Rochdale.

Mrs. Dearden,
Wardle, Rochdale.

Mr. Edmund Jones,
Clogger, Ending, Rochdale.

Mrs. Sarah Jones,
Wardle Post Office, Rochdale.

Mr. William Jones,
Fern Street,
Wardle, Rochdale

Miss Jones,
14. St. Lukes Grove,
Leeds

and for so doing this shall be your sufficient warrant.

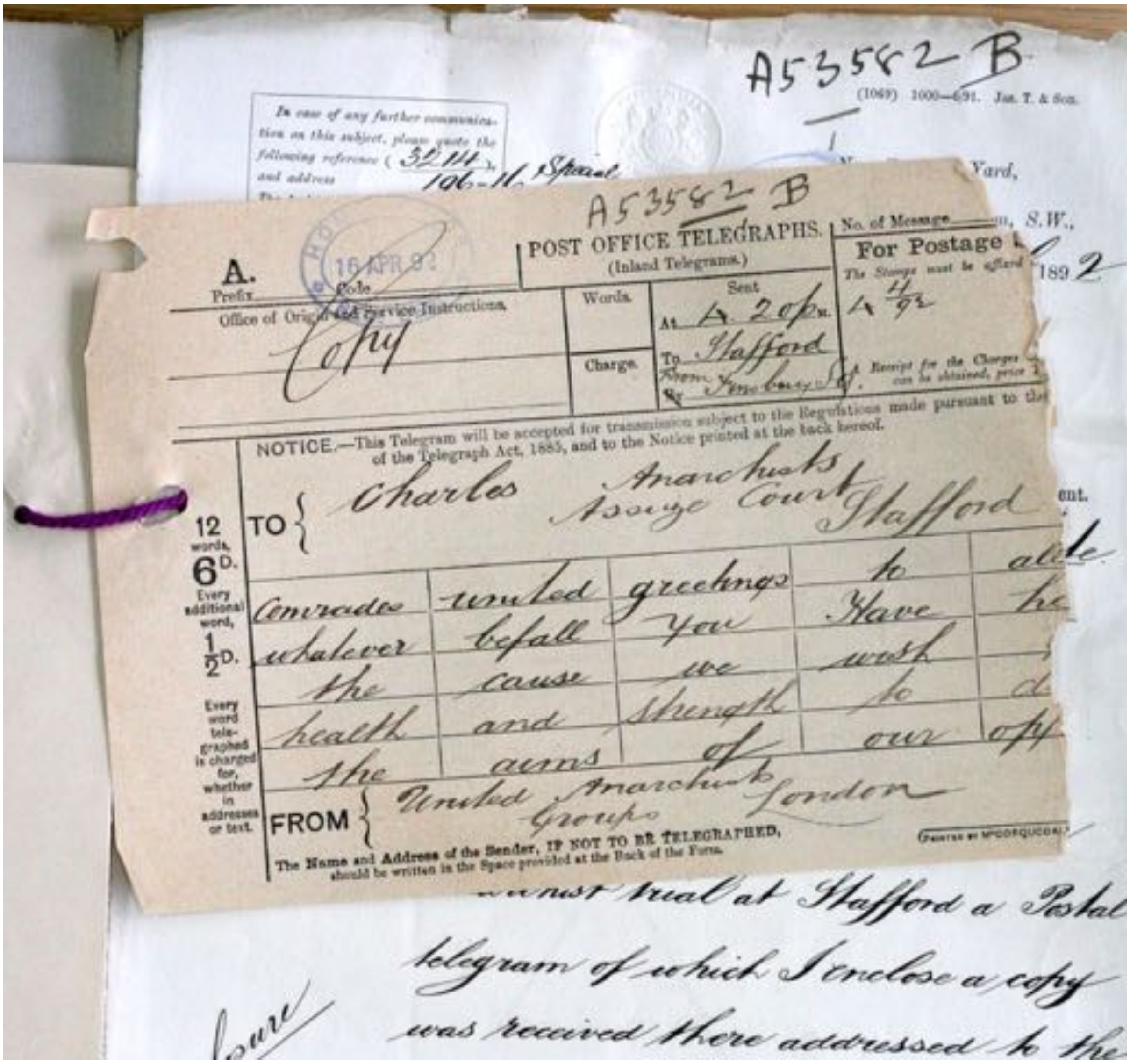
This warrant shall remain in force for three months from this date

Whitehall,
29th September, 1902.

A. Akers-Douglas
One of His Majesty's Principal
Secretaries of State

To His Majesty's Post Master General:
and to all others whom it may concern

Figure 5: a draft warrant in handwriting, and its typed copy, both in a tagged file, 29th September 1902



A53582 B

(1069) 1000—6/91. Jas. T. & Son.

In case of any further communication on this subject, please quote the following reference (32114) and address

106-11 Special

Yard,

S.W.,

189 2

A53582 B

POST OFFICE TELEGRAPHS.
(Inland Telegrams.)

A.
Prefix. Code.
Office of Origin and Service Instructions.
Copy

Words.

Charge.

Sent
At A 20 p.m.
To Stafford
From Finsbury
By

No. of Message

For Postage
The Stamps must be affixed
4/4/92

Receipt for the Charges can be obtained, price

NOTICE.—This Telegram will be accepted for transmission subject to the Regulations made pursuant to the of the Telegraph Act, 1885, and to the Notice printed at the back hereof.

12 words, 6D. Every additional word, ½D. Every word telegraphed is charged for, whether in addresses or text.

TO { Charles Anarchists Assize Court Stafford

Comrades	united	greetings	to	alle
whatever	befall	you	Have	he
the	cause	we	wish	
health	and	strength	to	d
the	aims	of	our	opp

FROM { United Anarchist Groups London

The Name and Address of the Sender, IF NOT TO BE TELEGRAPHED, should be written in the Space provided at the Back of the Form.

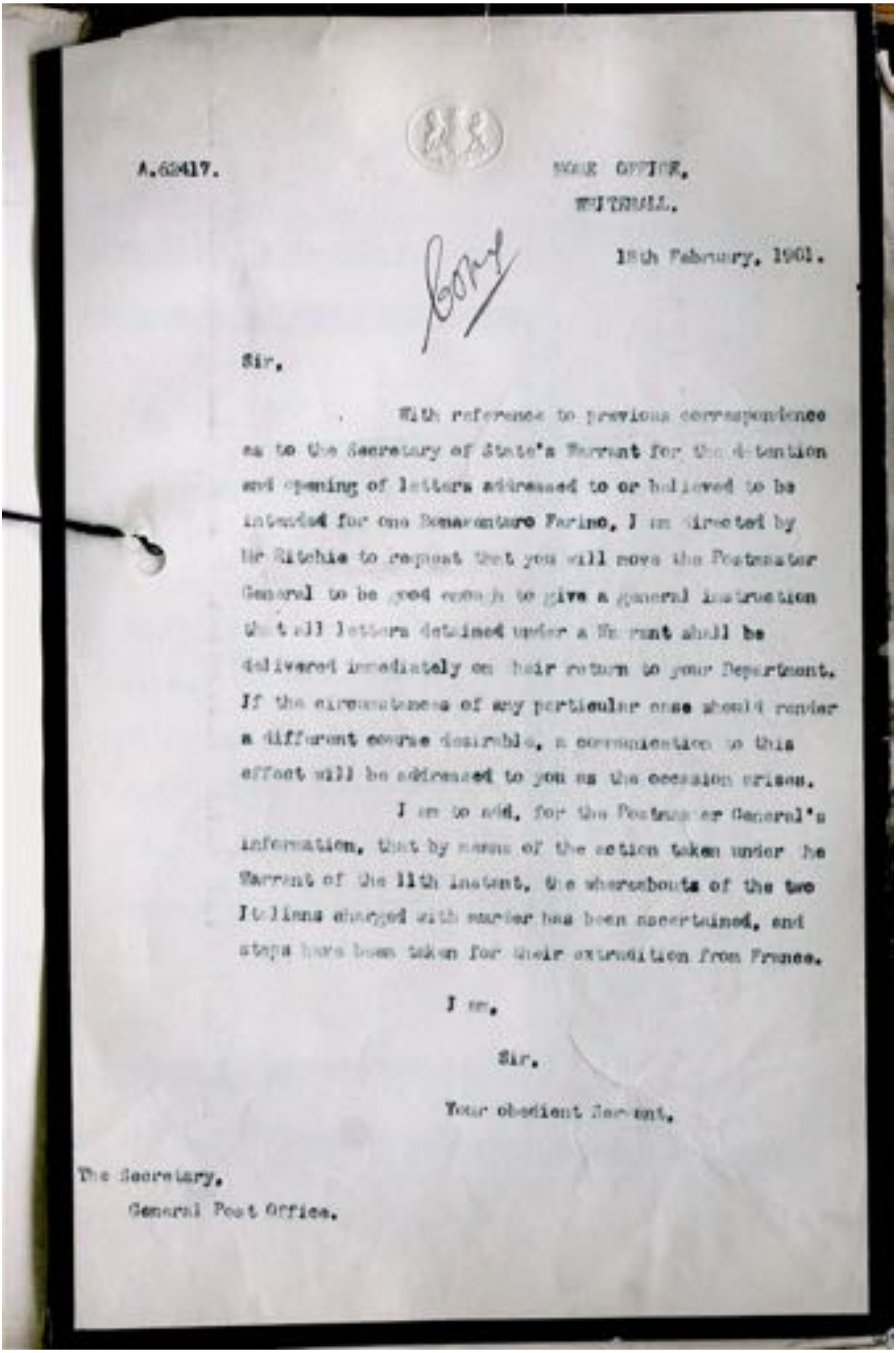
Printed by McCorquodale

ent.

against trial at Stafford a Postal telegram of which I enclose a copy was received there addressed to the

Enclosure

Figure 6: Copy of an intercepted telegram retrieved from storage for police purposes



A.62417.

HOME OFFICE,
WHITEHALL.

Copy

18th February, 1901.

Sir,

With reference to previous correspondence as to the Secretary of State's Warrant for the detention and opening of letters addressed to or believed to be intended for one Bonaventura Farino, I am directed by Mr Ritchie to request that you will move the Postmaster General to be good enough to give a general instruction that all letters detained under a Warrant shall be delivered immediately on their return to your Department. If the circumstances of any particular case should render a different course desirable, a communication to this effect will be addressed to you as the occasion arises.

I am to add, for the Postmaster General's information, that by means of the action taken under the Warrant of the 11th instant, the whereabouts of the two Italians charged with murder has been ascertained, and steps have been taken for their extradition from France.

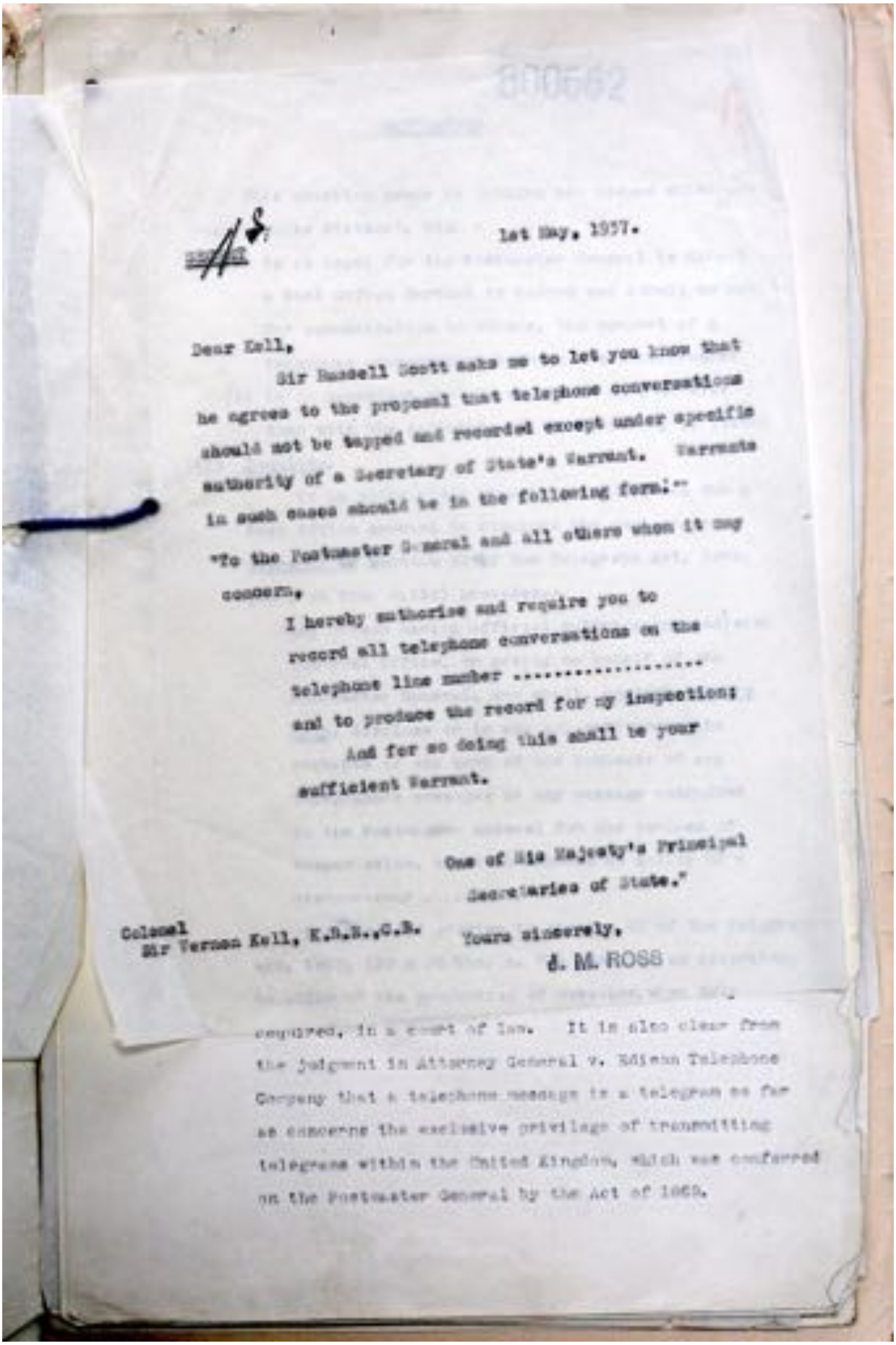
I am,

Sir,

Your obedient Servant,

The Secretary,
General Post Office.

Figure 7: Copy of typed letter from the Secretary, GPO, 1901



800562

1st May, 1937.

Dear Kell,

Sir Russell Scott asks me to let you know that he agrees to the proposal that telephone conversations should not be tapped and recorded except under specific authority of a Secretary of State's Warrant. Warrants in such cases should be in the following form:-

"To the Postmaster General and all others whom it may concern,

I hereby authorise and require you to record all telephone conversations on the telephone line number ....
and to produce the record for my inspection;

And for so doing this shall be your sufficient Warrant.

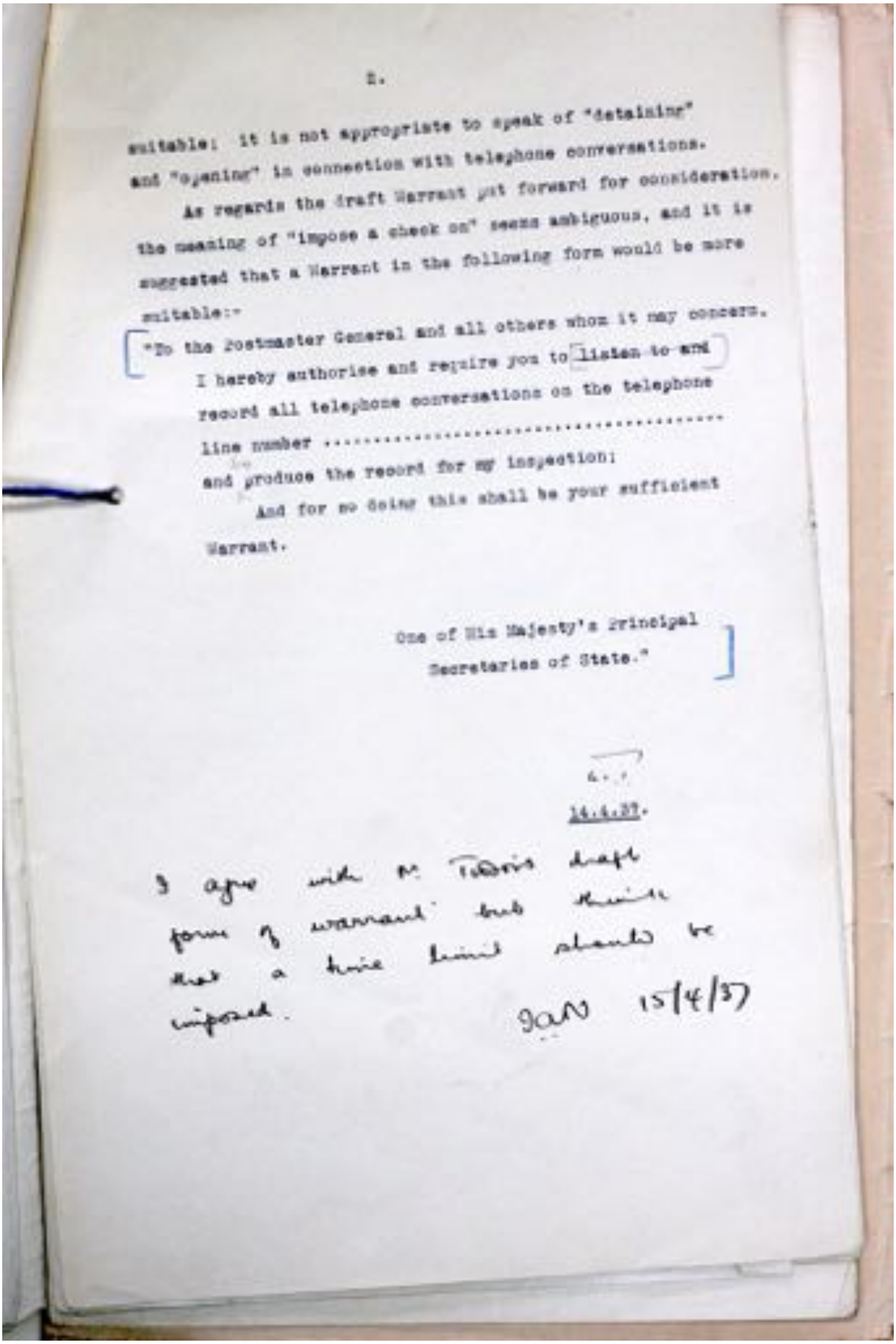
One of His Majesty's Principal
Secretaries of State."

Colonel
Sir Vernon Kell, K.B.E.,C.B.

Yours sincerely,
J. M. ROSS

required, in a court of law. It is also clear from the judgment in Attorney General v. Edison Telephone Company that a telephone message is a telegram so far as concerns the exclusive privilege of transmitting telegrams within the United Kingdom, which was conferred on the Postmaster General by the Act of 1869.

Figure 8: the first draft telephone warrant, 1st May 1937



2.

suitable: it is not appropriate to speak of "detaining" and "opening" in connection with telephone conversations.

As regards the draft Warrant put forward for consideration, the meaning of "impose a check on" seems ambiguous, and it is suggested that a Warrant in the following form would be more suitable:-

"To the Postmaster General and all others whom it may concern.

I hereby authorise and require you to ~~listen to and~~ record all telephone conversations on the telephone line number ....
and produce the record for my inspection;

And for so doing this shall be your sufficient Warrant.

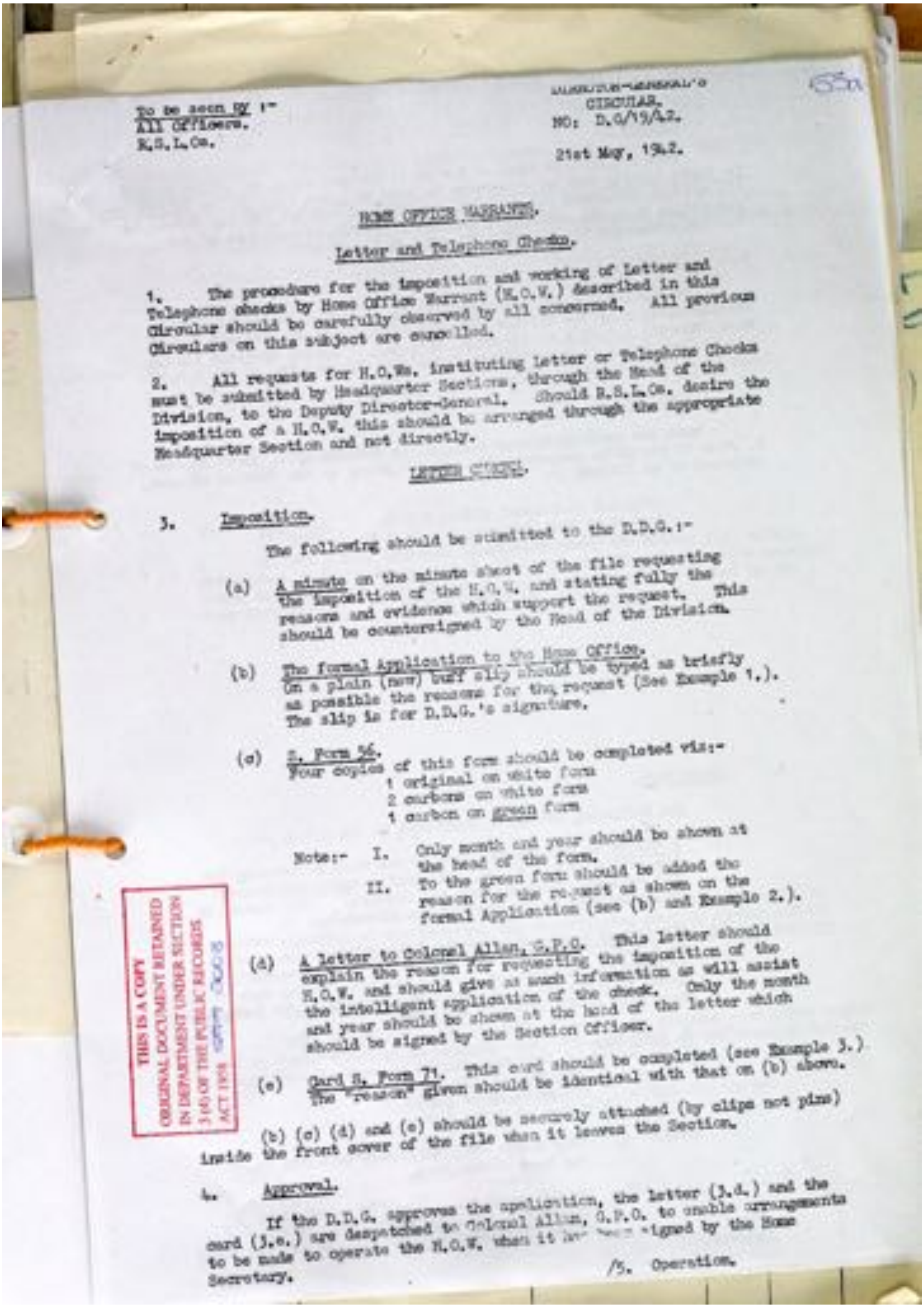
One of His Majesty's Principal
Secretaries of State."

14.4.37.

I agree with Mr [illegible] draft form of warrant but think that a time limit should be imposed.

JAN 15/4/37

Figure 9: Rejected draft warrant with comments, 14th April 1937



155a

To be seen by :-
All Officers.
R.S.L.Os.

DIRECTOR-GENERAL'S
CIRCULAR.
NO: D.G/19/42.

21st May, 1942.

HOME OFFICE WARRANTS.

Letter and Telephone Checks.

1. The procedure for the imposition and working of Letter and Telephone checks by Home Office Warrant (H.O.W.) described in this Circular should be carefully observed by all concerned. All previous Circulars on this subject are cancelled.

2. All requests for H.O.Ws. instituting Letter or Telephone Checks must be submitted by Headquarter Sections, through the Head of the Division, to the Deputy Director-General. Should R.S.L.Os. desire the imposition of a H.O.W. this should be arranged through the appropriate Headquarter Section and not directly.

LETTER CHECKS.

3. Imposition.

The following should be submitted to the D.D.G.:-

(a) A minute on the minute sheet of the file requesting the imposition of the H.O.W. and stating fully the reasons and evidence which support the request. This should be countersigned by the Head of the Division.

(b) The formal Application to the Home Office. On a plain (new) buff slip should be typed as briefly as possible the reasons for the request (See Example 1.). The slip is for D.D.G.'s signature.

(c) S. Form 56. Four copies of this form should be completed viz:-
1 original on white form
2 carbons on white form
1 carbon on green form

Note:- I. Only month and year should be shown at the head of the form.
II. To the green form should be added the reason for the request as shown on the formal Application (see (b) and Example 2.).

(d) A letter to Colonel Allan, G.P.O. This letter should explain the reason for requesting the imposition of the H.O.W. and should give as much information as will assist the intelligent application of the check. Only the month and year should be shown at the head of the letter which should be signed by the Section Officer.

(e) Card S. Form 71. This card should be completed (see Example 3.) The "reason" given should be identical with that on (b) above.

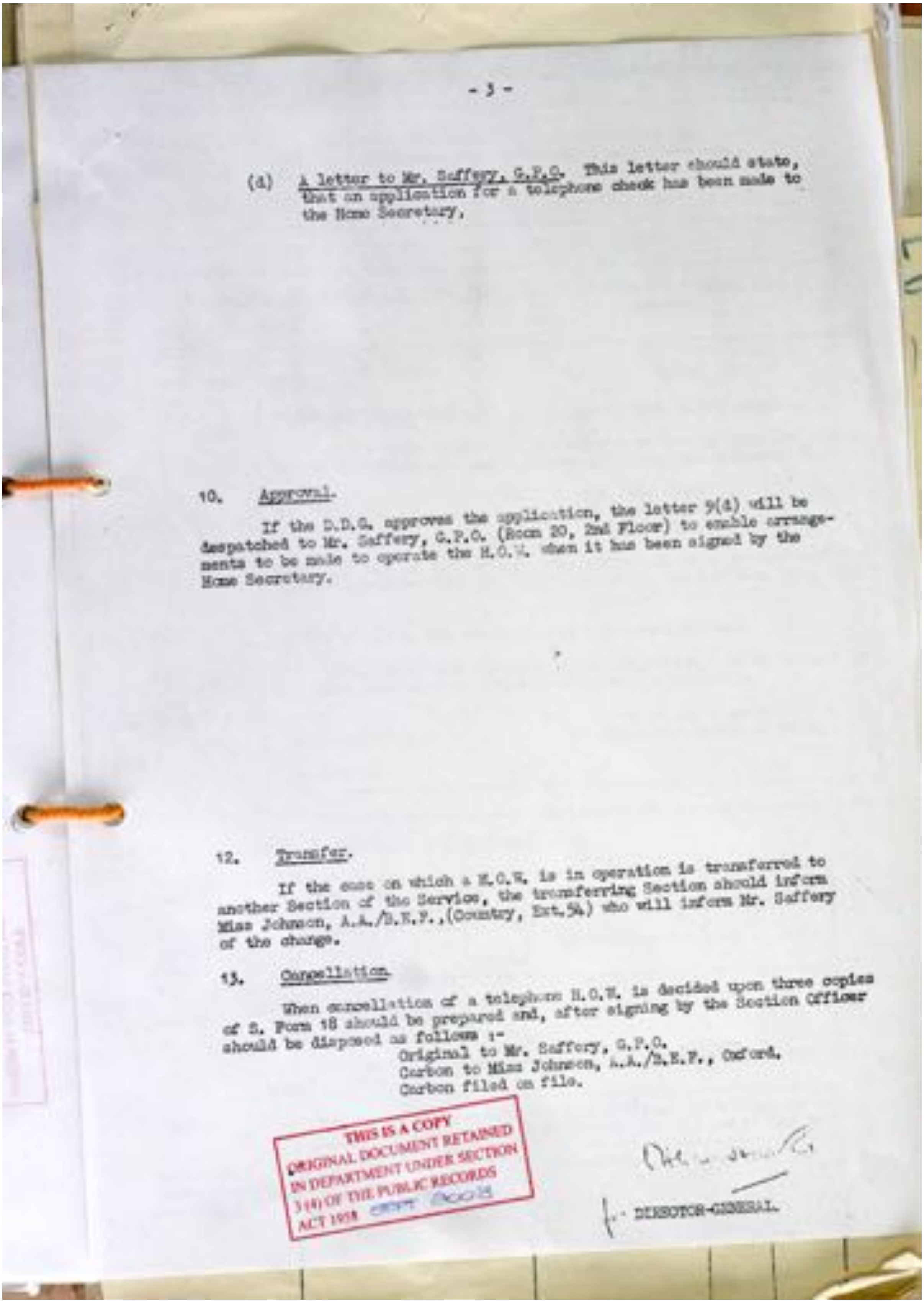
(b) (c) (d) and (e) should be securely attached (by clips not pins) inside the front cover of the file when it leaves the Section.

4. Approval.

If the D.D.G. approves the application, the letter (3.d.) and the card (3.e.) are despatched to Colonel Allan, G.P.O. to enable arrangements to be made to operate the H.O.W. when it has been signed by the Home Secretary.

/5. Operation.

Figure 10: New protocol for standardization of warrants, 21st May 1942, page 1 (page 2 is missing)



- 3 -

(d) A letter to Mr. Saffery, G.P.O. This letter should state, that an application for a telephone check has been made to the Home Secretary.

10. Approval.

If the D.D.G. approves the application, the letter 9(d) will be despatched to Mr. Saffery, G.P.O. (Room 20, 2nd Floor) to enable arrangements to be made to operate the H.O.W. when it has been signed by the Home Secretary.

12. Transfer.

If the case on which a H.O.W. is in operation is transferred to another Section of the Service, the transferring Section should inform Miss Johnson, A.A./B.E.F.,(Country, Ext.54) who will inform Mr. Saffery of the change.

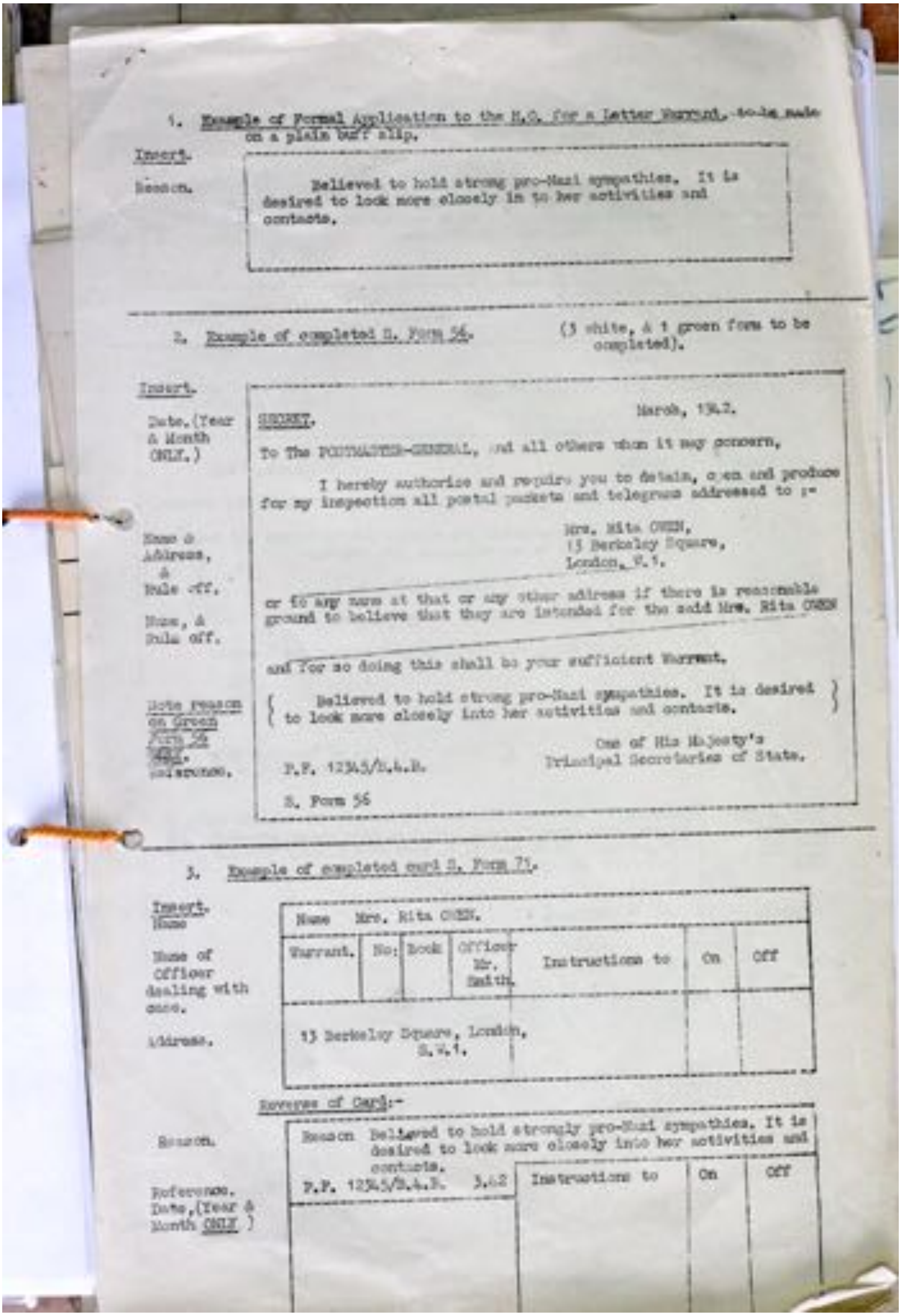
13. Cancellation.

When cancellation of a telephone H.O.W. is decided upon three copies of S. Form 18 should be prepared and, after signing by the Section Officer should be disposed as follows :-

Original to Mr. Saffery, G.P.O.
Carbon to Miss Johnson, A.A./B.E.F., Oxford.
Carbon filed on file.

f. DIRECTOR-GENERAL.

Figure 11: continuation of figure 10, page 3 of new protocol (page 2 missing)



1. Example of Formal Application to the H.O. for a Letter Warrant, to be made on a plain buff slip.

Insert.

Reason.

Believed to hold strong pro-Nazi sympathies. It is desired to look more closely in to her activities and contacts.

2. Example of completed S. Form 56. (3 white, & 1 green form to be completed).

Insert.

Date.(Year & Month ONLY.)

SECRET. March, 1942.

To The POSTMASTER-GENERAL, and all others whom it may concern,

I hereby authorise and require you to detain, open and produce for my inspection all postal packets and telegrams addressed to :-

Name & Address, & Rule off.

Mrs. Rita OWEN,
13 Berkeley Square,
London, W.1.

Name, & Rule off.

or to any name at that or any other address if there is reasonable ground to believe that they are intended for the said Mrs. Rita OWEN

and for so doing this shall be your sufficient Warrant.

Note reason on Green Form 56 ONLY.

{ Believed to hold strong pro-Nazi sympathies. It is desired to look more closely into her activities and contacts. }

Reference.

P.F. 12345/B.4.B.

One of His Majesty's
Principal Secretaries of State.

S. Form 56

3. Example of completed card S. Form 71.

Insert. Name

Name of Officer dealing with case.

Address.

Name Mrs. Rita OWEN.						
Warrant.	No:	Book	Officer Mr. Smith	Instructions to	On	Off
13 Berkeley Square, London, S.W.1.						

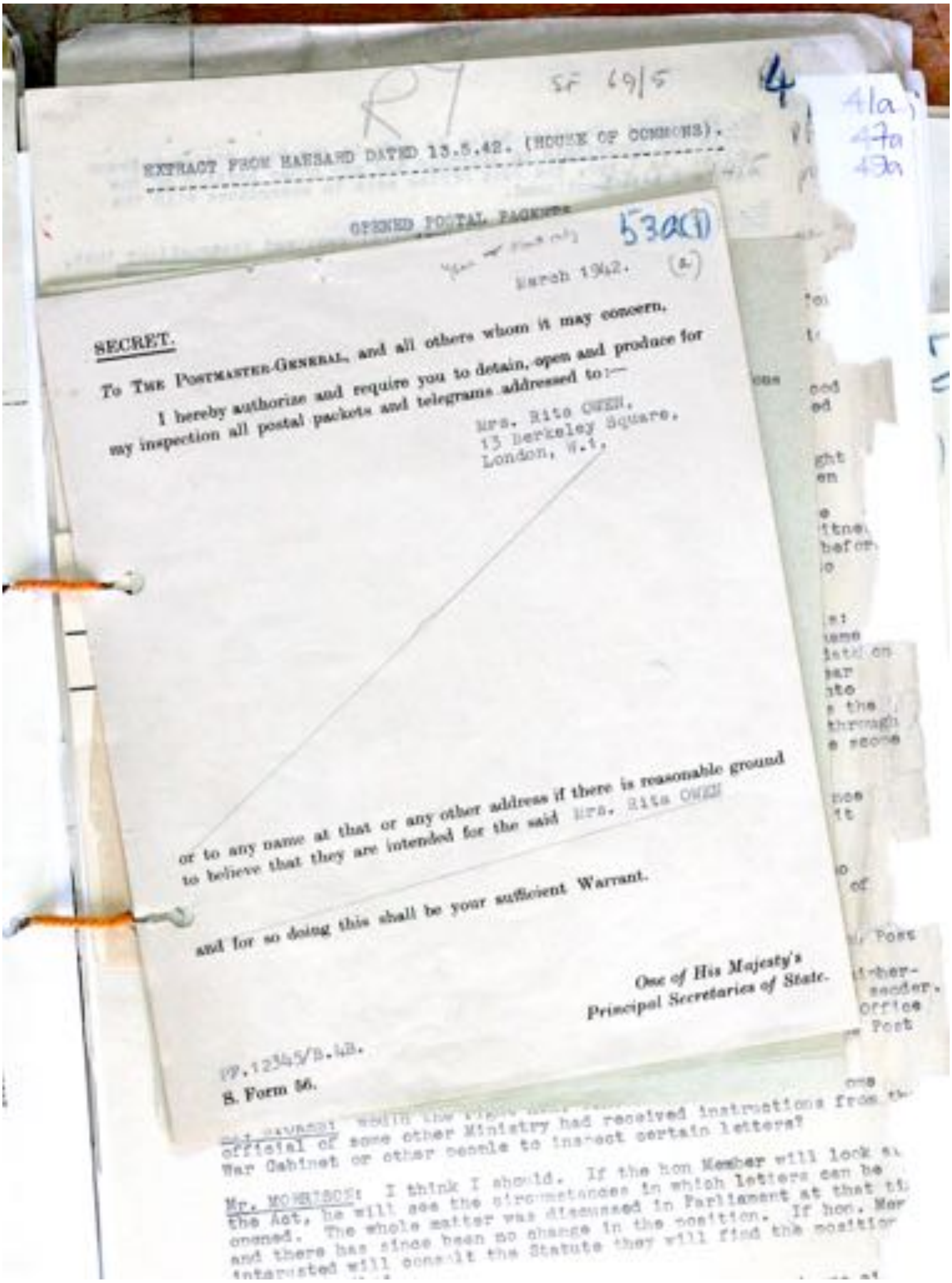
Reverse of Card:-

Reason.

Reference. Date,(Year & Month ONLY)

Reason Believed to hold strongly pro-Nazi sympathies. It is desired to look more closely into her activities and contacts.			
P.F. 12345/B.4.B. 3.42	Instructions to	On	Off

Figure 12: Formatting interception warrants and cards, continuation of figure 10.



R7 SF 69/5 4

41a 47a 49a

EXTRACT FROM HANSARD DATED 13.5.42. (HOUSE OF COMMONS).

OPENED POSTAL PACKETS

530(1)

March 1942. (a)

SECRET.

To The Postmaster-General, and all others whom it may concern.

I hereby authorize and require you to detain, open and produce for my inspection all postal packets and telegrams addressed to:—

Mrs. Rita OWEN,
13 Berkeley Square,
London, W.1.

or to any name at that or any other address if there is reasonable ground to believe that they are intended for the said Mrs. Rita OWEN

and for so doing this shall be your sufficient Warrant.

One of His Majesty's
Principal Secretaries of State.

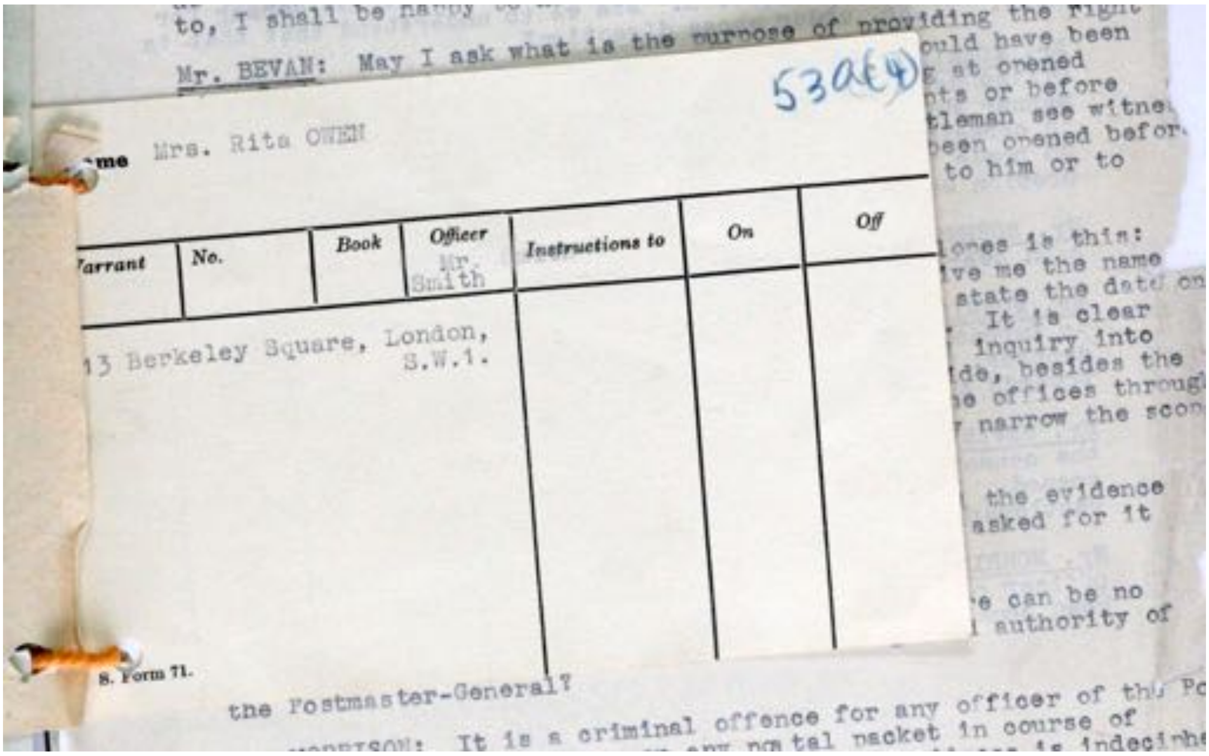
PF.12345/B.4B.

S. Form 56.

official of some other Ministry had received instructions from the War Cabinet or other people to inspect certain letters?

Mr. MORRISON: I think I should. If the hon Member will look at the Act, he will see the circumstances in which letters can be opened. The whole matter was discussed in Parliament at that time and there has since been no change in the position. If hon. Members interested will consult the Statute they will find the position

Figure 13: Sample warrant S Form 56, March 1942



to, I shall be happy ...

Mr. BEVAN: May I ask what is the purpose of providing the right ... ould have been ... g at opened ... nts or before ... tleman see witne ... been opened befor ... to him or to

53a(4)

Name Mrs. Rita OWEN

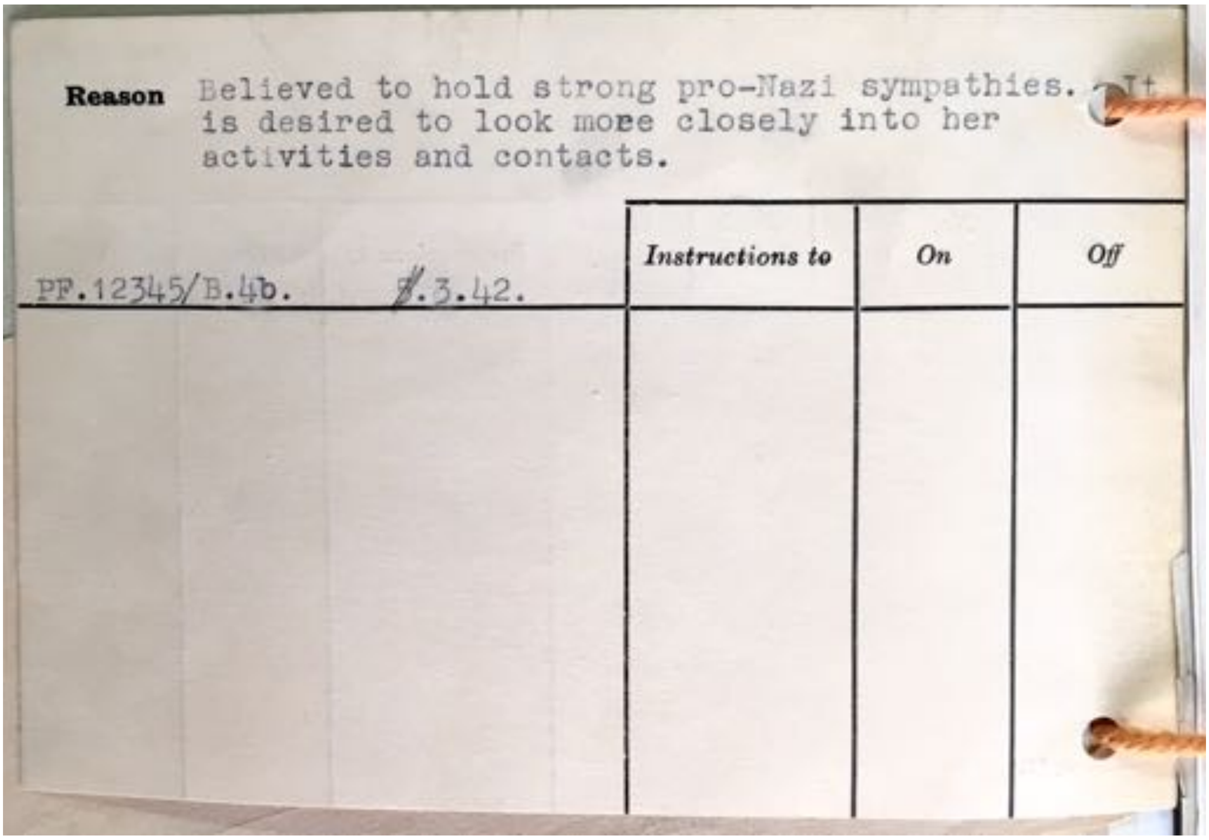
Warrant	No.	Book	Officer	Instructions to	On	Off
			Mr. Smith			
13 Berkeley Square, London, S.W.1.						

S. Form 71.

... lores is this: ... ive me the name ... state the date on ... It is clear ... inquiry into ... ide, besides the ... he offices throug ... narrow the scop ... the evidence ... asked for it ... e can be no ... authority of

the Postmaster-General?

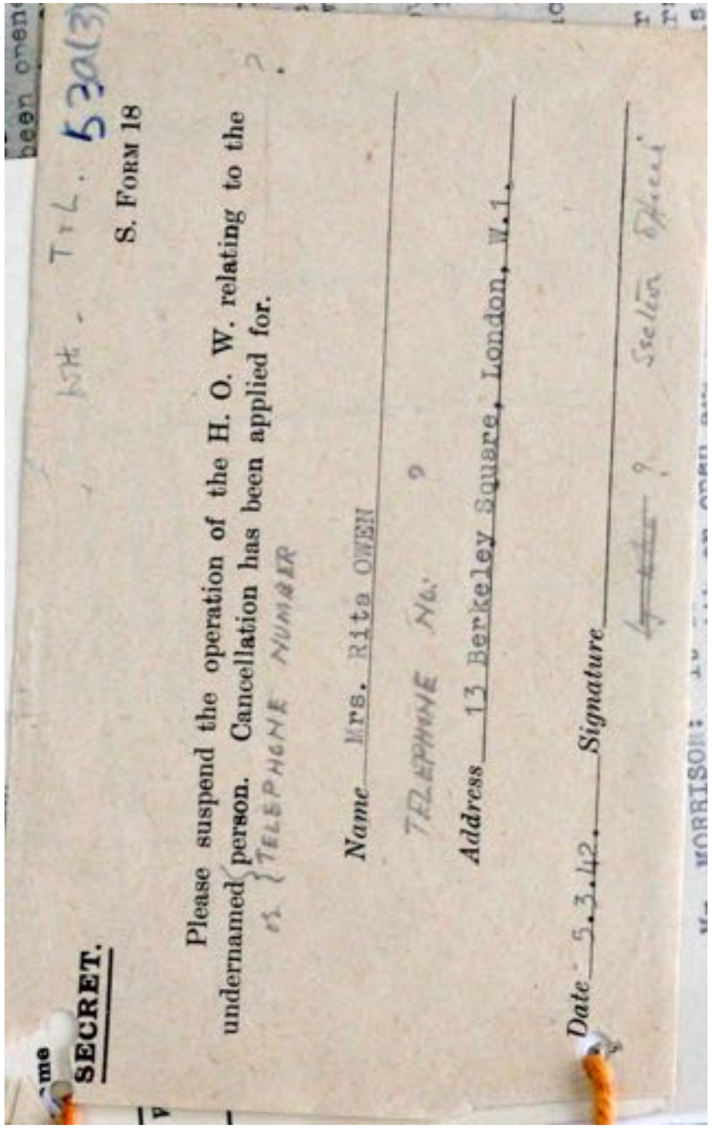
...ORRISON: It is a criminal offence for any officer of the Po... any postal packet in course of ... is indeciphe...



Reason Believed to hold strong pro-Nazi sympathies. It is desired to look moee closely into her activities and contacts.

		Instructions to	On	Off
PF.12345/B.4b.	8.3.42.			

Figure 14 & 15: Pre-printed sample interception card, two-sided, 1942



SECRET.

S. FORM 18

WH. T+L. 53a(3)

Please suspend the operation of the H. O. W. relating to the undernamed person. Cancellation has been applied for.
or TELEPHONE NUMBER

Name Mrs. Rita OWEN

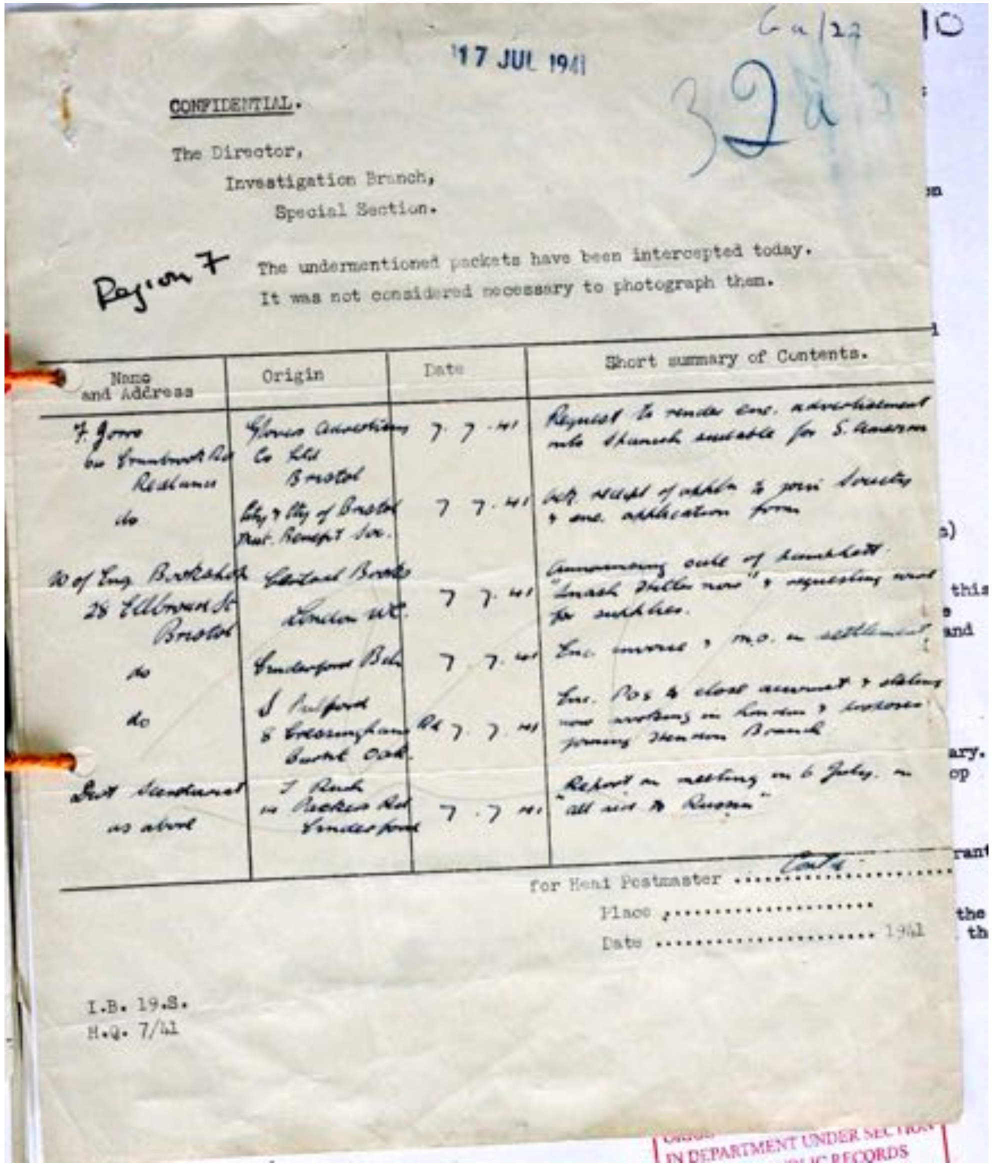
TELEPHONE No. ?

Address 13 Berkeley Square, London, W.1.

Date 5.3.42. Signature

~~[illegible]~~ ? Section Officer

Figure 15: Cancellation forms for interception warrants



'17 JUL 1941

CONFIDENTIAL.

32a 6a/22

The Director,
Investigation Branch,
Special Section.

Region 7

The undermentioned packets have been intercepted today.
It was not considered necessary to photograph them.

Name and Address	Origin	Date	Short summary of Contents.
F. Jones 66 Frenchwood Rd Redland	Glovers Advertising Co Ltd Bristol	7.7.41	Request to render Eng. advertisement into Spanish suitable for S. America
do	City & Cty of Bristol Mut. Benefit Soc.	7.7.41	Ack. receipt of cheque to join Society + enc. application form
Sec of Eng. Bookshop 28 Ellbroad St Bristol	Central Books London WC.	7.7.41	Announcing sale of pamphlet "Smash Hitler now", + requesting [illegible] for [illegible].
do	Frenchay Bk	7.7.41	Enc. invoice, M.O. in settlement
do	J Pulford 8 Greenbank Rd Burnt Oak.	7.7.41	Enc. P.O. to close account + stating now working in London & [illegible] joining Hendon Branch
Dist. Secretary as above	J Rush 11 Pucker Rd Fishponds	7.7.41	Report on meeting on 6 July on "all aid to Russia"

Contd.

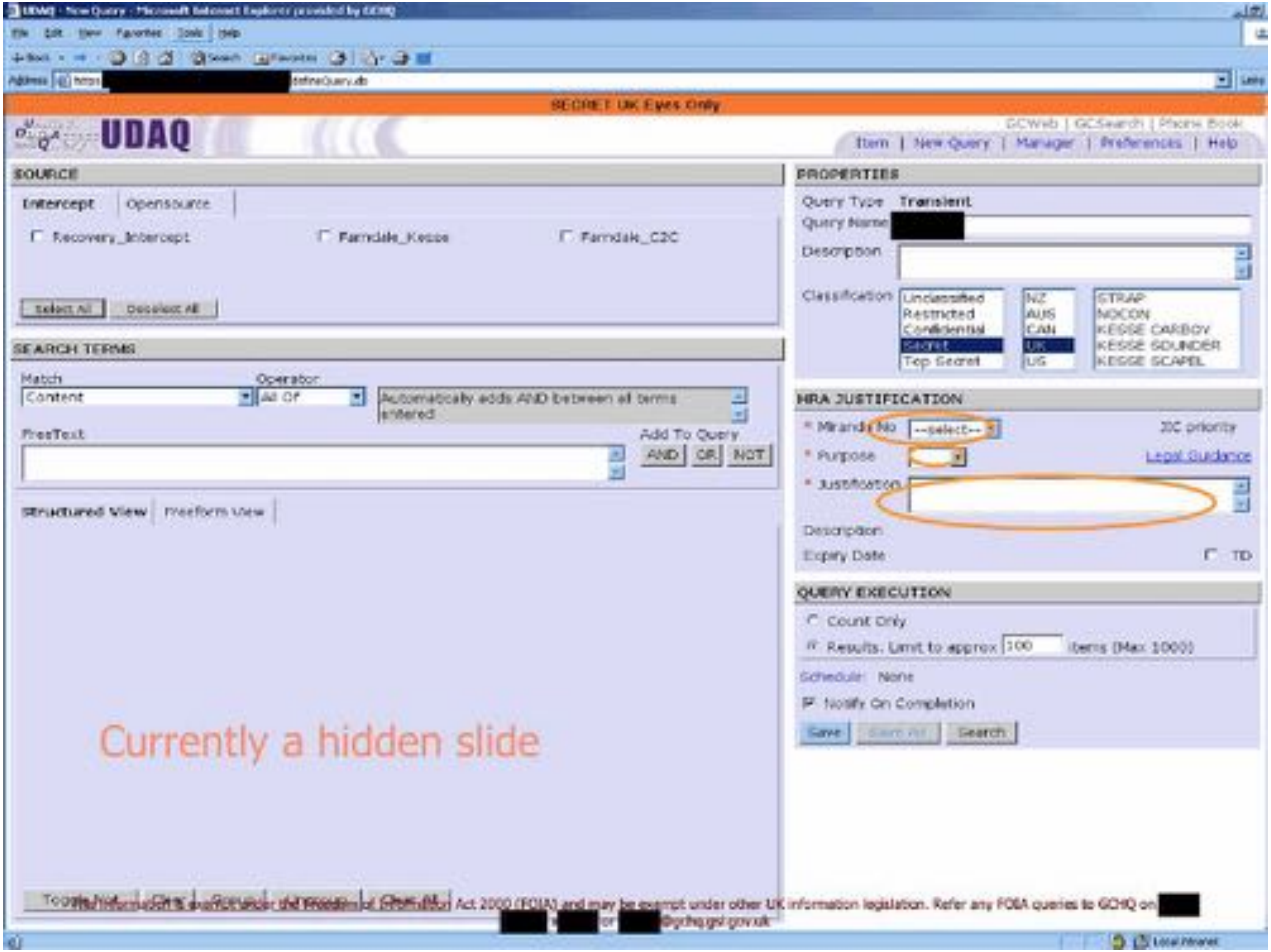
for Head Postmaster ....

Place ....

Date 1941

I.B. 19.S.
H.Q. 7/41

Figure 16: Feedback on intercepted packets under a warrant, 17 July 1941



UDAQ - New Query - Microsoft Internet Explorer provided by GCHQ
File Edit View Favorites Tools Help
Address https [redacted] defineQuery.do
SECRET UK Eyes Only
UDAQ
GCWeb | GCSearch | Phone Book
Item | New Query | Manager | Preferences | Help

SOURCE

Intercept | Opensource

□ Recovery_Intercept □ Farndale_Kesse □ Farndale_C2C

Select All | Deselect All

SEARCH TERMS

Match: Content
Operator: All Of
Automatically adds AND between all terms entered

FreeText

Add To Query: AND | OR | NOT

Structured View | Freeform View

Currently a hidden slide

Toggle Not | Clear | Group | Ungroup | Clear All

PROPERTIES

Query Type: Transient
Query Name: [redacted]
Description

Classification: Unclassified, Restricted, Confidential, Secret, Top Secret | NZ, AUS, CAN, UK, US | STRAP, NOCON, KESSE CARBOY, KESSE SOUNDER, KESSE SCAPEL

HRA JUSTIFICATION

* Miranda No: --select-- JIC priority
* Purpose Legal Guidance
* Justification
Description
Expiry Date □ TD

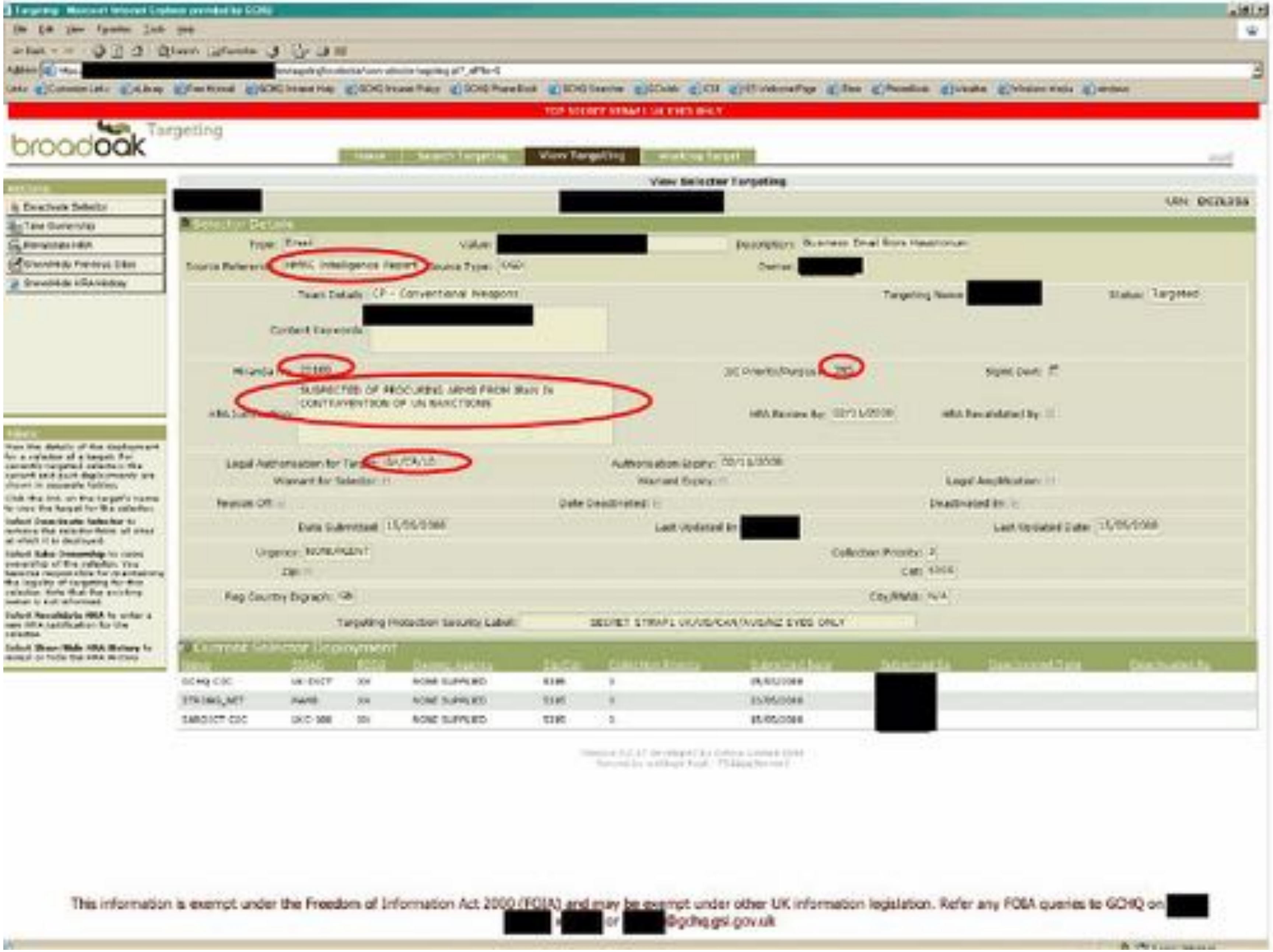
QUERY EXECUTION

○ Count Only
● Results. Limit to approx 100 items (Max 1000)
Schedule: None
☑ Notify On Completion

Save | Save As | Search

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] [redacted] [redacted] or [redacted]@gchq.gsi.gov.uk

Figure 17: UDAQ interface



TOP SECRET STRAP1 UK EYES ONLY

broadoak Targeting

View Selector Targeting

[redacted] [redacted] URN: 0026338

Selector Details

Type: Email Value: [redacted] Description: Business Email from [illegible]

Source Reference: HMRC Intelligence Report Source Type: [illegible] Owner: [redacted]

Team Details: CP - Conventional Weapons Targeting Name: [redacted] Status: Targeted

Content Keywords: [redacted]

Miranda No: 20160 JIC Priority/Purpose: [illegible] Signal Dept: [illegible]

HRA Justification: SUSPECTED OF PROCURING ARMS FROM [illegible] IN CONTRAVENTION OF UN SANCTIONS

HRA Review By: 03/11/2008 HRA Revalidated By: [illegible]

Legal Authorisation for Target: [illegible] Authorisation Expiry: 03/11/2008

Warrant for Selector: [illegible] Warrant Expiry: [illegible] Legal Amplification: [illegible]

Reason Off: [illegible] Date Deactivated: [illegible] Deactivated By: [illegible]

Date Submitted: 15/05/2008 Last Updated By: [redacted] Last Updated Date: 15/05/2008

Urgency: NON URGENT Collection Priority: 2

Zip: [illegible] Cat: 5306

Reg Country Digraph: GB City/Mobile: N/A

Targeting Protection Security Label: SECRET STRAP1 UK/US/CAN/AUS/NZ EYES ONLY

Current Selector Deployment

[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
GCHQ CDC	UK-EXCT	XX	NONE SUPPLIED	5186	3	05/05/2008	[redacted]		
STRING_NET	[illegible]	XX	NONE SUPPLIED	5185	3	15/05/2008			
SABOICT CDC	UKC-308	XX	NONE SUPPLIED	5185	3	15/05/2008			

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] [redacted] [redacted] or [redacted]@gchq.gsi.gov.uk

Figure 18: An active Broad Oak selector

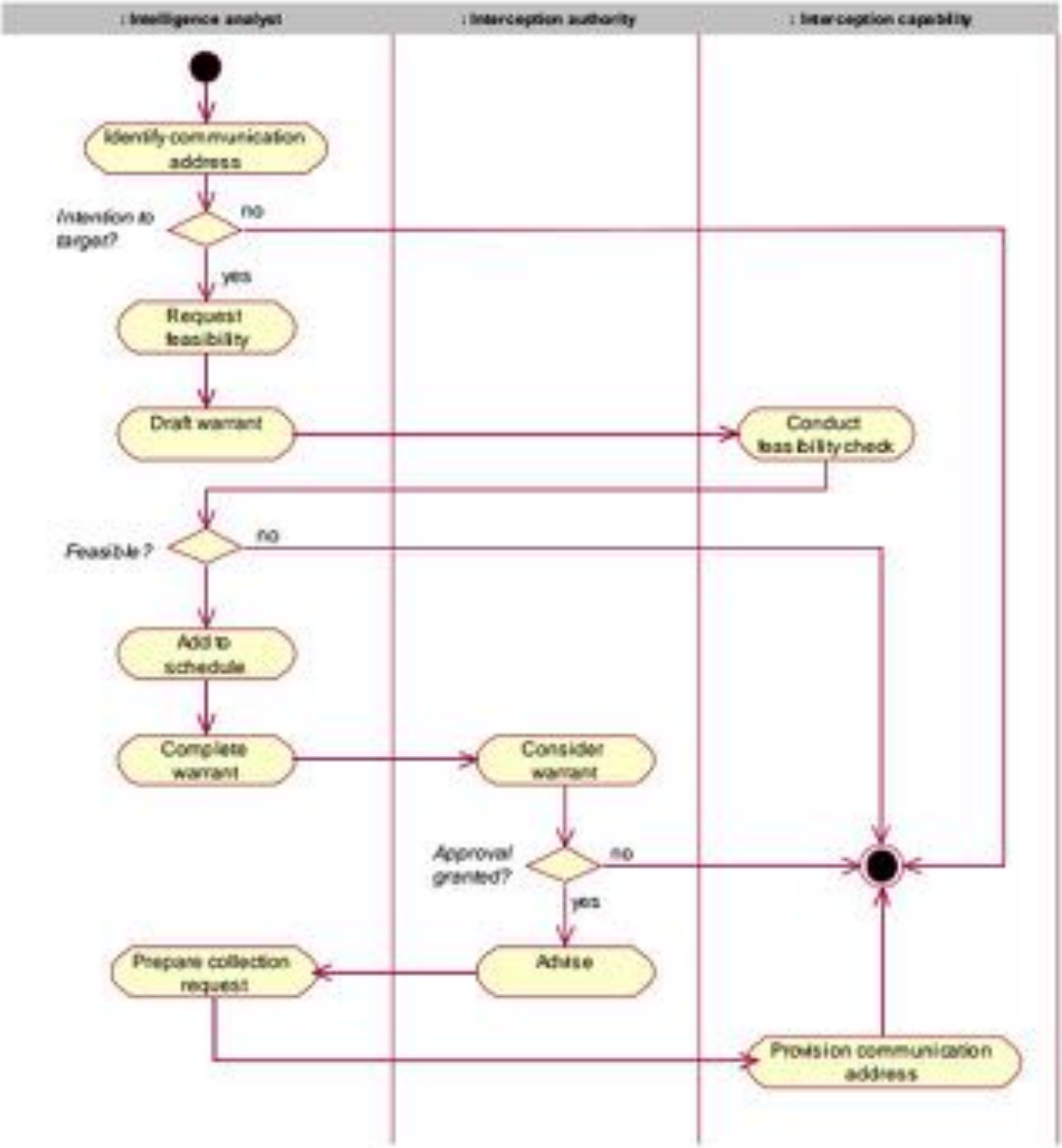


Figure 19: the procedure for instigating 'internal' interception

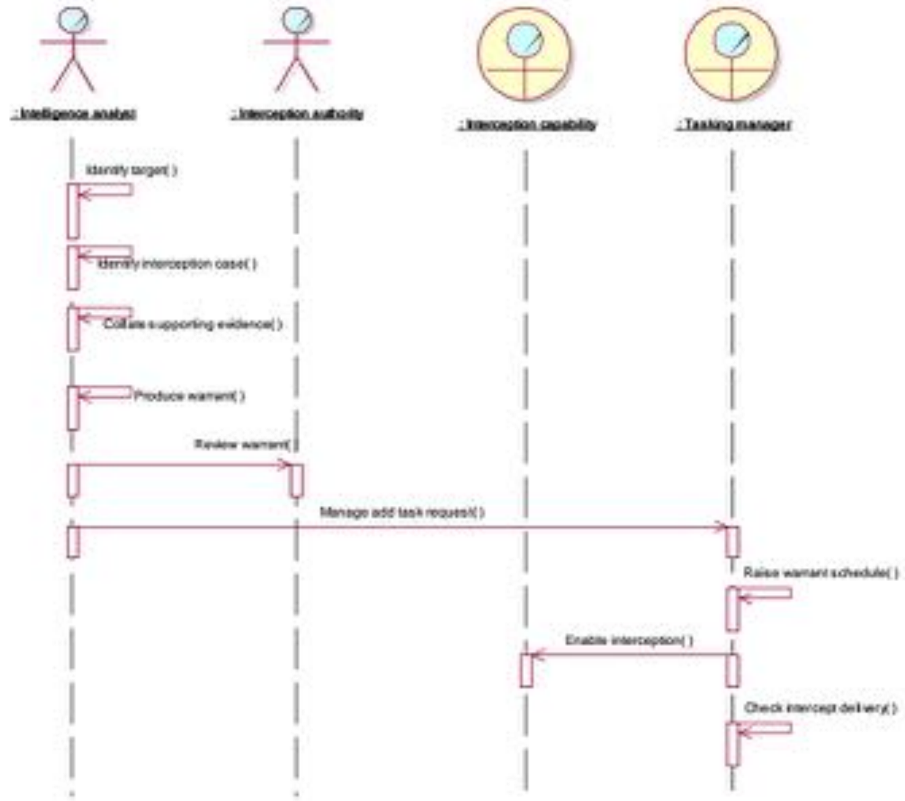

: Intelligence analyst
: Interception authority
: Interception capability
: Tasking manager
Identify target( )
Identify interception case( )
Collate supporting evidence( )
Produce warrant( )
Review warrant( )
Manage add task request( )
Raise warrant schedule( )
Enable interception( )
Check intercept delivery( )

Figure 20: the 'business process' of interception streams

6.3 Business Workers and Business Actors

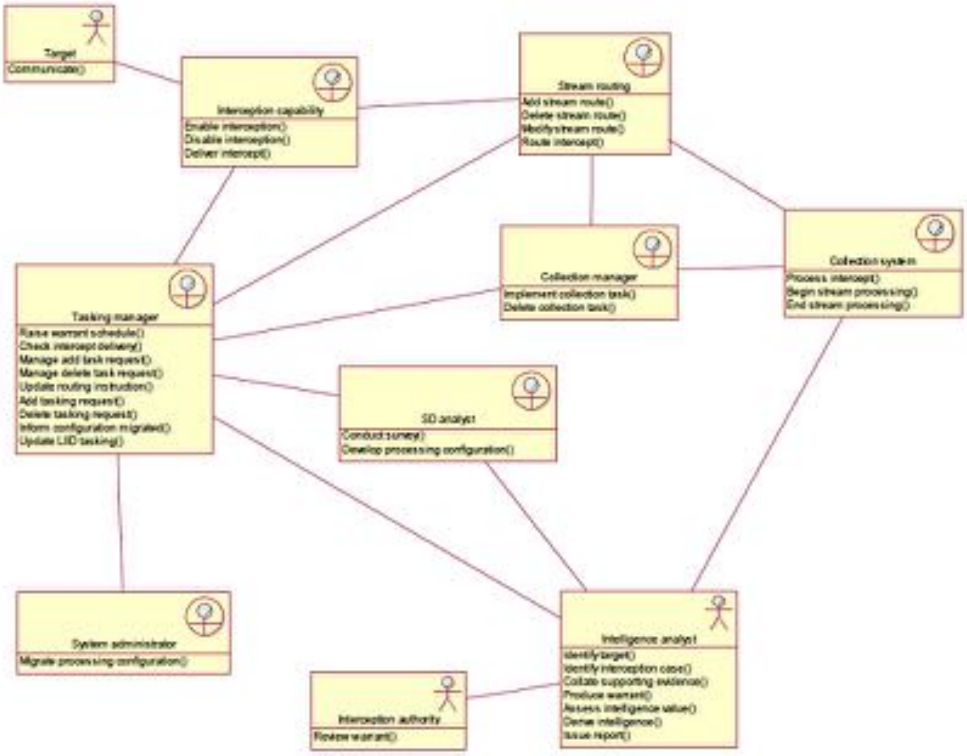
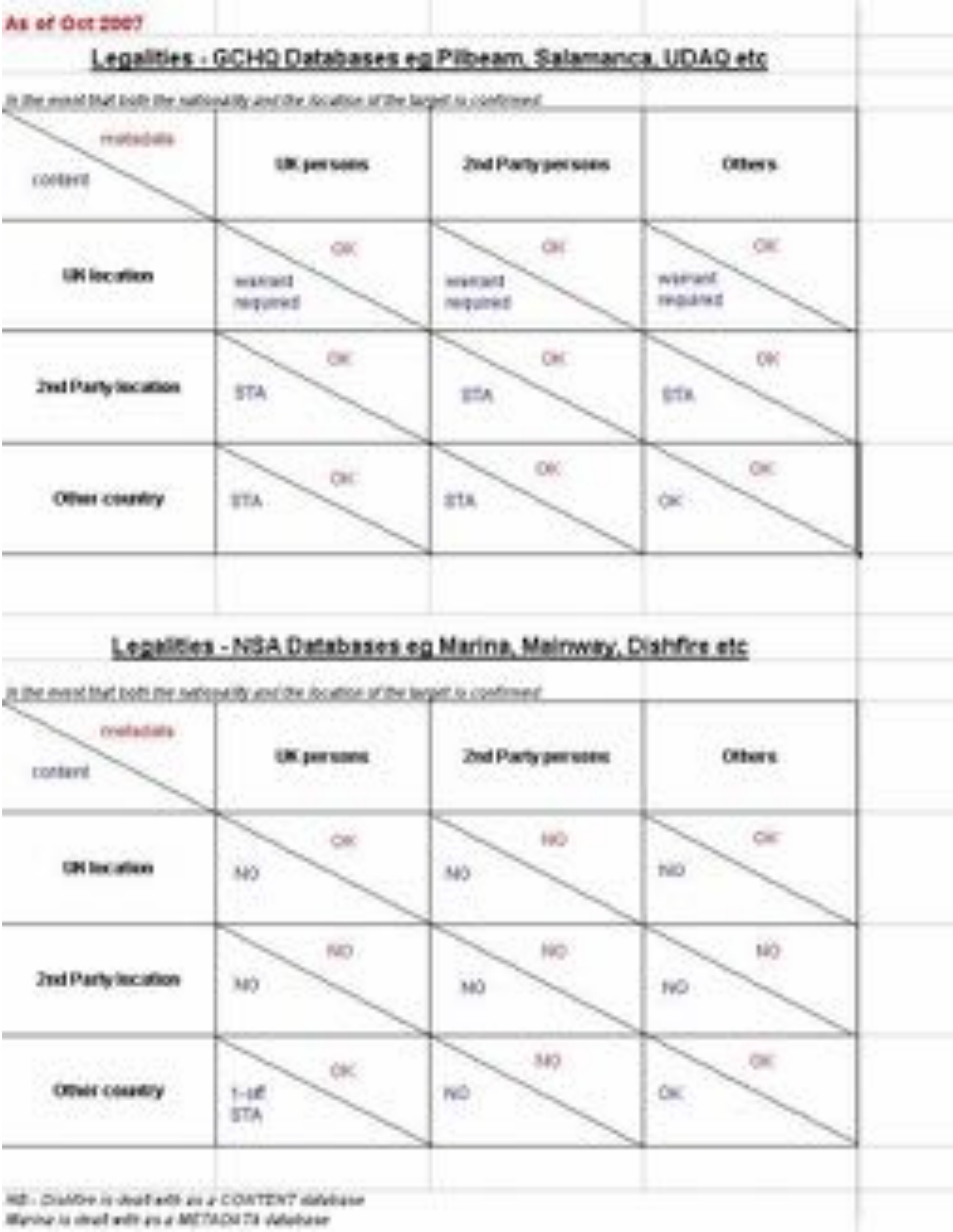


Figure 21: the operational process of interception, beyond the legal framework



As of Oct 2007

Legalities - GCHQ Databases eg Pilbeam, Salamanca, UDAQ etc

In the event that both the nationality and the location of the target is confirmed

metadata content	UK persons	2nd Party persons	Others
UK location	OK warrant required	OK warrant required	OK warrant required
2nd Party location	OK STA	OK STA	OK STA
Other country	OK STA	OK STA	OK OK

Legalities - NSA Databases eg Marina, Mainway, Dishfire etc

In the event that both the nationality and the location of the target is confirmed

metadata content	UK persons	2nd Party persons	Others
UK location	OK NO	NO NO	OK NO
2nd Party location	NO NO	NO NO	NO NO
Other country	OK 1-off STA	NO NO	OK OK

NB - Dishfire is dealt with as a CONTENT database
Marina is dealt with as a METADATA database

Figure 22: the 'legalities table'