Regulating the Technological Actor

How governments tried to transform the technology and the market for cryptography and cryptographic services and the implications for the regulation of information and communications technologies

Ian R Hosein
The London School of Economics and Political Science
Submitted for a PhD in Information Systems

144910

Abstract

The formulation, adoption, and transformation of policy involves the interaction of actors as they negotiate, accept, and reject proposals. Traditional studies of policy discourse focus on social actors. By studying cryptography policy discourses, I argue that considering both social and technological actors in detail enriches our understanding of policy discourse.

The case-based research looks at the various cryptography policy strategies employed by the governments of the United States of America and the United Kingdom. The research method is qualitative, using hermeneutics to elucidate the various actors' interpretations. The research aims to understand policy discourse as a contest of principles involving various government actors advocating multiple regulatory mechanisms to maintain their surveillance capabilities, and the reactions of industry actors, non-governmental organisations, parliamentarians, and epistemic communities.

I argue that studying socio-technological discourse helps us to understand the complex dynamics involved in regulation and regulatory change. Interests and alignments may be contingent and unstable. As a result, technologies can not be regarded as mere representations of social interests and relationships.

By capturing the interpretations and articulations of social and technological actors we may attain a better understanding of the regulatory landscape for information and communications technologies.

Table of Contents

Figures and Tables

Dedication and Memoriam

To my students over the years, for their tolerance, patience, and liveliness.

To Alan Hardcastle, a dear friend who would have liked to be here for this, yet I rest assured that he understood why I did what I do.

To Roger Needham, who I avoided for too long.

Finally, to Tommy Casey, who never got a chance to finish his.

Ian Hosein, 2003.

Acknowledgements

I owe many people much for their assistance and guidance. I will keep this as brief and professional as possible.

Within the doctoral process, Ian Angell for the incredible support and for choosing me and our conditions; Susan and the Boy Scott for getting me into this mess and for caring throughout; and Edgar Whitley for getting me out of it, and accompanying me along on the exit strategy.

Within the IS Department, Lucas Introna, Shirin Madon and Steve Smithson, Jimmy Tseng, and the administrative staff, who were always on hand for support and friendship. Similarly, within the world of policy, David Banisar, Ian Brown, Alberto Escudero-Pascual, David Sobel (and EPIC generally), Barry Steinhardt, and my colleagues on the FIPR advisory board. Academic reviewers to published work were also very helpful with their suggestions and encouragements.

For financial and administrative support, Roger Needham and Maggie Nicell, Mari Ann Lindqvist, Angela Leeke, Dieter Gollman at Microsoft Research. At IBM Research, Bill McLean and Joe Nemni. The Electronic Privacy Information Center and the Global Internet Liberty Campaign for trips to Washington and Brussels. Oshoma Momoh and Jason Whitehead for the accommodation and entertainment in Seattle and Washington. Department of Information Systems assistance and for letting me attend the Short Course on Regulation; and for general resources. Zero-Knowledge Systems for resources and attendance to G8-related events. Oxford University's Programme in Comparative Media Law and Policy, the Social Science Research Council, and Columbia University for the assistance.

For contact for research purposes, Brian LaMacchia and George Spix, Lyne Simard, Vera Murray, Kevin Lynch, Brian O'Higgins, Lynn McNulty, Israel Ben-Ishai; and all the people involved within John Young's Cryptome, Declan McCullagh's Politech mailing list, Phil Agre's Red Rock Eater list, GILC news, EFF, Crypto.com, FIPR, and yes, even the cypherpunks.

For personal support: Simon Davies and Rick Abbey, J and K King, John Harrison, Stephanie Perrin and the boys, and Onie Hardcastle for the homelife, whose company and consumption made this all possible; and my family. Marco Buttazzoni for the Guinness over the years. And those who made me want to stay, and made staying bearable or at least shared a drink along the way; the Pluvinage clan for the beach; The Brunch Club members who came, left and stayed. The staff at Wright's Bar. Erica W. for the shared misery. Dieter Z. for the shared experience and for convening Barcelona's mad writing session. Melissa, for sharing time and space.

Preface

Portions of this work has appeared in lectures, conference proceedings, book chapters, and journal publications. These are itemised below. I acknowledge my co-authors and the editorial staff and reviewers, while the research and the analysis presented in this dissertation is my own.

Chapter 1 is a result of

- lectures to IS140 on Introduction to Information Systems, IS143 on Introduction to the Information Society, an MSc module on networks, IS489 on Privacy and Data Protection, IS477 on Interorganisational Systems, and a presentation at Outlook for Freedom, a conference for Russian human rights organisations, Moscow, April 2000.

Components of chapter 2 have appeared in

- Hosein Ian (2001) The Collision of Regulatory Convergence and Divergence: Updating policies of surveillance and Information Technology. The Southern African Journal of Information and Communication 2(1), 18-33.
- Hosein Ian, Prodromos Tsiavos, and Edgar Whitley (2003) The Footprint of Regulation, in IS Perspectives and Challenges in the Context of Globalization (Poulymenakou Angeliki et al. eds), Kluwer Press.

Components of chapters 2, 3, and 5 have appeared in

- Hosein Ian, Prodromos Tsiavos and Edgar Whitley (2003) Regulating Architecture and Architectures of Regulation: Contributions from Information Systems, the International Review of Law, Computers & Technology, volume 17, no.1, 85-97.

Components of chapter 3 have appeared in

- Hosein Ian (2002) A Research Note on Capturing Technology: Towards Moments of Interest. In Global and Organizational Discourse about Information Technology (Wynn Eleanor H., Edgar A. Whitley, Michael D. Myers and Janice I. DeGross eds.), 133-154.
- Sørensen Carsten, Edgar A. Whitley, Shirin Madon, Dasha Klyachko, Gus Hosein and Justine Johnstone (2001) Cultivating recalcitrance in information systems research. In Realigning Research and Practice in IS Development: The Social and Organisational Perspective (Russo Nancy, Brian Fitzgerald and Janice I. DeGross eds.), 297-316, Kluwer, Boise, Idaho. (ISBN 0-7923-7420-7)

Components of chapters 3 and 6 have appeared in

- Hosein Ian and Edgar A. Whitley (2002) The regulation of electronic commerce: learning from the UK's RIP Act. Journal of Strategic Information Systems 11(1), 31-58. (ISSN 0963-8687)

- Whitley Edgar A. and Ian Hosein (2001) Doing politics around electronic commerce: Opposing the Regulation of Investigatory Powers Bill. In Realigning Research and Practice in IS Development: The Social and Organisational Perspective (Russo Nancy, Brian Fitzgerald and Janice I. DeGross eds.), 415-438, Kluwer, Boise, Idaho. (ISBN 0-7923-7420-7)

Components of chapter 6 have appeared in

- Hosein Gus (1998) Consultation and Contemplation -- What has Gone Before, a summary of the first UK Cryptography Policy consultation process. In Electronic Privacy Information Center 1998 Sourcebook, Washington D.C.

Components of chapters 7 and 8 have and will appear in

- Escudero-Pascual Alberto and Ian Hosein (200x) The hazards of technology-neutral policy: questioning lawful access to traffic data. Accepted on October 24, 2002 for publication in the Communications of the ACM.
- Hosein Ian (2000) Logical Propositions on Free Expression, Regulation, Technology, and Privacy, Media Asia, Volume 27, Number 2, 2000, pp.68-73, by Asian Media, Information and Communication Centre (AMICS) and the School of Communication Studies, Nanyang Technological University (SCS-NTU).
- Canadian Delegation Discussion Paper for Data Retention Workshop. Tokyo: Group of 8 Conference on High-Tech Crime, 2001, as a contributing author.
- Hosein Ian (200x) International Cooperation in Criminal Matters and Cybercrime, will appear in Governing Global Electronic Networks (Drake William and Ernest Wilson III eds.), MIT Press.
- Government of Canada Ministry of Justice-commissioned comparative study on interception of communications regimes in Australia, Germany, the Netherlands, United Kingdom, and the United States, April 2001, as a contributing author and co-editor.

A note on formatting

I have placed the references for chapters 5 and 6 at the end of each chapter, while the remaining references are in the References section at the end of this dissertation.

Chapter 1: Introduction

> I am not an advocate for frequent change in laws and constitutions, but law and institutions must go hand in hand with the progress of the human mind as that becomes more developed, more enlightened, as new discoveries are made, new truths discovered and manners and opinions change. With change of circumstances, institutions must advance also to keep pace with the times. We might as well require a man to wear still the coat which fitted him when a boy as civilised society to remain ever under the regimen of their barbarous ancestors.
>
> -- Thomas Jefferson, an American Cryptographer and Founding Father

> Serendipity is looking for a needle in a hay stack and finding the farmer's daughter.
>
> -- Professor Roger Needham

Abstract

Cryptography is considered an important technology, a technique essential for securing and generating trust in digital transactions. This chapter introduces cryptography as an artefact, as a technology in some of its mathematical splendour, and as a subject of policy. The chapter also presents the main argument for the dissertation: studying both the technology of cryptography and the policies to shape its development and use is required in order to understand the discourse of cryptography policy.[1]

1.0 Cryptography as a Challenge

In November 1992, enrolled as a first year student at the Faculty of Mathematics at the University of Waterloo, I decided to skip an Algebra lecture. I did not realise at the time that it would be important for me to learn the *Euclidean Algorithm* and the *Chinese Remainder Theorem*. The next lecture, however, I had been looking forward to for the entire term: *Cryptography*. Just as it was when I was young and could never fully understand the pig-Latin that my friends were so accustomed to conversing when parents were in the room (and no, I never had a secret decoder ring), the lecture on Cryptography made little sense to me. It was not due to the cryptic nature of the topic with its algorithms and keys; rather it was my lack of aptitude towards mathematics, and lack of appreciation, at the time, of mathematical theory.

In April 1993, unbeknownst to me, cryptography was invited openly onto a new stage: the open stage of the popular political process. Soon thereafter, it became common to associate cryptography with commerce, markets, criminality and terrorism, other technologies and

infrastructure, and government policies. This was all because the President of the United States announced the U.S. domestic cryptography policy. It was not the last such announcement; and over the years other countries also came forward. In 1996, the United Kingdom government announced its own policy. If only policy was so easy: statements and articulations to direct a path for a technology were not enough.

Cryptography is an art and a science, and requires a level of competency prior to application. Cryptography policy is no different. According to a team of leading private sector and academic cryptographers, cryptography policy is a complex arena, with scientific, technical, political, social, business, and economic dimensions (Abelson and others 1998). I aim to explicate this complex arena (Latour 1991, p.129), which in turn requires an understanding of these technological, political, and economic dimensions and their interplay. This interplay of these dimensions is what I call *policy discourse*: the interaction of actors as they negotiated, deliberated, consulted, objected, questioned, implemented, or ignored proposed policies.

The primary objective of this research is to understand the relationship between technology and society through looking at one of the more contentious technology policy debates of the 1990s. The secondary objective is to devise means through which we may understand regulation, possibly as a socio-technological phenomenon. This research aims to study the discourses surrounding the cryptography policy initiatives in the United States and the United Kingdom. I will argue that we may derive a deeper understanding of policy discourse if we take a socio-technological approach. Such an approach allows for greater detail regarding actors, their interests, and how alliances form and transform.

The goal of my research is to argue that a socio-technological approach enhances our understanding of actors and their interests; of the discourse and its outcomes; and regulatory change. This is not so simple as to consider technology alongside social forces; it is rather a more subtle heuristic involving social and technological actors at a granular level, translating action through various mechanisms, and articulating principles. Such a socio-technological approach will answer the call from Orlikowski and Iacono (2001) for attention to the technological within the social sciences; attend to Stigler's call for research on the process of policy formation rather than only its effects (1983, p.541), while also provide further depth in understanding policy transformation (Hood 1994).

The socio-technological approach to policy and regulation is described in Section I on this dissertation (chapters 1, 2, and 3). The methodology and the two policy discourses are

presented in Section II (chapters 4, 5, and 6). The analysis and implications for other technology-policy discourses is discussed in Section III (chapters 7 and 8).

The present chapter will introduce the challenge of cryptography policy, by discussing its political and technological traits; and in turn the policy strategies that have been pursued, and their relationships with cryptography itself. Section 1.1 will first review cryptography as a socio-historical artefact. Section 1.2 will present cryptography as a science, technique, and technology; while §1.3 will present some of the policy views regarding cryptography. These strands will converge at §1.4 where I will present a typology of policy strategies that will be used to classify the policies discussed later in this dissertation.

1.1 Cryptography as Artefact

The history of cryptography is as rich and interesting as the stories of society itself. In the seminal study on the history of cryptography, David Kahn's *The Codebreakers* (Kahn 1996) notes,

> It must be that as soon as a culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously -- as its parents, language and writing, probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write. (p. 84)

Kahn finds that one of the earliest known occurrences of the use of cryptography was in 1900 BC, when an Egyptian scribe used non-standard hieroglyphs in an inscription. As well, he found multiple motivations for the use of cryptography beyond political secrecy,

> The Yezidis, an obscure sect of about 25,000 people in northern Iraq, use a cryptic script in their holy books because they fear persecution by their Moslem neighbours. Tibetans use a kind of cipher call 'rin-spuns' for official correspondence (...). The Nsibidi secret society of Nigeria keeps its pictographic script from Europeans as much as possible because it is used chiefly to express love. (p. 85)

Cryptography was often used to protect state communications; the most common example was its use by the Roman Empire.

> In this renowned application, Caesar would communicate with his centurions using the Roman alphabet, but would *shift* each letter he intended in his *plaintext* by three letters, thus producing *ciphertext*. Therefore, Caesar's alphabet started with the letter D, rather than A, and so on for the rest of the alphabet. (Kahn 1996, p.84)

The model described from Caesar's time is very traditional: the plaintext that is *encrypted* into ciphertext, using a relatively small key (three, the size of the letter shift).

The Catholic Church during the 16th century pioneered the use of ciphers to protect diplomatic correspondence. By the 18th century, European governments routinely read diplomatic mail by *breaking* the algorithms of other nations (NYT Staff 1998).

The majority of the developments outlined in Kahn's book and other works on the history of cryptography, however, are civilian developments (Ellison 1996).

> It was the amateurs of cryptology who created the species. The professionals, who almost certainly surpassed them in cryptanalytic expertise, concentrated on down-to-earth problems of the systems that were then in use but are now outdated. The amateurs, unfettered to those realities, soared into the empyrean of theory. (Kahn 1996, p. 125-126)

Non-governmental applications include the Kama Sutra of Vatsyana, that lists cryptography as the 44th and 45th of 64 arts men and women should know and practice. Interestingly, perhaps the earliest use of regulation and restriction arises from this very same situation: "Man should study the Kama Sutra and the arts and sciences subordinate thereto (…). Even young maids should study this Kama Sutra, along with its arts and sciences before marriage and after it they should continue to do so with the consent of their husbands." (from Ellison 1996)

In 1930s America, Mafia bootleggers used cryptography to communicate details of shipments of alcohol. "Some of these (ciphers) are of a complexity never even attempted by any government for its most secret communications," wrote Mrs. Elizebeth Smith Friedman, a leading government cryptanalyst at the time (from (Kahn 1996, p. 804)). In 1917 Gilbert Vernam at AT&T developed the Vernam cipher, using a key that is completely random and never repeats -- a *one-time-pad*. This is a provably secure cipher, i.e. unconditionally secure (Stinson 1995, p.51). Designed as a machine, it was offered to the U.S. Government for use in World War I but was rejected and put on the commercial market in 1920 (Kahn 1996, p.401), but failed because of efficiency factors (Kahn 1996,p. 402; Stinson 1995, p.51).

In 1840 Edgar Allan Poe wrote *A Few Words on Secret Writing*, a non-fiction work that included the statement, "It may be roundly asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve" (from NYT Staff 1998). During the World Wars, the governmental use of cryptography was most noteworthy. Kahn begins his book, describing the U.S. government efforts to *break* Japanese Naval communications codes.

More widely known are the efforts of mathematicians, academics, and even chess players at Bletchley Park in Coventry, England, gathered by Winston Churchill with the mission of intercepting and understanding German communications. The Germans *encrypted* their communications using a rotor-based machine, *Enigma*. Breaking the code was an invaluable source of intelligence for the Allies.

After the war, cryptography policy began, albeit quietly. President Truman placed cryptography on the U.S. Munitions List, restricting its export. In 1952 Truman secretly signed the directive that created the formal agency of the U.S. Government that was responsible for continuing the mission of intercepting communications and decrypting foreign communications, the National Security Agency (NSA). Today this secretive agency has one of the largest governments budgets, in the order of $3.6 billion.[2]

The post-war period included the increased use of computing by an increased amount of sectors of society and the growth of digital communications networks. This in turn gave rise to new conditions for cryptography, and new potential applications. Algorithms grew more complex, keys grew larger, and were sometimes separated.

There are two periods of modern cryptography history: before 1976 and after (Dunn 1997). In 1976, Whitfield Diffie and Martin Hellman, and Ralph Merkle independently, developed publicly the notion of *public key cryptography*. In this decade, cryptography changed radically. In order to appreciate fully not only this change, but also how it affected the actors and interests within the arena of cryptography policy, a review of cryptography as a technique is required.

1.2 Cryptography as Technology and Technique

Cryptography is the mathematical art and science of securing data for viewing only by its intended audience. Modern cryptography depends on the existence of difficult mathematical problems (RSA Laboratories 1998) to create and break *cryptosystems*.

Stinson (1995) defines a *cryptosystem* formally as:

> .. a five-tuple (P, C, K, E, D) where the following conditions are satisfied:
>
> 1. P is a finite set of possible plaintexts
> 2. C is a finite set of possible ciphertexts
> 3. K, the keyspace, is a finite set of possible keys
> 4. For each k in K, there is an encryption rule e_k in E and a corresponding decryption rule d_k in D. Each e_k [that maps P to C] and d_k [that maps C to P] are functions such that $d_k(e_k(x))=x$ for every plaintext x in P.

This is a general definition, while below I will present two specific definitions: one where k for encryption is the same as decryption; and another where each operation uses different keys.

1.2.1 Symmetrical Cryptography

Cryptography is accordingly a tool for information security. Information security principles include *confidentiality*, *integrity*, and *authentication*.[3] Cryptography affords confidentiality to plaintext by transforming it into ciphertext. Integrity of the message, i.e. assuredness that the message has not been altered, can be derived from the decryption process: if the message decrypted properly (without errors), then it can be assumed that the message was not changed since being encrypted. Finally, authentication is provided through key distribution. That is, the recipient has a good idea of the authority of the sender of an encrypted message, because if the message decrypts successfully, the recipient can assume that it was encrypted using the same key used for decryption. If the recipient assumes that the only person with such a key would be the person that he expected to receive the message from, then he can be sure that it was indeed she who sent it. These principles hinge on the trustworthiness of the algorithm and appropriate key distribution and management procedures.

In this process, the keys and the algorithms are the essential information; even more valuable than the message content. That is, if the message is recovered, then the confidentiality of a single message is lost; if the algorithm is flawed or key is divulged, all messages, past and future are compromised.

Keys, in their modern usage, tend to be a very large number, ranging in size from 2^{40}, to 2^{56}, 2^{64}, 2^{80}, to 2^{128} and even 2^{256}.[4] Another notation for these key-lengths is to refer to keys in the order of 2^x as being x-bit keys (e.g. keys of the order of 2^{256} are 256-bit keys). A method of attacking this cryptosystem would be to use *brute force*: if the key exists within the *keyspace* (Stinson's 'K') of 1 to 2^{40}, then an attacker can use a computer (or many) and try every number in the keyspace and see which one provides understandable plaintext.

An alternative attack on a cryptosystem would be to find a flaw in the algorithm. In accordance with Kerchkoffs' principle, the effectiveness of the cryptosystem must not rely on the secrecy of the algorithm (Kerckhoffs 1883). Accordingly, most modern algorithms are published openly to the community of cryptographers, in the hope that they will be reviewed and flaws identified, intentional *back doors* removed, and other such weaknesses in the algorithm highlighted. Trust in an algorithm is generated through this openness. In the open community of competing interests, where companies vie for adoption of their own

algorithm as a standard, academics and practitioners endeavour for credibility by finding flaws, governments concerned with national and domestic security create their own solutions; the presumption of open review is that stronger algorithms will emerge.

1.2.2 Asymmetric Cryptography

In the late 1970s, Diffie and Hellman (1976), and Merkle (1978)[5] independently found solutions to problems that plagued symmetric cryptosystems: how do you communicate securely with multiple untrusted people? and how do you secure a message over an insecure medium? (Levy 2001) If the medium is insecure, sharing keys will be a hazardous exercise. The more recipients that exist within a network of communicators, the more keys that are required, and managing these secret keys becomes burdensome.

Using an elegant mathematical problem of computing the logarithms of large numbers, Diffie and Hellman created the *Diffie-Hellman Key Exchange* algorithm. Here, two people, Alice and Bob[6], are able to create a symmetric key over an insecure network so that even if someone was passively intercepting their initiating conversations in the process of creating a shared key, the secrecy of their communication will not be compromised.

> Alice selects a random number **a**, and Bob selects a random number **b**.
> Both users agree upon a non-secret number pair **x** and **n**.
> Alice raises **x** to the power of **a**, *modulo* **n**, thus $\mathbf{x^a}$ *modulo* **n** and sends the result to Bob.
> Bob raises **x** to the power of **b**, *modulo* **n**, thus $\mathbf{x^b}$ *modulo* **n** and sends the result to Alice.
> Alice now has **a** and $\mathbf{x^b}$ and computes **(***modulo* **n)** $\mathbf{x^{ab}} = (\mathbf{x^b})^{\mathbf{a}}$.
> Bob now has **b** and $\mathbf{x^a}$ and computes **(***modulo* **n)** $\mathbf{x^{ab}} = (\mathbf{x^a})^{\mathbf{b}}$.

Both users are in possession of the same value $\mathbf{x^{ab}}$, but an eavesdropper can only capture the values $\mathbf{x^a}$ and $\mathbf{x^b}$. With a sufficiently large modulus it is computationally infeasible for the eavesdropper, Eve, to compute the common key without knowledge of **a** or **b**. This value of $\mathbf{x^{ab}}$ can be used within a symmetric algorithm as the key for encryption and decryption purposes. Diffie and Hellman also suggested the notion of *keypairs*, claiming that if there were two keys then it would be possible to create the digital equivalent of signatures.

Two years later, Rivest, Shamir and Adleman (1978) created a public-key cryptosystem, *RSA*. *RSA* relies on the difficulty of factoring large integers (Stinson 1995, p.119).

Select two large (e.g. over 100 digit), unequal prime numbers, **p**, and **q**.
Compute **n** = **pq**.
Compute **f(n)** = **(p-1)(q-1)**.
Randomly select an integer **d** that is larger than **p** and **q**, and less than **n-1**, and ensure that **d** and **f(n)** have no common factors.
Compute **e** = $\mathbf{d}^{-1}$ *modulo* **f(n)**
Publish the encryption key **e and n**, while strictly maintaining the secrecy of the decryption key **d**, and the numbers **p**, **q**, which are used in the computation of **d** and **e**.

To Encrypt:
C = $\mathbf{M}^{\mathbf{e}}$ *modulo* **n**
Where **M** is the message coded into numbers, **C** is ciphertext.

To Decrypt:
M = $\mathbf{C}^{\mathbf{d}}$ *modulo* **n**

Their contribution was a successful algorithm allowing for two keys: an encryption key (**e**, **n**) and a decryption key (**d**). The public encryption key (*public key* or *encryption key*) can be published widely without any concern about its security, while the private encryption key (*private key*, *decryption key*, or *secret key*) can remain solely in the possession of the recipient. The mathematical relationship between the keys is such that if a message is encrypted with one key, only the other can decrypt it.

If Alice wished to communicate securely with Bob over an insecure medium, Bob would first generate a public and private encryption keypair. Bob would then send the public key over the insecure medium to Alice (or the key could be published in a database, or *keyserver* where Alice could retrieve this key) who would then use it to encrypt the message. The moment the message is encrypted, Alice can no longer decrypt the message; the only person who could feasibly decrypt the message is the owner of the private key, presumably Bob.

RSA relies on the challenge of factoring large integers. Thus, the resulting keys for *RSA* are usually longer than 512-bits, and tend to be 768, 1024, or 2048-bits in length. Other schemes exist based upon other mathematical problems, requiring different key-lengths. For example, *Rabin*'s security is derived from the difficulty of finding square roots *modulo* a composite integer (Schneier 1996, p.475). Another example is *Elliptical Curve Cryptography*, which allows for keys in the order of 128-bits.

Meanwhile, *ElGamal* is similar to *Diffie-Hellman Key Exchange* in that it relies on the difficulty of calculating discrete logarithms (Stinson 1995, p.115).

Choose prime **p**, and two random integers, **g**, and **x** such that they are less than **p**.

Calculate $\mathbf{y} = \mathbf{g}^{\mathbf{x}} \textit{modulo } \mathbf{p}$
The public key is (**y**, **g**, **p**). The private key is **x**.

ElGamal allows for an additional capability: digital signatures (Stinson 1995, p.205). What is interesting about some implementations of *ElGamal* and its keys is that there is the possibility of another key, that is the *private signature key*, which unlike in *RSA* implementations, this private signature key is *similar* to the private encryption key, but it is restricted to acts of *signing*. This will be discussed in greater detail in chapter 5, with an outline of the development of the Digital Signature Standard.

1.2.3 Some Implications of Public Key Cryptography

The most notable contribution of public-key cryptography is the notion of the digital signature, and associated services of certification.

Digital Signatures I

The mathematical relationship between the public and private keys is symmetric. If Bob was to *encrypt* a message using *his private key*, then **anyone** who had Bob's public key could decrypt it, including Alice, the intended recipient, Eve the eavesdropper, and Mallory, the malicious actor. In this case, however, Bob is not necessarily concerned with confidentiality, but rather cares only about authentication.

Consider the distribution of the keys: while everyone in the world can have a copy of Bob's public key, Bob is, under ideal information security circumstances, the only person with possession of his own private key (Abelson and others 1998). If the recipient of Bob's encrypted message can decrypt the message using Bob's public key, then she can safely assume that because of the mathematical relationship between the two keys in the keypair, the person who encrypted the message held the private key. Presuming that Bob is the only person in possession of this private key, then Alice can assume with some level of certainty that Bob created the message. This is *authentication*, where information regarding the origin of a message can be inferred.[7]

This process of encrypting data with a private key is often called the *digital signature*. When Bob encrypts his message using his private key, he is digitally *signing* the message, saying essentially: *"The owner of the private key that signed this message certifies that this message was created by the owner of the private key."*

Certification

Alice can not always be certain that Bob is in fact the owner of the private key. Consider the case of Mallory, the malicious intruder in their conversation.

What if Bob sends his public key to Alice, but the communication stream is intercepted by Mallory? Mallory can then create her own keypair, and send a copy of her public key to Alice as though it was Bob's; without Alice knowing any better. After all, a key is merely a large number. When Bob sends a signed message to Alice, Mallory can intercept the message, remove the signature, alter the message, then *sign the message with her own private key* and send the message onward to Alice. Alice receives the message, and verifies the signature with the public key she thinks comes from Bob (which in fact came from Mallory). Alice is led to believe that Bob had signed the message.

The same applies to public key cryptography for confidentiality purposes. That is, Alice can retrieve Bob's public key from a server, when it is in fact Mallory's key that Mallory slipped into the key server without Bob's knowledge. Any subsequent message that Alice encrypts to Bob is in fact being encrypted to Mallory, who then intercepts, decrypts, reads, possibly alters and may send on to Bob without either Alice or Bob being any the wiser.

There are various solutions to this problem, the leading scheme being *certification*. A certificate consists of a public key, and personal and technical information regarding this public key and its owner. That is, Bob's certificate could consist of his public key, information about the public key (e.g. its size, date created), and his personal information, (e.g. email address and home address).

To ensure that the information on the certificate is accurate and not fraudulent, some have suggested the creation of a public key infrastructure (PKI). Each certificate is digitally signed by a Certification Authority (CA), a third party who is responsible for verifying that Bob's details are true: that Bob is in fact Bob, and that Bob's key is in fact Bob's. If the CA agrees with these details about Bob, then the CA signs Bob's certificate with its own private signature key, thus certifying Bob's public key. The CA's signature can be verified with its public key, which may also be a certificate, signed perhaps by a Regulatory CA, and so on *ad infinitum*. This structure and scheme is consistent with the X.509 standard of certificates, a commonly implemented standard.

Constraints on Public Key Schemes

The above outline of the public-key schemes for encryption, decryption, digital signatures, and certification is lacking in some precision. *Encryption*, *Decryption*, *Signing*, and *Verifying*

using *RSA* and *ElGamal* cryptosystems are very demanding processes, compared to symmetric algorithms at least. When implemented in hardware, *RSA* is about 1000 times slower than *DES*, a common symmetric cryptosystem; while in software, *RSA* is about 100 times slower than *DES* (Schneier 1996, p. 469). *ElGamal* is also remarkably slower than *RSA* (Schneier 1996, p. 479). Generally, symmetric cryptography is used when a large amount of data needs to be encrypted; asymmetric cryptography is used for shorter messages.

Hybrid Cryptography

Due to the resources constraints of public key cryptosystems, a hybrid scheme is commonly used. In most practical implementations, public-key cryptography is used to secure and distribute an ephemeral random *session key*.

These session keys are generated and then used with symmetric algorithms to secure message traffic (Schneier 1996, p. 33). That is, Alice generates a random session key, and encrypt the message with that session key and a symmetric algorithm. She then encrypts the session key using an asymmetric algorithm and Bob's public key, and appends it to the message. Bob decrypts the session key with his private key and asymmetric algorithm, and then decrypts the message with the session key and the symmetric algorithm.

Digital Signatures II

The process of a digital signature is also different due to resource constraints. If Bob wanted to sign a message to Alice, Bob would generate a *hash* of that message. A *hash* is a *one-way* mathematical function. That is, it takes the message, and transforms it into a relatively unique value, though this value can not be reversed back to the original message. As commonly implemented, the likelihood of two messages having the same hashed value is only one in 2^{160} (Schneier 1996, p. 37). If the message is changed even slightly in transit, the hash of the transmitted message would be noticeably different from the original hash.

Upon generating the hash of the message, or the *message digest*, Bob signs it with his private key, and appends the signed message digest to the original plaintext message. Bob will then send the message and the signed message digest to Alice.

Upon receiving the message, Alice would perform a hash on the message plaintext, also generating a message digest. She would then decrypt, and verify the signature of the message digest that Bob generated. If the value of the hash that Alice performed is equal to the value of the message digest that Alice decrypted from Bob's message, then the signature is verified: integrity and authentication are assured.

A final point to draw is that within *RSA* the private key is used to create signatures. That is, the *private encryption key* is the same as the *private signature key*, with the same functionality. This is not always the case, however. *ElGamal* has a signature key that can only be used to generate signatures, not for decryption; the U.S. federal standard, the *Digital Signature Scheme*, is structured similarly. This was a source of techno-political controversy; the reasoning behind the key separation will be raised in chapter 5, while some implications for cryptography policy will be discussed in chapter 6.

1.2.4 Algorithms and Implementations

Effective cryptography is not as simple as ensuring effective algorithms. Implementing cryptography into hardware, software, modules, and programmes is a challenge. Even if programmers are granted access to all the cryptography-enabling programming libraries available, and the algorithms are reviewed openly and accepted by the community, security is still not assured.

Implementing cryptography is very complex. This includes assuring sufficient randomness in pseudo-random number generators for key-generation, as was discovered faulty in Netscape's Secure Sockets Layer (Goldberg and Wagner 1996); highlighting enforced weaknesses in the keys, as discovered in the GSM phones where the key size, although 64-bit, included a large set of zeros (Briceno 1999); avoiding faulty design of key protection, as Anderson (1993) notes regarding Automated Teller Machine cards and passcodes; defending against statistical analysis, as with 802.11 standard for wireless communications (Borisov, Goldberg, and Wagner 2001); to name a few conditions.

As a result, within the epistemic community (Haas 1992, see chapter 2) of cryptography and security experts, trust in applications is developed over time, and often-times through openness similar to the treatment of the algorithms (Levy 2001; Schneier 1996). In chapter 5, a selection of implementations will be reviewed. Although these implementations often include traditional *trusted* algorithms, the details of the implementation are interesting, particularly due to the political environment of their development. Therefore, I will not treat cryptography as a *black box*. Understanding the politics of cryptography requires opening that black box; as will be argued in chapter 3.

1.3 Cryptography as Policy

The history, structure, and application of cryptography is connected with the policies surrounding its development, implementation, and use. Throughout the 1990s, starting with concern for the National Information Infrastructure, the Global Information Infrastructure,

then electronic commerce and the dot-com boom, cryptography was considered to be a key component for security and trust.

There was a felt need, by governments mostly, to establish policies. These policies often gave rise to debates, sometimes heated. According to a seminal National Research Council report on cryptography policy,

> The debate over cryptography policy has been hampered by an incomplete analysis and discussion of various policy options -- both proponents of current policy and of alternative policies are forced into debating positions in which it is difficult or impossible to acknowledge that a competing view might have some merit. (NRC 1996, p. ix)

The now defunct U.S. Congress Office of Technology Assessment (OTA) introduced the issue likewise:

> Policy discourse over cryptography used to be as arcane as the technology itself. Most people didn't regard government decisions about cryptography as directly affecting their lives. However, as the communications technologies used in daily life have changed, concern over the implications of privacy and security policies dominated by national security objectives has grown dramatically, particularly in business and academic communities that produce or use information safeguards, but among the general public as well. (OTA 1994, p.9)

Rarely does technology policy prompt this level of controversy. Even in the first public announcement of the Clinton Administration's first cryptography policy initiative, the actors and their conflicting interests were identified.

> For too long, there has been little or no dialogue between our private sector and the law enforcement community to resolve the tension between economic vitality and the real challenges of protecting Americans. Rather than use technology to accommodate the sometimes competing interests of economic growth, privacy and law enforcement, previous policies have pitted government against industry and the rights of privacy against law enforcement. (The White House 1993)

Cryptography policy in the April 1993 announcement discussed the use of cryptography for communications over telecommunications infrastructure, the concerns of law enforcement, of individuals, of industry, and ultimately, the notion of regulation, keys, and *key escrow*.

From this announcement, a crisis followed. According to the editor of the NRC report,

> I believe that the crisis is a policy crisis, rather than a technology crisis, an industry crisis, a law enforcement crisis, or an intelligence-gathering crisis. (NRC 1996, p.xv)

The NRC report listed the multiple and varied interests as including personal liberties and constitutional rights, the maintenance of public order and national security, technology development, and economic competitiveness and free markets.

> At a minimum, policy makers (and their critics) must understand how these interests interrelate, although they may decide that one particularly policy configuration better serves the overall national interest than does another. (NRC 1996, p. viii-ix)

Similarly in the United Kingdom, a wide ranging set of actors arose and interests emerged in the discourse surrounding the policies announced from 1996, to the passing of the Regulation of Investigatory Powers Act in 2000.

The empirical data section of this dissertation will present the proposed policies and regulatory regimes, the actors, their articulated interests, and some of their actions. Cryptography policy was indeed a policy crisis, an attempt to regulate the development or use of a technology that faced serious opposition. To appreciate fully the challenges in cryptography policy, however, a socio-technological approach is required. That is, to understand the types of strategies and policies used, their implications for technological design and social use, some understanding of keys, processes, algorithms, key lengths, etc., is required.

1.4 Does Politics have Technology?

One challenge for the regulatory policies is to enable cryptography to proliferate without causing harm to law enforcement and national security interests. The same confidentiality that cryptography offered to governments is now being developed and used by individuals; equivalent levels of protection only afforded to governments are now deemed necessary for electronic commerce (e-commerce), the protection of human rights, among many other applications. The policy crisis necessarily involved social actors, but it also involved a technology, and a shifting technological environment, that in turn affected the actors and their interests.

In 1993, the concept of Internet communications was valued only by a relatively small group of users, e-commerce was barely considered, and cryptography was an esoteric issue. By the time the United Kingdom released its policy statement in 1996, e-commerce was a key component of election platforms, and millions of users of cryptography were on-line. At the time of the submission of this dissertation, every operating system and most Internet-client applications are crypto-enabled.

The environment has changed significantly since 1993 with the growth of the Internet and global communications; much as the environment changed since 1976 in heavily regulated telecommunications networks; or as the environment changed since 1900 BC with atypical Egyptian hieroglyphs. What remains is a perceived need for secure communications and transactions, and this affects actors and their interests in a variety of ways. How the regulatory frameworks designed for one environment change as the environment changes is worthy of study.

A number of countries with varying legal, political, economic, and technological environments over the years have tried to regulate cryptography. In its international review, the Electronic Privacy Information Center (EPIC) noted a number of controls.

- ? controls maintained by the governments on the domestic use of cryptography in their countries
- ? controls maintained by the governments on the importation to their countries of applications and equipment that allow use cryptography
- ? controls maintained by the governments on the export of applications and equipment that use cryptography (Electronic Privacy Information Center 1999, p5)

While this typology of controls is useful, I offer an alternative conceptualisation. The EPIC typology is useful to identify political strategies, but does not sufficiently identify the technological nature of these regulations. Rather, I offer the following typology of policy strategies in order to present the regimes as both a social and technological phenomena.

Type 0
Restricting the development, implementation, and use of cryptography.
Type I
Policies affecting the development, implementation and use of algorithms
Type II
Policies of allowing for lawful access to keys
Type III
Policies maintaining capacities to brute-force keys

Table 1.1 Cryptography Policy Typology

Each strategy used by governments involved technological and social actors. Each strategy gave rise to technological and social reactions, and affected the technological and social actors differently. For example, France until 1999 had a ban on cryptographic implementations using keysizes larger than 40-bit; the choice of 40-bit keys was intentional, and affected the regulatory environment in a number of ways. Each of the regulatory strategies pursued by the United States and the United Kingdom are of one or more of these types; as will be summarised in chapter 7.

As the regulations were socio-technological in nature, this dissertation will study the discourses surrounding the regulations in a socio-technological manner. Through looking at how cryptography policies were introduced, discussed, and embedded into technology and circumvented using technology, objected to, and ignored, I will monitor the regulatory shifts and transformations within each discourse. Understanding the role of the technological actor alongside the traditional social actors will contribute to our understanding of regulatory change.

In chapter 2, I review the regulation literature, focussing particularly on the existing ability of the diverse theories on regulatory regimes to accommodate policy shifts, reversals, and technological change. I contend that the literature may benefit from a more socio-technological approach to understanding regulatory regimes and policy environments.

To understand the relationships between technology and society, in chapter 3 I review the society and technology literature. Viewing each discourse as a socio-technological phenomenon is non-trivial from a theoretical perspective, as it entails treating technology as an actor along-side the traditional social actors that we commonly consider. I develop a frame of capture, *moments of interest* within a discourse where social and technological actors take form and *translations* occur, that I will use to decide upon socio-technological data.

Cryptography policies were heavily debated political discourses. In chapter 4 I present the methodology used to gain access to the discourses and to collect data. This interpretive research was a combination of a number of methodologies and methods in order to gain access while also ensuring a fair representation of the various actors and their interests.

The policy discourse in the United States is presented in chapter 5, focussing primarily on the period from 1993-2000. The chapter shows the variety of policy strategies used by the Clinton Administration, the shift in instruments and regulators, the shift in focus from mandated technology to development-guidelines. I also present a number of technologies that were introduced to the discourse, and open their black boxes to see what they represent, the politics inside, and the arising challenges.

The United Kingdom domestic policy discourse is studied in chapter 6, focussing on the 1996-2000 period. This discourse saw a change of government, a change of regulator, and a complete shift in the object of regulation, as the environment also shifted. Although the technology was not regulated overtly, there were technological implications to the policy recommendations.

The analysis chapter, chapter 7, compares and contrasts each discourse, using a framework of analysis from the literature on regulation, noting the regulatory mechanisms used, the actors present, and their articulated principles. The chapter highlights the emergent actors in each discourse and the subsequent shift in policies, and the detailed socio-technological nature of the policies and their implications. It outlines the attempts at translation by various actors, how some were more successful than others, and accounts for these changes using regulation theory while incorporating the technological actor.

The implications of this research are discussed in chapter 8. The socio-technological research approach is presented as a contribution to Information Systems research. The additional understanding that a socio-technological approach offers to the study of regulation is also discussed in further detail, as other examples of technology policy discourses are considered.

1.5 Cryptography as a Technology and an Actor

In a Secret and blacked-out report from the U.S. National Security Agency that developed the policy threat model, i.e. the potential opposition to proposed policies, the NSA included the following,

- Rights to privacy supersede law enforcement needs. Law enforcement needs outweigh rights to privacy.
- Any government solution which involves the NSA would be suspect.
- If Government wants to decrypt, they should pay to keep up with technology.
- Voluntary co-operation vs. legislation.
- Government ability to decrypt will make US products non-competitive in the world market (and vice versa).
- Government action would displace RSA/DES.
- Mandating a solution restricts future improvements or changes to cryptographic products.
- Government solution will hold back/restrict technology.

(NSA Undated)

In retrospect, the NSA's predictions were relatively accurate, not just for the early policies in the U.S., but also the later policies and even the discourse in the United Kingdom. This dissertation's challenge is to capture and explain two policy discourses that include these articulations, and the actors surrounding each.

Throughout this chapter, I attempted to present the landscape for cryptography, as an issue of contention, as a technology, and as a policy. I also introduced some of the strains in the interests. The industry interests in e-commerce, governments' interests in law enforcement and national security, civil society's interests in privacy and human rights all appear to be on

a clear collision course. A deeper investigation of these interests, alongside the notion of a technological actor, however, will show that these elaborations are simplistic, and that even the interests are quite complex. It is my hope that viewing cryptography and other technologies as actors that must be investigated in detail alongside other actors, will permit deeper understanding regarding the nature of technology policy discourse.

Endnotes

1. This chapter is dedicated to my algebra professors.
2. This amount is derived and estimated by the Federation of American Scientists for 1998. FAS argues it is within a 5% margin of error. See http://www.fas.org/irp/agency/budget1.htm for more information.
3. A common listing of the C-I-A principles tends to include Availability, rather than Authentication; authentication is often included as a fourth.
4. Key sizes represented in bits refer to binary digits, where a 512-bit key is equivalent to a key that is in the range of 2^{512}. For reference, 2^{56}=72,057,594,037,936, while 2^{57} is twice that amount.
5. Although both contributions were written in 1976, Schneier (1996) states that "due to a glacial publishing", Merkle's work was not published until 1978.
6. Alice and Bob are common elaborations of A and B, used in the cryptography world as two sources and destinations of information. Eve, or 'E' tends to refer to a passive listener, and Mallory, or 'M' refers to a malicious active interceptor.
7. Definitions of authentication may vary.

Chapter 2: Technology Policy and Regulation

We felt that (installing seat belts) was an unnecessary imposition and unnecessary cost...because the belt would do the customer no good unless used.

-- Paul Ackerman in 1959, then-vice-president of Chrysler

Many of the temporary standards are unreasonable, arbitrary, and technically unfeasible...If we can't meet them when they are published we'll have to close down.

-- Henry Ford II in 1966 on federal safety requirements for laminated windshields, collapsible steering assemblies, enhanced door locks, and lap and shoulder safety belts.

But the shoulder harnesses, the headrests are complete wastes of money ... and you can see that safety has really killed all of our business. We are in a downhill slide, the likes of which we have never seen in our business. And the Japs are in the wings ready to eat us up alive.

-- Lee Iacocca in 1971, then-president of the Ford Motor Company, in a (taped) conversation with President Nixon.

Abstract

Understanding cryptography policy requires an understanding of the literature on technology policy. While the technology and economic policy literature argues that we must look specifically at the technology in order to understand the policies, this literature assumes that government has benign interests. The literature on regulation sees regulation as a political act, involving actors and interests; however technology is often in the background of analysis. I present the case for bringing technology forward, so long as it is studied in the context of the policy *discourse*. This will lead to chapter 3 where I present the tools to capture socio-technological discourse.

2.0 Introduction

The first chapter of this dissertation presented a typology of cryptography policy that highlights the socio-technological nature of the regulatory regimes.

Type 0
Restricting the development, implementation, and use of cryptography.
Type I
Policies affecting the development, implementation and use of algorithms
Type II
Policies of allowing for lawful access to keys
Type III
Policies maintaining capacities to brute-force keys

Table 2.1 Cryptography Policy Types. See chapter 1

Types I to III are identified by looking at the process through which cryptography functions. That is, the *trustworthiness* of the processes of encryption, decryption, and signature verification can be relayed by the algorithm used, whether it has any faults, intentional or unintentional.

This trustworthiness is often established through open review of the algorithm, which is an interpretation of Kerckhoffs' principle that security should not rely on the algorithm's secrecy (Kerckhoffs 1883; Schneier 2002). Any limits to this review, or shaping of the process is a Type I policy. Similarly, a policy that mandates a specific form of implementation is also of Type I.

If we treat the algorithm as a black box, then access to plaintext can be achieved via the keys. So Type II policies try to establish procedures for lawful access to these keys, achieved through legal and technological means.

Type III policies aim to ensure that these keys are *weak*. Such a policy usually dictates that keys are kept sufficiently short in length ensuring a limited number of keys are available (i.e. a small keyspace). Fewer keys means that the computational burden of brute-forcing is minimised.

Finally there is an alternative policy of Type 0 that bans cryptography outright. Although implemented in some countries, Type 0 policies were not formally proposed in either country in this study.

Each of these policy types indicates an interplay between technological and social controls. A Type I policy affects both the conduct of the cryptographers, but also how the cryptography may be implemented. Similarly, a Type III policy affects the actions of companies developing software, but also affects the constitution of code developed. An understanding of technology policy and regulation is required to make sense of how such policies are formed and implemented, how they are transformed within discourse, and ultimately succeed or fail.

This chapter will review the literature in order to generate an analytical foundation for understanding cryptography policy. The technology and economics literature is reviewed in §2.1. The more politically astute literature on regulation is reviewed in §2.2. A deeper appreciation of technology within regulation is argued for in §2.3. Technological change and regulatory change are investigated in §2.4, leading to discussion in §2.5 of the need to capture socio-technological discourse to appreciate fully explanations of regulatory change.

2.1 On Technology and Economic Action

The literature on economics and technology begins by 'opening the black box' of technology (Rosenberg 1982, pvii). Once opened, markets, policies, and institutions emerge. This body of literature studies the interaction between institutions that govern innovative activities and market-based patterns of change (Dosi and Orsenigo 1988, p.21). The work focuses on diffusion and use of technology and how a technology becomes embedded in infrastructure (Arthur 1988, p.591); and less so on the policy process itself.

Technology may embed itself within a market; but this does not mean that stasis is inevitable. Rosenberg (1982, p.106) acknowledges that technology, as argued by Schumpeter, disrupts and structures markets. Much of Rosenberg's focus resides, however, on how policies structure innovation within the market; such as how government policies in the aircraft industry affected demand, research and development, and market structure (p.163). Rosenberg and Mowery's research shows that government is powerful at choosing winners and losers and creating incentives for development and innovation (Rosenberg 1982, chapter 8). Rosenberg and Mowery view this generally as an acceptable development, since government would possess a great amount of information regarding the technologies and the appropriate market structure.

This information does not give the government full agency in influencing technology diffusion. Arthur (1988) notes that an authority with full information can tilt the market within narrow windows of opportunity to create change where it may not have otherwise arisen. This is admittedly merely theoretical: Arthur notes that full information is unlikely, as is knowing the 'best' technology ahead of time (1988, p.602).

Granting government the power to set policies to choose winners and losers in the marketplace is regarded generally as a positive development within this literature. Rosenberg and Mowery argue that the classical theories that view innovation decided by market forces are unsupported by evidence (Rosenberg 1982, p.194). Rather, they argue that not only do governments have a large role to play in fostering innovation, but governments and policies may be necessary to innovation (1982, p.236). They take a benign view of the interests of the policy makers towards the technology, as they assume that innovation is being promoted.

The literature also assumes that diffusion is the aim of government policy (Rosenberg 1982, p.19). Dosi argues that technology is developed within a techno-economic paradigm,

defined contextually as "the needs that are meant to be fulfilled, the scientific principles utilised for the task, the material technology to be used". That is,

> A technological paradigm can be defined as a 'pattern' for solution of selected techno-economic problems based on highly selected principles derived from the natural sciences. (Dosi 1988, p.224)

Technologies are considered to be 'notional possibilities' within paradigms (van den Belt and Rip 1987, p.138-139). However, this paradigmatic approach does not include consideration for the politics of these patterns: the politics involved in the selection process and the technologies that are eventually developed. While the literature notes that the market is not the over-riding concern, and that government can stimulate relationships in the user-producer field (Lundvall 1988, p.358), they tend to ignore the interests of government. In particular, governments may be interested in *preventing* technology diffusion.

On occasion the literature notes some interesting selections of technologies based on policy. In discussing the case of nuclear power in the United States, Cowan (1990) documents how government's interests are very powerful in deciding winners and losers and shows how the 'best' technology may not win, presenting the case of nuclear reactors. The 'winning' technology was chosen based on the interests of the Department of Defense. Even in deciding which was the *weaker* technology, between the technology promoted by the U.S. and Canada, choosing the metrics for making the decision was also a political process. The U.S. eventually started exporting the technology to developing countries, in spite of export controls, because of fears of the Soviets selling their technology instead.

While the parallel to cryptography policy is striking ('winning' technology chosen by governments, possibly 'inferior' to technology that is available in foreign markets, and export controls being modified to meet state interests rather than market ideals) some significant differences remain. First, governments generally wished to *inhibit* diffusion of cryptography, particularly with Type 0 and Type I policies. Second, while the choice of U.S. nuclear technology was chosen more due to trajectory (the 'winner' was the technology first used by the U.S. Navy (Arthur 1988, p.595)) the eventual Type I, II and III policies led to choices based on governmental self-interest in maintaining law enforcement powers and national security interests. Third, the metric of *cost versus efficiency* in the case of nuclear power only affected national governments who purchased the technology, and economies of scale reduced the costs, as did foreign policy subsidies. In the cryptography policy discourses, the cost versus efficiency debate involves industry interests, civil liberties, foreign availability of products, sometimes developed by individuals, changing government interests, and media that grew interested in the issue. Therefore, the conflict of principles (Braithwaite and Drahos 2000) within the two policy discourses were quite different.

In summary, the technology and economics literature assumes a benign policy. It is argued that the technology policy promotes the development of technology and its diffusion. Finally, technology is seen as a creator of externalities, and accordingly is induced by and induces economic change (Nelson and Soete 1988 p.633). Within cryptography policy, however, the policy-setters are self-interested, and diffusion is not necessarily supported by the policies considered. Cryptography, arguably, does more than create externalities; it also shapes interests and constrains action. A more ideal body of literature, for this study, would recognize the prevalence of self-interest within all the actors, and a more active role for technology apart from the end result of policy or a creator of externalities.

2.2 On Regulation

The literature on Regulation has long seen the politics involved in regulatory policy. It also has a poverty in explication, however. According to Stigler,

> There is an interesting asymmetry in the success of this literature in dealing with two problems into which the theory is commonly divided: Why are regulatory policies adopted and abandoned? What are their effects? Economists have been much more successful in measuring effects of policies than in explaining their adoption. The explanation is that one can choose the effects of a policy to study, and usually more easily measured effects are chosen for study. (Stigler 1983, p.541)

Explaining the formation and transformations in cryptography policy in the U.S. and the UK is therefore a challenging task. This section will review the approaches of regulation theories.

The literature on regulation is filled with divergent theories on actors, interests, and even explanations of policy shifts. In fact, even a description of what constitutes regulation remains unresolved. Separating the definition of regulation from the politics of regulation is not easy.

> The paramount role traditionally assigned to government regulation was to correct the failures of the private market (the unconsidered effects of behavior on outsiders), but in fact the premier role of modern regulation is to redistribute income. (...)This change in the fundamental role of regulation is so widely accepted, and so copiously documented, that it would be pedantic to cite the vast and growing host of supporting studies. (Stigler 1988, p.xii)

This regard acknowledges self-interest and politics: policy is not necessarily benign.

To explain what regulation does, Baldwin and Cave (1999) describe further dimensions aside from wealth deployment. They start by first considering the "the basic capacities or

resources that governments possess and which can be used to influence industrial, economic, or social activity" (p.34). Governments have the capacity to command using legal authority to pursue policy objectives; the ability to harness markets through channelling competitive forces to particular ends; to manage information flows such as those used in consumer protection; to confer protected rights, using incentives and constraints; and to act directly on the market and affecting individuals.

Knowing how government regulates, and what regulation does, does not mean that there is a consensual understanding of regulation and its purpose. Other disciplinary approaches to understanding regulation have arisen, growing beyond economic theories (Baldwin, Scott, and Hood 1998, p.35). Each discipline in turn has its own perspective on the roles of regulation. According to Thatcher (2000), the differing interpretations of regulation can be summarised as

Classical economics

Regulation is an interference in the market that may be necessary

Political economy

Regulation is inherent to society, such as laws of contracts, used by the state to ensure that the market functions

Political Science and Law

Regulation steers public activity; regulation is concerned with controls over private activity

Sociological

Regulation is information norms that guide behaviour

Thatcher argues that each of these are problematic: classical economics rests on a purist view of what constitutes a market; political economy fails to discern between purposeful action and action that occurs anyway; the political science and law interpretation is culturally-bound; and the sociological is too broad.

Similarly, Baldwin, Scott and Hood (1998) offer three definitions to regulation. The first involves the "promulgation of an authoritative set of rules, accompanied by some mechanism, typically a public agency, for monitoring and promoting compliance with (...) rules." (p.3) A second definition involves all efforts of state agencies to steer the economy, consistent with the political science definition. Finally, they offer the more all-encompassing definition of regulation as "all mechanisms of social control -- including unintentional and non-state processes" (p.4). This last definition incorporates some sociological ideas.

> Thus a notion of intentionality about the development of norms is dropped, and anything producing effects on behaviour is capable of being considered regulatory. Furthermore a wide range of activities which may involve legal or quasi-legal norms, but without mechanisms for monitoring and enforcement, might come within the definition. (p.4)

This last definition is sometimes considered the 'European approach', taken as a synonym for 'governance' (Hood 1994, p.19); and is consistent with approaches taken in socio-legal studies (Lessig 1998).

The social-control or socio-legal definition is taken further by Braithwaite and Drahos (2000), who reframe the very objects and subjects of regulation, incorporating a number of mechanisms used by both the powerful and the weak. Regulation, in their view, consists of plural webs of many actors that regulate while being regulated themselves; individuals, states, industries, organisations are objects and subjects of regulation (p.10). In their compendium of global business regulation, Braithwaite and Drahos identify actors, mechanisms, and principles that arise within a discourse, of what they call a *web-of-influence*. This framework (actors-mechanisms-principles) helped them to analyse the conduct of the discourse and the regulatory outcome. In each discourse studied, a number of these actors attempted translations (to ally or co-opt other actors; see chapter 3), and principles conflicted and aligned, as various policies were attempted using different mechanisms. In a sense, the regulation can not be separated from the discourse.

As a result, this dissertation interprets regulation as a sociological phenomenon, in accordance with Baldwin, Scott, and Hood's consideration of wide mechanisms of control. While I focus on regulations that begin with intervention from the state, the outcome of the regulations that are included in this study are not limited to state-sanctioned activity. Therefore, the Braithwaite and Drahos definition involving actors, mechanisms, and principles sought within what I call a discourse, and they consider a web-of-influence, is the definition of choice for the purpose of this study.

As with definitions of regulation, both the conduct of the actors within regulatory discourse and the means of explanation vary. The following subsection will review the theories of actors and action commonly used in regulation studies.

2.2.1 On Regulatory Actors and Interests

There are a number of divergent schools of thoughts on how to view regulatory strategies, the actors, and the interests that arise. The topology of these approaches presented here are from Thatcher (2000).

Public Interest

This is the oldest approach to regulation, involving a functionalist perspective with an apolitical ontology. That is, state action is considered a means to correct market failures, or in the 'public interest', managing natural monopolies, public goods, and externalities that may arise (such as in the area of defence, or pollution issues), informational problems, and transaction costs.

This is a paternalistic approach where government is assumed to have more information than other actors. Regulation is considered a positive development in its own right (Hood 1994, p.20). There is often little explanation, however, of how the 'public interest' is actually achieved through regulation. This is symptomatic of a lack of regard of the self-interest of government and the regulators, similar to the problems with the technology and economics literature.

Capture / Cyclical

This theory arose as political scientists noted that in some cases the regulators and the regulated achieved a level of consensus. This occurred particularly when regulatory agencies were taken over by the interests of the regulated (Hood 1994, p.21); in effect they become enrolled (Latour 1991). In this view, regulations are a means of protecting the interests of the regulated industries rather than as a means of protecting the interests of consumers and new entrants into a market (Baldwin and Cave 1999, p.36).

A benefit of such an approach is that it explains regulatory change (as regimes are translated in the interests of the regulated), emphasising conflict, interpretive flexibility of regimes, and subversion of intentionality. This theory is weak, however, at explaining why some regulations fail to meet the interests of the regulated industries, as it lumps together the interests of the regulator and the regulatees uncritically. Even within a given industry affected by a regulation, a number of interests may exist; this theory presupposes monolithic interests that may be embedded within a regulator, something that Hood (1994, p.22) qualifies as 'simplistic'. It also pays insufficient attention to the interests and actions of other actors such as the courts, consumers, and voters.

Capture theory is an improvement from the public interest theory as it considers the politics of regulating, and translations of interests. By limiting its analysis to monolithic 'industry' and 'regulator' actors and interests, this approach will not help in showing the richness of the discourses, however, including the multitude of actors and interests involved in cryptography policy.

The Economic Theory

The *Economic Theory of Regulation* is associated with the Chicago School (Stigler 1988). Regulation is seen as arising from the interaction between rent-seeking interest groups demanding regulation and politicians supplying it. It is argued that all forms of regulation actually disadvantage consumers, as interest groups pursue regulatory rents, and these groups tend to be producers or powerful users (Hood 1994, p.23).

This approach allows for an analysis of specific interests in specific actors. The school's view of interests, however, is criticised as being too narrow as it focuses only on material self-interest, failing to see other possible interests (Hood 1994, p.24). Assuming the interests of actors for the sake of explanation is hazardous; rather articulated interests may emerge from the discourse, be contingent, and perhaps conflicting.

Public Choice Theory

Public choice theory separates politicians from regulators, seeing even more actors make up the discourse. Politicians are seen as a group of actors interested in maximising budgets, distributing patronage; or perhaps instead as actors seeking smaller government through tax cuts. Bureaucrats and regulators are seen as actors pursuing larger budgets, or wishing for autonomy, power, and prestige.

Approaching regulation studies in this way permits an elicitation of numerous motivations behind a given regulatory regime, beyond simpler rents like money and votes. This view does not explain deregulation adequately, however: if interests are aligned behind a regulatory regime, there is little reason for regulatory change (Noll 1998, p.140).

Historic Institutionalism

In this theory, institutions are the most important units of analysis. That is, institutions are stable and have a history, and in turn affect which actors have power. This view helps to explain why different states develop different interests and in turn different regulations.

In a move beyond economic and public choice theories, interests are seen as emerging from a context, rather than something to be assumed. While this theory can explain differences among regimes, it suffers from failing to explain regulatory trends and changes (Thatcher 2000).

The above review of a number of theories has led to an appreciation of approaches that looks for many actors within a regulatory discourse. Importantly, interests should be

allowed to emerge from the data, rather than be assumed. In the above set of theories, however, the actors are also assumed to be purely social beings; an allowance may be created for technological actors as well.

2.3 Regulation and Technology

The above approaches to regulation focus on the interests and actions of humans. It was considered novel when the Chicago school began to encompass "phenomena previously treated as exogenous in economics" (Stigler 1988, p.ix) by including politics. Understanding that a technology policy discourse also includes technology is arguably another step in understanding regulation.

The need to consider technology in regulation is not new. While it may be acknowledged as a disruptive force, as Peltzman notes within telecommunications rate structures (1989, p.117) and interest rate regulation (p.121), it is not investigated in detail. Levin (1966) notes, with regard to radio spectrum management, that "(n)ew communications has required the reexamination of many policies and assumptions in recent years." Porter and van der Claas (1995) find that the literature on environmental regulation tends to assume a static view of the technology, products, and processes, and supported the idea of bringing technology into the regulation to stimulate innovation and competitiveness. Sprinz and Vaahtoranta (1994) find that technological factors could lessen costs and increase the likelihood of countries supporting international environmental regulation. While the previous section reviewed how actors and interests construct regulations, it appears that technology may construct and disrupt regulations.

The inclusion of technology into regulation theory is proposed by Lessig as the New Chicago School (Lessig 1998). Consistent with the Old School in seeing law as merely one regulatory mechanism, both schools consider how the market and norms may also regulate action effectively (Lessig 1998, p.665). Lessig argues that *architecture* can also regulate individuals.

> I mean by 'architecture' the world as I find it, understanding that as I find it, much of this world has been made. (...) These features of the world -- whether made, or found -- restrict and enable in a way that directs or affects behavior. They are features of this world's architecture, and they, in this sense, regulate. (p.663)

He builds from Bentham and Foucault's conceptions of the panopticon to show how structures regulate (p.665-6).

Regulation, as a result, is exerted by the market, laws, norms, and architecture. These *modalities of regulation* (Lessig 1998, p.663) regulate differently (p.664). Markets may regulate through the device of price (p.663); laws threaten through sanction *ex post* (p.662); and norms constrain human behaviour in an informal manner (p.662, fn.7). Changing any of these modalities changes regulation.

In his later work, Lessig (2000) goes even further to say that Code, the constitution of architecture, is akin to Law as a regulator of human action. Lessig questions whether code can be regulated by law, i.e. the *regulability* of Code (p.19). His answer is that some architectures are more regulable than others (p.20). From this, he warns that governments would favour *regulable* architectures more; and contends later that industry would as well (p.44).

Law may regulate technology, or any other modality in a process called *indirect regulation* (Lessig 1998, p.666), akin to what Black (2000) calls 'gatekeeper' regulation. Lessig provides two American examples of indirect regulation: the Communications Assistance for Law Enforcement Act (CALEA) and cryptography policy. In the former example, CALEA involved a subsidy for developing interception capabilities in new telecommunications infrastructure,

> Its indirect effect is to improve law enforcement, but it does so by modifying code-based constraints on law enforcement. It selects an architecture that distributes the burdens of code in a collectively valued way. Regulation likes this works because telephone companies are few. (...) Thus, indirect regulation depends on there being a useful target for regulation. But if there is such a target, and that target can control the code of the network, then the government can regulate the code. (Lessig 2000, p.45)

Indirect regulation "may allow the government to achieve a regulatory end without suffering political cost" (Lessig 1998, p.690). Rotenberg (2000) notes that this is indeed a contribution to understanding CALEA: while the objective of previous regulations was to constrain the actions of the government, CALEA regulated industry and the technology to meet the interests of government.

With cryptography, the strategy also involved regulating the market. Lessig argues that through subsidising the development of government-approved cryptography, the U.S. government was indirectly regulating to ensure for surveillance through the market modality (2000, p.48).

Lessig's argument is that we should look at the full process through which regulation works.

> I believe we need a more general understanding of how regulation works. One that focuses on more than the single influence of any one force such as government, norms, or the market, and instead integrates these factors into a single account. (2000, p.86)

The four modalities of regulation and their interplay is the unit of his analysis. Each is interdependent.

> Each (modality) can support or oppose the others. Technologies can undermine norms and laws; they can also support them. Some constraints make others possible; others make some impossible. Constraints work together, though the function differently and the effect of each is distinct. (...) Each modality has a complex nature, and the interaction among these four is hard to describe. (2000, p.88)

Technology can therefore be constructed to regulate in accordance with law; but can also disrupt legal regulations.

Missing from Lessig's formulation is how technology can be shaped, or translated, or disrupts, within a regulatory discourse. He seems to focus on dismissing the ideas of technological determinism that were predominant in the 1990s with regards to the Internet.

> There were times these other constraints were treated as fixed -- when the constraints of norms were said to be immovable by governmental action, or the market was thought to be essentially unregulable, or the cost of changing real-space code was so high as to make the thought of using it for regulation absurd. But we see now that these constraints are plastic. That they are, as law is, changeable, and subject to regulation. (Lessig 2000, p.91)

He does not sufficiently or consistently elaborate on this 'plasticity', however.

At one point Lessig appears to claim that, unlike how norms and markets may resist regulation, technology will acquiesce because it is naturally regulable (2000, p.91). He notes later that technology can constrain regulation (p.189), thus reducing the power of the state. "To understand a state's power to regulate we must ask: How well does its infrastructure support a structure of regulation?" (p.189)

Again later he attends to the idea of technology resisting law and regulation.

> What unites (architectural constraints to regulation) is the agency of the constraint: no individual or group imposes the constraint, or at least not directly. Individuals are no doubt ultimately responsible for much of the constraint, but in its actual execution the constraint takes care of itself. Law needs police, prosecutors, and courts to have an effect; a lock does not. Norms require that individuals take note of nonconforming behavior and respond accordingly; gravity does not. The constraints of architecture are self-executing in a way that the constraints of laws, norms, and the market are not. (Lessig 2000, p.236)

Lessig does not offer a means for capturing this constraining of regulation, nor theoretical grounds for analysing its plasticity. He warns, however, that "a complete account of how constraints change is an account of how these different constraints interact, but the complexity of this complete account easily overwhelm." (1998, p.685)

This is not just a study of the modalities, however; it is a study of a socio-technological discourse through which policy is negotiated.

2.4 On Transformative Regulatory Discourse

The theories outlined above, their treatment of actors and interests, social or technological all deal with the issue of regulatory transformation and reversal in different ways and with differing levels of success. Cryptography policy discourses arose from changing conditions, changing interests, problems with the existing policies, changing technology and international conditions, amongst other reasons. Accounting for these transformations and pressures is another challenge of understanding regulation.

2.4.1 Explanations for Regulatory Transformation

A number of explanations of regulatory transformation arise from the literature; Hood (1994) classifies these into four types. First are explanations on how reversals arise from new ideas and the arising force of these ideas that upset the *status quo*. Second, reversals can be seen to arise from the pressure of interests. Third, transformations arise from changes in the social 'habitat' that makes old policies obsolete. Finally, there is the explanation that policy reversals arise from endogenous factors, where policies and institutions self-destruct.

Force of Ideas

This type of reversal involves a transformation of the ideological climate caused by intellectual developments and changes in the world of ideas (Hood 1994, p.5). New ideas can arise through the release of experimental evidence, logical force, or rhetorical power.

This type of explanation is often used for the success of deregulation policy in the 1980s. Deregulation is explained by the flow of ideas from the Chicago school of regulation, fed into the design of new regulation, in essence destroying the very idea of regulation. This also occurred at the time of the persuasive power of the new right and economic rationalism (p.28).

Power of Interests

This view of reversals places the dynamic of political interests into the centre of the theoretical stage, and explains policy development by the formation of new interest coalitions that stand to benefit from change (Hood 1994, p.7).

In essence, this involves contextual social and economic change (p.8). A number of dynamics are identified within this contextual change, including coalition behaviour in the domestic sphere; dynamics in international politics involving state alliances or where states innovate on policy due to international incentives; and finally a process of 'policy entrepreneurship' where policy entrepreneurs put together support for new policies (p.8) through mobilising diffused beneficiaries of policy change and turn them into votes (p.30). Particularly, the larger the cost of regulation, the greater incentive for the losers to organize (p.32).

There are also situations in which those who benefit from regulation as originally designed may find it in their interests to demand regulatory change, even deregulation. This arises when producers decide that they could gain more market share under a new regime; or where companies decide to break into new, previously protected markets.

Changes in Policy Habitat

Particular social structures form the 'habitat' for a policy; when the social structure changes, policy habitats are altered (Hood 1994, p.10). Changes to a habitat also involve background changes in technology. Hood notes a relationship between this view and views regarding the 'post-industrial society' with their consideration of new technologies (p.11). Policies can shift if technology or other developments affect the original purpose of regulation; such as market failures in telecommunications with new switching systems, alternative means of communication such as microwaves and satellites, or regulations in banking and finance being changed by technologies affecting market structure (p.47).

There are faults in both these views, however (p.12). Firstly, Hood contends that change in policy is not automatic from technological change. Secondly, just because similar policies are adopted by different societies, this does not necessarily mean that they are responses to similar functional problems. Finally, Hood argues that such explanations are often too technocentric, leaving little room for the dynamics of politics. Regulatory change occurs in many technological sectors but does not always require technological change (p.149).

Self-Destruction

In contrast to the deterministic effects of exogenous factors, the self-destructive view of change explains reversals arising from internal forces. Institutions or policies may lead to their own demise (Hood 1994, p.13). If the worldview is that actors are seeking rents from the state and related institutions, over time this produces an increasingly 'sclerotic' economy, and the basis on which the policy rested is destroyed (p.13). Groups of actors who aligned to seek rents may find incentives to cheat on other members, and the coalition begins to fall apart, and the rents no longer provide the protection previously expected (p.33).

Alternatively, there is the view the policies themselves create unexpected side effects that create conditions for the introduction of new corrective policies. In particular, it may be noticed that some actors are benefiting from being outside the 'ring-fence' of the regulation (and offering near-substitutes to the regulated product). Either the policies would be broadened to include other sectors, or deregulation may be introduced (p.34).

Other explanations involving policy self-destruction may consist of a combination of factors. Some of these factors may include intellectual changes or institutional self-destruction and changing balances of interests. Hood's argument, however, is that none of these explanations are sufficient on their own; even in defining each type of explanation there are overlaps with the others. "Put 'ideas' in a glass case, and 'interests' start crawling in too. Put 'institutions' in the case, and sociotechnical changes start to intrude." (p.17) In each area of regulatory change there are articulations involving ideology, interests, shifting habitat due to economic and sociotechnical change, and self-destruction.

2.4.2 Factors of Change: Technology and Arbitrage

There are two issues in the background of Hood's study. First is the role of technology. Second is regulation in an international context.

Regarding technology, Hood notes that

> It is fashionable to decry 'contextualism' in political science, that is the notion that politics is narrowly determined by social and technological change. But it seems hard to ignore the effect of long-term changes in technology and related social behaviour in accounting for policy change. (p.148)

Even as theories assume a change of policy habitat, they fail to deal with technology adequately.

> What is not so clear is the role, if any, played by broader sociotechnical developments, since few accounts of deregulation put this element at centre stage and it seems at best to have been part of the background. (p.36)

Meanwhile, international politics and 'bandwagoning' to modernize economies and other related rhetoric can have an effect.

> What needs to be shown is how international politics should have changed to cause governments to reverse policy. Again it may simply be that the 'policy habitat' changed. So if the international politics regime favoured public enterprise from the 1940s to the 1960s, what changed the nature of the international game by the 1980s? (p.48)

This could even be explained as a habitat loss to Keynesianism due to altered global conditions (p.77). Yet there may be other explanations as well. He continues that

> technological competition may have changed the kind of assets which counted as 'strategic' for state sovereignty. For example, nationalization of railways in Japan in 1906 was heavily motivated by military considerations, and the same went for telecommunications in many states. (...) (B)ut as transport and communication technology moved on after the Second World War, railways or telephone systems may have become increasingly irrelevant to defense and security. (p.48)

Changing perceptions of technology and international politics and the related strategic value of both may affect regulatory change. These fall under all of the explanations, however, and are inter-related.

> Habitat change, including the globalisation of markets (...), the development of financial markets and the erosion of technological insulation of some sectors, are stressed by many commentators as part of the explanation for the shift (...). Hence such habitat changes are hard to separate from the changing patterns of interests, particularly the rise of (...) the role of policy entrepreneurship. And policy self-destruction is stressed (...). Hence, onœ more, a 'cocktail' of processes may have been at work, incorporating some combination of habitat change, self-induced destruction and the development of new predators hunting these life forms to extinction. (Hood 1994, p.56)

Technology and international politics may have significant roles to play in any explanation of policy change, as they may affect ideas, interests, habitats, and create the conditions for policy self-destruction.

International pressures to change policies have been investigated in some detail by the regulation literature. Differences in policies in various countries give rise to competition under a number of pre-conditions. Notably, a precondition is that actors must have freedom of movement between jurisdictions and information regarding alternative

regulatory regimes in other countries (Baldwin and Cave 1999, p.180). Sun and Pelkmans (1998, p.459) argue that there must be a credible likelihood of movement. Then regulatory competition may occur, consisting of a competitive adjustment of rules, processes, or enforcement regimes in order to secure an advantage, usually attracting investment with a more favourable environment (Baldwin and Cave 1999, p.180). So long as regulatory competition exists, countries can not establish overly restrictive regulations (Sun and Pelkmans 1998, p.457).

This does not infer an immediate flight risk of producers, technology, and consumers. Transaction costs for firms to operate across jurisdictions may be high. Regulators may find it in one another's interests to collaborate to manage externalities, or may collude to limit competition (Baldwin and Cave 1999, p.184). This lends towards ideas of harmonization of policies in order to remove distortions in business uncertainty across borders (Sun and Pelkmans 1998, p.461). As a result, regulations can change in any direction: regulations may be pushed to the lowest common denominator where competition is high, but regulations may equally benefit from the 'California effect', where one regulator pushes for the highest standards, setting models for others to follow (Baldwin and Cave 1999, p.188).

Harmonization requires further interrogation, however. In their review of global business regulation, Braithwaite and Drahos (2000, p.482-3) find that some countries (notably the U.S. and the UK) push for certain regulatory standards in international bodies and then bring those regulations home under the requirement of harmonization and the guise of multilateralism. Alternatively, these same countries push for weaker regulations to meet the interests of national industries to allow for increased trade, using mechanisms such as economic coercion, reciprocal adjustment, and modelling.

Explaining change within an environment of politics and negotiation involving regimes, technology, and international issues only becomes more challenging. Hood's view of 'explanations' is that they are emergent, interpretable, and difficult to identify authoritatively. In fact, they are also based on ontological, epistemological, and methodological approaches, brought to light particularly in comparative studies.

> (E)ven if a similar pattern of policy extinction appeared to take place in several countries, we cannot necessarily conclude that those extinctions occurred everywhere for the same reason and with the same effect. In fact, it often happens that reforms which look similar when viewed from a distance turn out to have been adopted for quite different purposes and with different effects. (Hood 1994, p.152)

In my studies of the U.S. and UK policies it would be tempting to promote the idea that liberalisation is inevitable and occurred for the same reasons, with the same results.

Although they exhibit similar tendencies, the discourses were quite different. Hood's work suggests following the establishment of a policy by hearing many explanations and accounts, with an ability to approach the data from a micro and macro perspective; while also incorporating some of Lessig's framing to include technology and Braithwaite and Drahos' attention to international politics, as well as their analytical frame.

2.5 Technology within a Changing Regulatory Discourse

Following from Stigler's challenge to understand the formation of policies, the above literature review tried to understand the actors and interests that are included within such studies. Beginning with apolitical assumptions regarding the government and its legislators, and the observations of political scientists on the capturing of the interests of the regulators, a number of theories emerged on how to account for the emergence of regulation. Generally, the regulatory process is seen as a locus for actors pursuing interests; although the number of actors, the granularity of these actors, and the complexity of the perceived interests varied.

In this dissertation I view regulation as a discourse, where change is inherent, consisting of multiple modalities, actors, and interests affecting one another. I also introduce the notion of looking at the non-humans, the technological actors.

Looking at regulatory discourse involves looking at how regulations form, shift, transform, and are reversed. There are a number of explanations for why regulatory change occurred, based on a number of theories regarding regulation and interests. In a relevant example, Hood says that institutional understanding of regulation may argue that because state mail services were set up as public monopolies to allow governments to conveniently spy on their subjects' correspondence (Hood 1994, p.37), one may assume that when the UK Conservatives nationalized telegraph companies in 1869, considerations of national security may well have been *invoked.*

> But it is also notable that the event took place just before a general election and was used to pick up rural votes by cross-subsidizing less profitable rural telegraph services from the proœeds of profitable urban areas. (p.42)

Understanding interests of actors may be a complex process, and may be interpreted in many ways. Interests are not necessarily monolithic, with government pursuing its own interests of re-election **or** national security, and industry pursuing rents necessarily (Hood 1994, p.22). Interests are also possibly contingent; otherwise policies presumably

representing the interests of the actors involved in the establishment process would never change as the alliance between rent-seekers and government would remain static.

Even Stigler notes that explaining the emergence of a policy based on self-interest or on interests at all is unsatisfactory because political activity is conducted by coalitions (Stigler 1988, p.xiii). He then calls for research on how coalitions are formed, or abandoned (p.x).

Consensus is not necessarily the outcome of coalitions, alliances (Braithwaite and Drahos 2000), or alignments (Latour 1991). Negotiations occur at all stages; and policies transform and shift due to recalcitrance of actors who fail to align, including technological actors.

Braithwaite and Drahos' remarkable research (2000) tried to focus on the actors and the process through which alignment is achieved: translation. Translations of goals of various actors occur as alliances are formed within networks of actors. Mechanisms are used to promote and shift regulations. Braithwaite and Drahos map the use of mechanisms to monitor the successes of translations.

Within the realm of actors, the traditional actors usually appear, including government and industry, but Braithwaite and Drahos also note within each case the existence and influence of Haas' notion of the *epistemic community*.

> An epistemic community is a network of professionals with recognized expertise and competence in a particular domain and an authoritative claim to policy-relevant knowledge within that domain or issue area. (Haas 1992, p.3)

Within each regulatory study they identify the role of the epistemic community in shaping the eventual outcome, alongside the other more traditional actors.

Braithwaite and Drahos find that there are many actors involved within a regulatory discourse, or a web of regulatory controls that are continually rewoven to remake the regulatory state (p.548). Negotiation and translation, and alliances and alignments are the constitution of this discourse. They argue that an interests-based approach is unlikely to be successful to explain these alliances and translations. This is because of the number of motivations each actor exhibits within a given regulatory environment (p.547).

As a result they abandon rational-choice accounts of economic and international relation theories (p.548). Rather, to understand a regulatory regime they argue that we must investigate the process through which it was established; researchers should go back and reconstruct how each 'brick was laid', by which actors pursuing which *principles*.

> While most actors may lack any synoptic grasp of their interests, we can understand how concern gets mobilized among a limited range of actors with a capacity to lay some bricks. We find that once such concern is catalyzed, the bricks most likely to be laid first are principles in a framework agreement or convention. (p.548)

The principles are common articulations that can be derived from the theories explaining regulatory emergence and regulatory change; we see these articulations as we monitor the discourse, and discover others as they emerge (Braithwaite and Drahos 2000, p.30). Such articulations include strategic trade, harmonisation, transparency, national security, national sovereignty, and lowest-cost location (p.26). From each discourse additional principles may emerge as we listen to the stated motivations of actors, their concerns, and their efforts to establish alliances. As a result, the negotiation of regulatory regimes is more appropriately seen as a contest of principles between actors, rather than only as a conflict of monolithic pre-assumed interests.

One weakness in their work, however, is that Braithwaite and Drahos fail to incorporate technology into their frame of reference sufficiently, although they do allude to it briefly in the context of telecommunications policy (p.322). While the technological is beyond the scope of their study, I contend that it is an essential component of the discourse. It may not always play a large role, but it is likely to be present, and should be interrogated. Considering the statements quoted at the start of this chapter regarding automobile safety, inadequate or insufficient interrogating of notions regarding technology, costs, and risks, may lead an imbalanced understanding, if not absurdity.

Incorporating technology into the unit of study must be done carefully. While it may be tempting to consider technology as part of the policy habitat, Hood's critique of such notions is that they grant technology a level of determinism; regulatory change is not automatic from technological change (1994, p.12). Society and technology theorists are well aware of these concerns. This is consistent with the anti-essentialist theory that argues we must never assume that technology is an object in itself with its own capacities, but rather these capacities are always being interpreted (Grint and Woolgar 1997).

Therefore a richer view is required. Technology may not be deterministic; yet, human action is not deterministic either as technology objects and also regulates human action. Lessig argued for consideration of *modalities of regulation* that constrain individuals. While he regards these constraints as plastic, and malleable, he does not give sufficient regard to how the shaping and malleability is considered. Like Hood, Lessig is trying to combat determinism. In so doing he does not allow for how the other modalities of regulation will interpret the technology in different ways (e.g. the market views cryptography differently than the law).

Following from Lessig and Hood, I contend that in the foreground of our techno-regulatory analysis we need to have both societal and technological factors, interacting, interpreting, and objecting.

> Thus in its design stage, the character of an object is endlessly debated; what will it look like, what will it do, what will it be used for, what skills will its users need, what maintenance will it require? Such talk is heterogeneous. Indeed engineers transform themselves into sociologists, moralists or political scientists at precisely those moments when they are most caught up in technical questions. (Callon 1991, p.136)

The work of Callon and Latour, their sociology of translation, later Actor-Network Theory and beyond, argues that we can move between levels of analysis (Latour 1991, p.124), look specifically at the technology and how it is spoken for, and argue how discourse is heterogeneous, with humans and non-humans.

Within a discourse a number of strategies are attempted, programs of action where new actors are introduced and new mechanisms are added to attain a desired outcome. In turn, if we look at regulation as a socio-technological discourse, with human actors inscribing interests into regulation and technology, interpreting the technology, but the technology being able to object, then we may better understand how a policy habitat is developed, sustained, and lost; how the interests of actors are transformed; how new ideas force regulatory change; or how the policy may self-destruct. This also involves adding other actors, other mechanisms, introducing new principles, and other strategies to the regulatory regime in an attempt to translate the actors to meet the goals of the translator, or the regime. These ideas will be further investigated in the next chapter, as I develop a means of capturing socio-technological discourse. The notion of this socio-technological discourse as a regulatory discourse will be analysed in section III of this dissertation, in a review of the policy negotiations in the U.S. and the UK, as presented in section II.

Chapter 3: Capturing the Technological Actor

I was in a lifeboat, designed for ten, and ten only. Anything that systematic will get you hated. It's not a deal, nor a test, nor a love of something fated.

-- **nautical disaster**, The Tragically Hip

There is a remarkably close parallel between the problems of the physicist and those of the cryptographer. The system on which a message is enciphered corresponds to the laws of the universe, the intercepted messages to the evidence available, the keys for a day or a message to important constants which have to be determined. The correspondence is very close, but the subject matter of cryptography is very easily dealt with by discrete machinery, physics not so easily.

-- Alan Turing

Abstract

The *technological* is often in the background of both the regulation literature and the Information Systems literature. This chapter reviews the literature on society and technology to understand how we may find the *technological* within a discourse. This chapter then proposes that within a discourse there are *moments of interest* where we can observe, interrogate, and develop an understanding regarding the form of both the *social* and *technological* actors.

3.0 Cryptography Determines or is Determined by?

The first chapter of this dissertation introduced cryptography and the types of cryptography policy pursued by governments. The second chapter introduced the notion of regulatory discourse, and the potential for considering this discourse as socio-technological. This chapter will present the means to capture socio-technological discourse at *moments of interest*, when the actors, *social* and *technological* take form.

A key question arising from technology policy discourses is whether technology is thrust upon us as an external force, or if we have a duty to shape technology to meet social goals. This is indeed the crux of the cryptography policy debate: cryptography will force governments to abandon their capacity to intercept communications; or cryptography needs to be constructed in order to serve public policies and the public interest.

In the mid-1990s, a debate raged between Dorothy Denning, a professor in computer security who supported constrained use of cryptography, and a group of *cypherpunks*, often libertarian technologists who believed that unrestrained access to cryptography was a positive inevitability. In the Cypherpunks Manifesto, it is argued that a revolution was about to occur because of technology and cryptography:

> The technology for this revolution (…) has existed in theory for the past decade. The methods are based upon public-key encryption, zero-knowledge interactive proof systems, and various software protocols for interaction, authentication, and verification. (...) The State will of course try to slow or halt the spread of this technology, citing national security concerns, use of the technology by drug dealers and tax evaders, and fears of societal disintegration. (...) But this will not halt the spread of crypto anarchy. (May 1994)

Cypherpunks see cryptography as a force, and this will change the world. In this debate, Denning (1996) responded

> the crypto anarchists' claims come close to asserting that the technology will take us to an outcome that most of us would not choose. (...) A new paradigm of cryptography, key escrow, is emerging and gaining acceptance in industry. Key escrow is a technology that offers tools that would assure no individual absolute privacy or untraceable anonymity in all transactions. I argue that this feature of the technology is what will allow individuals to choose a civil society over an anarchistic one. (Denning 1996)

This is a preference for a more socially constructed technology. Both camps included experts in security and cryptography, but their ideas and interpretations diverged.

There are also differing views on the actual *nature* of the technology. Cryptographers define cryptography as a mathematical method. Engineers define it as a science. When the U.S. Government announced its first policy of the 1990s, cryptography was discussed as a

> dual-edge sword: encryption helps to protect the privacy of individuals and industry, but it also can shield criminals and terrorists. (The White House 1993)

Human rights advocates and libertarians consider cryptography as a protection from oppression. There is similar confusion over the definition of *strong cryptography*, whether it merely involves large keys (at least 128-bits for symmetric cryptography or 1024 for asymmetric); or if it must also exclude any form of key recovery/escrow due to the risks introduced or the political implications; or if its strength is based on the difficulty of *some* opponents in decrypting the ciphertext. Similar *articulations* are considered within Section II.

Bringing these articulations together, and making sense of the discourse that arises, is challenging. The Information Systems literature is a useful place to start, as are the ideas from the literature on society and technology.

IS research, however, has been accused of poorly attending to technology, and this is reviewed in §3.1. The idea of giving sufficient regard to both the social and the technological will be introduced in §3.2. A review of the society and technology literature in §3.3 will present the possibility of considering both social and technological actors within

various theories and approaches. There are also gaps within this second body of literature, and solutions are proposed in §3.4. Finally §3.5 summarises and generalises the moments of interest within socio-technological discourse when the actors take form.

3.1 Technology and Society within *IS*

Information Systems is a discipline that is positioned perfectly to acknowledge the roles that technology, the markets, and governance play together in a system that can be considered as *socio-technological*. Bowker et al. (1995) argue that information infrastructures change work practice, knowledge, and moral order though allocating resources and structuring markets. Hanseth et al. (1995) see standardisation of infrastructure as having "far-reaching implications of economic, technical, and social nature." Steinbart et al. (1992) claim that technical problems associated with establishing and running a global computer network is aggravated by the existence of politically imposed constraints on international communications and data flows.

IS uses the social sciences, rather than natural and technical sciences, because its proponents believe that the socio-technological view brings more depth and value in analysis of the use of information and communications technology in a specific context. According to Walsham (1991), a neglect of the socio-political elements of the context of computer-based systems frequently has negative consequences in terms of human needs and aspirations. Computing technology has been found to be adopted selectively in a given social world and organised to fit the interests of dominant parties (Kling 1980). Vidgen and McMaster (1995) argue that a strength of IS is the potential to treat context and technology symmetrically, thus differentiating IS research from technology-facing disciplines such as computer science and engineering, and context-oriented disciplines, such as management.

The weakness of IS research, however, is that *the technological* usually remains in the background of the context, and subsidiary to *the social*. Monteiro and Hanseth (1995) suggest that IS researchers are not specific enough about the technology. They argue that we need to be able to describe in some detail how and where technology restricts and enables action. As a result they wish to support an inquiry that

> traces the social process of negotiating, redefining, and appropriating interests back and forth between a particular, explicit form and a form where they are inscribed within a technical artefact. (p.331)

For Monteiro and Hanseth, the artefact is the outcome of a discourse of negotiating the development, adoption, and use of technology. Looking at the artefact may allow researchers to understand the actors.

They apply their ideas to Orlikowski's research. First they critique a research case where she discusses Lotus Notes within an organisation (Orlikowski 1992b), and point out that she does not refer to its functionality. They find this disappointing due to the programmability of Lotus Notes. Then they critique another case study of a CASE tool in an organisation (Orlikowski 1992a). They argue that the technology is again regarded as a tool; to them, a CASE tool is actually the result of a long process where interests of management are translated into a heterogeneous network encompassing career paths, work guidelines, and methodologies.

Their notable critiques suffer from a shortcoming, however: Monteiro and Hanseth are not specific about the technology either. They do not describe how the CASE tool interacts with other entities, if there are unintended uses of the technology, the process of management inscription of interests into the tool (and the failures to inscribe such interests), and the arising interpretations, i.e. *interpretively flexibility*. While they believe that we must look at the discourse, and look specifically at the technology by *opening the black box*; Monteiro and Hanseth do not offer a means for doing so, nor what we should look for.

This is a point that Orlikowski and Iacono (2001) later pursue. They argue that IS researchers do not generally know how to regard the technological because we often we take it for granted.

> (T)he tendency to take IT artifacts for granted in IS studies has limited our ability as researchers to understand many of their critical implications - both intended and unintended - for individuals, groups, organizations, and society. (Orlikowski and Iacono 2001, p.133)

IS researchers may be accustomed to thinking about technology; and theories may reflect technology, but often in our research there is a lack of due regard (Markus 1997, p.16).

A preferable approach would study both the social and the technological. Social actors and technological actors are all part of the discourse; as researchers we may be accustomed to social actors, but the technological actors requires some attention and interrogation.

3.2 The Challenge of Symmetrical Actors

The work of Callon and Latour, beginning with the sociology of translation, and with other theorists who developed Actor Network Theory, and beyond, long argued for generalised symmetry as a form of analysis. Generalised symmetry is a state where human and non-humans are studied together, both as actors (Callon 1986), actants (Latour 1991), or entities (Latour 1999). Latour's argument for this approach is that

> (i)n order to understand domination we have to turn away from an exclusive concern with social relations and weave them into a fabric that includes non-human actants, actants that offer the possibility of holding society together as a durable whole. (1991, p.103)

He questions the division between technology and society, and searches rather for a network of actors including the non-human actor.

An actor, however, is contingent upon its capacity to act, and this capacity is dependent on relations to other actors (Lee and Stenner 1999, p.83). The action of actors is primarily *translation*.

> On one hand, the translation operation consists of defining successive layers of vocabulary, of attributing goals, and of defining impossibilities; on the other hand it consists of displacing -- hence the other meaning of translation -- one program of action into another program of action. (Latour 1991, p.125)

Callon (1991) develops the idea more practically as

> **A** translates **B**. To say this is to say that **A** defines **B**. It doesn't say anything about **B**'s status as an actor. **B** might be endowed with interests, projects, desires, strategies, reflexes, or afterthoughts. The decision is **A**'s -- though this does not mean that **A** has total freedom. (Callon 1991, p.143)

Translations may be intentional acts, or mere moments when **A** speaks for **B**; but there are limits to translations.

If **A** is to translate **B** then we have two problems. First, if **A** and **B** are symmetric and both brought into the foreground then we must allow for the situation where **A** may be a non-human. Such a situation where a non-human is translating a human may be interpreted, wrongly, as technological determinism. The second point is more elusive: some translations are more likely or possible than others. If a technological actor can resist the translation of a social actor, then this may be worthy of further study as it may say something about both the human and the non-human.

As a result, bringing the *technological* to the foreground of the analysis alongside the *social* gives rise to two immediate challenges for researchers. The first challenge for researchers is to avoid the problem of endowing the technological actors with interests. Such an approach may appear to place the social at the mercy of the technological or worse yet, may make the researcher appear to be a technological determinist.

The second challenge is to avoid rendering the technological actor as some mute agent. A technological actor can be (and is often within the social sciences (Latour 2000)) assumed to

be merely an agent that is waiting to be enrolled or aligned, endowed with interests by its creators, or the powerful. In so doing, however, we continue the trend of disregarding the technological and merely considering social forces; in effect social determinism (Hughes 1994).

We therefore need a way of giving form and focus to the technological and the social simultaneously without becoming deterministic. It is my contention that looking at the technological will shed light on the social; while our understanding of the technological can come from many social sources. The following subsections review the literature on society and technology in an attempt to resolve the role of the technological actor, to identify means of capturing socio-technological discourse.

3.3 Finding Moments within Society and Technology Research

The nature of technology (how it is thought up, developed, applied and how it is put to use, and then becomes part of society) is a challenge for those who construct technology, those who implement it, those who use it, and those who are affected by it. Technologies can be interpreted and be implemented in ways beyond the intentions of the developers. Technologies do have political strength as they may change social relations, but they can also stabilise, naturalise, depoliticise, and translate these into other media (Akrich 1994, p.222). And sometimes the technology is not even the issue. Consider the Russian involvement in the International Space Station.

> Although Russia's space station experience far outweighed that of the U.S.A., the decision to include Russia was rooted in politics, one of many consequences of the end to Cold War hostilities. In its simplest terms, it represented an attempt to deflect former Soviet industry from concentrating on missile production and, in times of financial crisis, to limit the 'brain drain' of engineers and scientists to 'unfriendly nations'. Thus ISS became the ultimate jobs programme, inextricably linked with U.S. foreign policy. (Williamson 1999)

The space station is an artefact, but could be portrayed as an active agent representing social interests.

The following review of the theories and approaches on technology and society will identify a number of different views towards actors, actions, and interests. We will also see varying regards to the nature of the social and the technological. From this review, an understanding of technological actors may emerge.

3.3.1 Anti-Essentialism

The greatest critique to any research approach that brings technology into the foreground of analysis comes from the anti-essentialist viewpoint. Anti-essentialism rejects attempts to discuss 'the technology itself' without scrutiny. The concern is that the *opening of the black box* concept implies that a technological artefact can be shaped most during the design process, and once its black box is closed, that is the design is complete, it becomes progressively less alterable (Grint and Woolgar 1997, p.19), and we are to live with the consequences of the black boxed artefact (p.27).

What emerges from the black box, according to Grint and Woolgar (1997) is not necessarily a consensual understanding. They argue that technology is an unstable and indeterminate artefact whose significance is negotiated and interpreted, but never settled (p.21).

> A technology's capacity and capability is never transparently obvious and necessarily requires some form of interpretation; technology does not speak for itself but has to be spoken for. Thus our apprehension of technical capacity is the upshot of our interpreting or being persuaded that the technology will do what, for example, its producers say it will do. (p.32)

Anti-essentialists are sceptical about arguments that discuss the *essential* features of technology, and the resulting presumptions that technology may be *distorted* by actors because the idea of distortion pre-supposes a natural state for the technology.

This reasoning has discourse-observation implications: opening the black box and looking at the technology specifically is a problematic process since only interpretations will emerge. Rather, Grint and Woolgar argue that we must listen to the various interpretations; listen for how the technology is spoken for (1997, p.35).

Anti-essentialism's *interpretive flexibility*, that is the way in which a technology can be interpreted in many ways for many applications, does have a limit. Anti-essentialists do not deny that there is a level of 'resistance', or objection, from the technology. It is not the case that all constructions are possible. "However, the important point (...) is to resist the idea that constructions result from some imagined intrinsic properties of the technology." (Grint and Woolgar 1997, p.10)

Ignoring the technology altogether is not recommended either.

> Importantly, this does not entail a policy of eradicating all accounts which mention or implicate technological capacity. Even if it were possible, this would be tantamount to concentrating only upon issues 'outside the black box', a form of social determinism which is as unsatisfactory as the technological determinism (...). Instead we need

> to find a way of 'taking the technology seriously' without having to depend on uninterrogated notions of technical capacity, and to account for the intermingling of technical and social without merely nurturing the view that these are essentially independent variables conjoined through 'interaction'. We want to avoid, in other words, the impression that either the technical or the social has a discrete impact. (Grint and Woolgar 1997, p.10)

This is the ontological, epistemological and methodological challenge: taking the technology seriously, being specific, and opening the black box, but without assuming that there is consensus on what is found within.

This view may be valuable from a methodological standpoint. Anti-essentialist analysis focuses on controversies -- that is when the technology is most debated and most interpreted. While presenting statements from various human actors at these moments will prove that the technology is interpreted and thus the human actors are representing the technology, we are also adding to our understanding of the socio-technological discourse. At worst, we learn only about the divergent interests of the human actors; at best we may learn something about the technological too.

The anti-essentialist point that some technologies may *resist* interpretation more than others is also valuable. This allows us to peer within the black box and listen to statements of human actors as to the ability and refusal of the technological actor from accepting translation.

However, this approach does not discuss in detail how we can make sense of the technological beyond collections of interpretations, how we can identify which speech to capture, and how we can understand the implications of a technology resisting interpretation.

3.3.2 Social involvement in the Technological

The general theme of the social construction or shaping of technology literature is that of alignment of various agents in the development and diffusion of a technology. Interests, politics, economics and other social issues are everywhere in this alignment process; sometimes constructing technologies, other times shaping them.

The social *construction* of technology approach sees technology and society as human constructs. Technology is shaped by societal structures and power relationships, and also by the ingenuity and emotional commitment of individuals (Bijker 1995, p.3); not necessarily through a rational process (Bijker and Pinch 1987, p.22). Technologies are shaped and acquire their meanings in the heterogeneity of social interactions (Bijker 1995, p.6).

Bijker (1995) provides a selection of case studies to elaborate this approach. After discussing the technology of light bulbs and fluorescence, he argues that General Electric's high-intensity fluorescent bulb was a social construction as opposed to the more readily developed high-efficiency bulb. The high-intensity bulb was created on a conference table by the Utilities companies and General Electric (GE). Utilities companies viewed the high-efficiency bulb as a threat to their interests. Making use of 'technical constraints' to support their arguments ('load on electricity networks', and 'the power-factor issue'), the Utilities companies lobbied the U.S. government. These articulated constraints were treated as 'facts', but Bijker proposes that they could be used within the discourse as both a means of supporting the high-efficiency bulb, or opposing it. Even the experts disagreed with one another over these constraints, and in a U.S. Congress hearing it was admitted that no one really understood the specific issues.

Bijker's notion of interests is congruent to the notion of technology in the anti-essentialist view: interests are temporarily stabilized outcomes of interactions, and the stabilisation partly occurs in the form of artefacts -- so technology is in some form the inscribed interests of a temporary stabilisation (1995, p.266). Technology allows for *interpretive flexibility*. Eventually choices become fixed in artefacts and socio-economic structures, and the original flexibility vanishes once the initial commitments are made (Winner 1986, p.29).

Technology is not always awaiting construction and interpretation, however.

> (S)ome artefacts are more obdurate, harder to get around to change than others. ... Exploring the obduracy of technology offers one way to gain understanding of the role of power in the mutual shaping of technology and science. (Bijker 1995, p.4)

Bijker assumes that by being specific about the details of construction, down to periodic elements and capacities, then obduracy is established. Like anti-essentialism, there is no additional detail about how we may understand how technology refuses interpretation, or becomes obdurate, resisting changes.

There is a level of symmetry within this approach: "the technical is socially constructed, and the social is technically constructed." (Bijker 1995, p.273) However, the interests of the technology, and the related concept of interpretive flexibility, seem to become congealed once the technology is constructed. Once the high-intensity bulb was created, the potential for interpretation died, and the interests of the lamp represented the stabilized outcome of the construction process. This fails the anti-essentialist critique: a technology is more than the congealed interests of its creators or design process because after a technology is 'created', it can still be spoken for, can act, and be translated by other actors.

The social *shaping* of technology approach takes a more 'objective' view of technology, where localized social groups and interests play a vital role in shaping technology (MacKenzie and Wajcman 1999). A valuable case study is how the AR-15 machine gun was refused to U.S. Marines in Vietnam, and how they were rather provided with a *poorer* technology, the M-16 (Fallows 1999). Although an interpretative viewpoint would question a value statement on the relative 'goodness' of a technology, the study concluded that individual Marines agreed that the M-16 was inferior, and this inferiority was later confirmed through Congressional reviews. Technological actors arose through failure: because of the poor choice of gunpowder, bullets were not shot; the M-16 did not work.

From the social shaping of technology perspective, technology appears more obdurate, with less room for interpretation. Social shaping theorists would say that social interests shape the development and adoption of technology, but technology is an object, a black box that is used to construct greater black boxes. A consensus was reached within Congressional reviews and surveys of Marines on the capacity for failure. Perhaps the M-16 was the congealed interests of its developers (and thus did not work), but it was not only the fault of the social actors; it was also because the technological actors resisted alignment with each other (the bullets and the gunpowder).

Agreement by many actors may indicate 'weakness' and the 'strength' of a technology; bearing in mind interpretation, however, we cannot conclude that because there is general agreement then it is a 'fact'. Rather we can reverse the order and state that there are varying interests and views as to the strength and merits of a technology, but there are times that we can see the arising of a 'fact' that the technology may be poor, and this is when various actors agree, or when the technology fails. Again, we must seek out these focal points to see if there is some type of consensus eventually (soldiers can not shoot, Congress agrees). This is not to say that the conclusion of the masses needs to be considered 'the truth'. Rather it only helps to confirm that varying interests are at play, and also confirms that specific moment of controversy and consensus as a *moment of interest*, as it will play a role in future developments.

3.3.3 Technological Momentum

According to Hughes (1994), systems are socio-technological in nature. Often they are born technological, but they grow over time and become larger and involve more and more actors, social and technological. As these systems grow, technological momentum increases.

In his study of the EBASCO power system, Hughes notes,

> As the EBASCO system became larger and more complex, thereby gathering momentum, the system became less shaped by and more the shaper of its environment. By the 1920s the EBASCO system rivaled a large railroad company in its level of capital investment, in its number of customers, and in its influence upon local, state, and federal governments. Hosts of electrical engineers, their professional organisations, and the engineering schools that trained them were committed by economic interests and their special knowledge and skills to the maintenance and growth of the EBASCO system. Countless industries and communities interacted with EBASCO utilities because of shared economic interests. These various human and institutional components added substantial momentum to the EBASCO system. (1994, p.107)

The momentum increased as social institutions were added to the system, but as the system became larger, it shaped the environment, even the engineers.

This momentum can be broken, often involving other forces, sometimes exogenous. In the case of EBASCO, the Great Depression broke its momentum (Hughes 1996, p.108). The Strategic Defense Initiative (Star Wars) became larger as U.S. Congress Representatives latched on to the idea through lobbying for contracts for their constituencies -- the system became so large and the momentum so great that only the demise of the Soviet Union brought the system to a halt (Hughes 1996, p.112), for the moment. The technological system of the petrol-guzzling American automobile required an oil embargo and the rise of petrol prices to turn competitive forces against the Detroit manufacturers, as consumers began purchasing imported compact automobiles. The exogenous forces were not the only persuasive factors however. With the environmentalists persuading the public, the public persuading the politicians, who would enact legislation for anti-pollution technology and gas-mileage standards, engineers and designers within the Detroit manufacturers began to respond with innovations and technical developments (Hughes 1996, p.113).

To synthesise this review so far: in understanding the development and distribution and use of technology in society, we encounter controversy over the role of the technology and the role of the social. Controversies arise in the development stage when we determine the technology at the core of our systems (as with Hughes) or the factors and interests we take in to consideration in deciding the technologies (as in Bijker's high-intensity light bulb), as capacities are debated, and when we question the alignments that exist. In the distribution stage alliances continue to be developed and markets affected, and strategies developed, and yet the technologies continue to be interpreted by different actors, and these controversies of interpretation do provide an interesting point of study. Finally in the use stage, we see the failure of the technological solutions as they react to their development (gunpowder-bullet alignment fails), application (power-factor controversies), or other forces (fuel crises, environmentalism). These very points where controversies arise over the obduracy of

technology from societal influences are also interesting points of study. We can consider searching for these points of controversy, these *moments of interest*, and identifying the surrounding actors with their goals and interests, and following them as they continue to argue and decide the nature of the system, the network, the web, collective, or regulatory regime.

Although we have identified the *moments of interest*, and the importance of the actors, the case has not been made for how non-human actors can shape other actors, i.e. where **A** is non-human, without appearing to be a technological determinist.

3.3.4 Being Determinist for a Moment

Few people today support technological determinism outright; in fact there is little evidence of academic literature to support this view explicitly (Grint and Woolgar 1997, p.14; Winner 1977, p.76). Classic notions of technological determinism involve two prevailing components. First, technology is autonomous as it naturally emerges and propagates itself, i.e. the inventor loses control of the technology (if he or she ever truly had control). Second, technology determines society.

One of the leading academic representations of this perspective is Heilbroner (1967), who argues technology developments are non-random as we can see simultaneous inventions across cultures, and as we are able to predict future inventions somewhat. Even so, we are constrained by the limit of humanity's knowledge, the material competency of the age, and labour and capital limitations (Heilbroner 1967).

With respect to technology policy, Heilbroner argues that

> (t)he course of technological advance is responsible to social direction: Whether technology advances (...) depends in part on the rewards, inducements, and incentives offered by society. In this way the direction of technological advance is partially the result of social policy. (...) An advance in technology not only must be congruent with the surrounding technology but must also be compatible with the existing economic and other institutions of society. (1967)

This bears a remarkable resemblance to social constructivism except that it is in fact more socio-technological because it also relies on the congruency with surrounding technology.

In revisiting his 1967 article, Heilbroner (1994) re-frames technological determinism as

> a framework of explication that ties together the background forces of our civilization, in which technology looms as an immense presence, with the foreground problem of the continuously evolving social order in which we live.

Heilbroner misses the opportunity to bring both the technological and the social to the foreground; if we believe Latour's point that social order consists of social and technological actors.

Pitt (1987) softens the determinist approach, arguing that the notion of autonomous technology is a simplistic account of unintended uses and consequences: no one can foresee all the consequences of any act. It is also trivial, Pitt continues, to consider autonomy as the moment that the technology is made available and the inventor loses control of his invention; this is arguably true of all aspects of our society (Jones 1999). Even if we assume that the interests of the creator are embedded within a technology, the unforeseen consequences and unintended uses, by definition, involve uses and consequences that the inventor had not intended; unless the inventor is omnipotent and foresaw all applications and consequences. A follow-up assumption is that the technology can be shaped once beyond the grasps of the creator; but even as the technology is shaped by others, the shapers can not account for all of the possible applications, uses, and further developments on the technology.

Technological determinism is then fragmented by Bimber (1994). Bimber offers three distinct types of deterministic-accounts: Normative accounts (claims that technology is an important influence on history only where societies attach meaning to it), Nomological accounts (positive descriptions of an inevitable technological order based on laws of nature rather than norms), and Unintended Consequences accounts. Bimber states that true technological determinism is where the laws of nature determine the technology that determines society. Anything else is not technological determinism.

The worry over technological determinism can thus be put to rest. The greater danger is that we over-socialize the technological by ignoring it and placing it at the mercy of the creator by ignoring how it can be used and shaped in ways that are unintended to the creator. This is in line with the anti-essentialist viewpoint, surprisingly. Anti-essentialists claim that the social must interpret the technological; the unintended consequences accounts claim that the technological is interpreted by the social in ways that are unforeseen by the creator. The difference in the two is that the former view mentions that some interpretations are not possible; the latter argues that the technology is an object in its own right.

We still do not have an understanding of what kind of object it is, nor what kinds of interpretations are not possible.

3.4 Articulations, Translations, and Symmetrical Actors

Anti-essentialists believe that researchers must listen to the social interpretations of the technological; the technological actor does not speak. Social constructivists argue that we must open the discourse and look at the granular details of the construction of the technological to see that it is a social and technological construction. Those who support the social shaping approach say that social actors may affect the construction of the technological; although the technological actor may also refuse to work. Technological momentum notices that systems may radically change due to social and technological shifts in the environment. Finally, technological determinism proposes that the social may be determined either by nomological properties of the technological; the social attributing meanings to the technological and then being determined; or the technological always being used and seen in different ways by the social. We may gather any, and all of these approaches from the discourse. As a result, we may regard the technological in any of these of ways.

We can now accept the inclusion of the technological in the foreground of analysis alongside the social without fears of determinism; in fact we can do so to prevent it. Now the challenge is to identify a means of capturing the technological within a discourse.

Winner (1986, p.20) and Latour (2000) both question the idea of anti-essentialism, regarding it as the comfort of the social scientists, and allowing social scientists to treat technology as they have treated welfare policy (Winner 1986) or even God (Latour 2000). Latour (2000) challenges the social explanation of the technical. If the social explanation of the technological succeeds, it replaces an object in nature by another that is represented by forces and powers in society behind it. The social scientists have destroyed the object: giving a social explanation of any object is tantamount to limiting oneself to what is not objective, but only social. Latour concludes that

> a general feature of all objects (...) is that they are so specific that they can not be replaced by something else for which they are suppose to be a stand-in. (2000)

The *social* consists of the objects, the artefacts, and you therefore can not replace the artefacts with a social explanation. The *social* is more appropriately considered as a heterogeneous collection of translated entities; and Latour argues that the artefacts have the capacity to construct this *social* (Latour 1991). This is a fine, but key point, with a link to Grint and Woolgar (1997): where they argue against ever assuming a technology exists without society and is somehow objective; Latour argues that technology is not just a

reflection of society because this infers there is a society that exists without the technology. The artefacts do not reflect society because society is made up of this 'stuff' (Latour 1999); and worse yet, society is not stable enough to project itself into an object (Latour 1999, p.179).

A technological actor will always have unintended consequences and applications. If we remove the human actors, we are left with an object; and this leaves us with technological determinism. If we remove the technological actor we are left with a social deterministic case. So long as we have social and technological actors properly solicited in the discourse, determinism can not prevail.

3.4.1 Technological Translations and Interests

We still have not resolved the situation of how interests and intentionality (or goals) of a technological actor are solicited and understood; we only know that they are not *determined* by social actors. As there are limits to what human actors can do to a non-human, considering the points at which the technology refuses to be interpreted, i.e. where interpretive flexibility fails, allows us to harden the nature of the technological actor. Even the anti-essentialists agree that there is a point where some technologies can not be interpreted widely.

As a result, with unintended consequences accounts we consider the actors $\mathbf{A_1}$, $\mathbf{A_2}$,..., $\mathbf{A_n}$, who shape and try to translate actor **B** we have to consider situations where the technological actor **B** refuses to be shaped into a new actor, or such a translation gives rise to a new actor $\mathbf{B'}$ that no longer meets the goals intended by any of the actors $\mathbf{A_1}$, $\mathbf{A_2}$,..., $\mathbf{A_n}$, effectively rendering the technological actor useless to any of the human actors' intended goals. This gives rise to an interesting situation, however; if actor **B** refuses to be translated, this may cause actors $\mathbf{A_1}$, $\mathbf{A_2}$,..., $\mathbf{A_n}$ to reconsider their own strategies. In effect, **B** ends up translating the interests and actions of $\mathbf{A_1}$, $\mathbf{A_2}$,..., $\mathbf{A_n}$. **B** translates $\mathbf{A_n}$, but **B** is a technological actor. Or in our old notation, **A** can translate **B** where **A** is a non-human actor and **B** is human by forcing a change of strategies or alignments.

3.4.2 Translations and Articulations

Endowing the technological actor with interests as a result of this obstructionist approach remains problematic, however. Falling back upon a nomological approach for cryptography is not an option. Beyond the quotation from Turing that started this chapter, the field of cryptography does not necessarily invoke physical laws, like the sciences. Cryptography is

based on mathematical principles, shaped by computational feasibilities, practices and norms.

Perhaps science is not too different, however. Latour (1999) argues that science, as a practice, is not based on laws either; rather it is a discourse based on *articulations*. Articulations become reduced as time goes on; Latour (1999) shows how a statement about "Joliot's concept of neutrons" will be reduced as time goes on to be just about "neutrons" and a purely *scientific* statement:

> A little later, this sentence, without a trace of qualification without author, without judgment, without polemics or controversies, without even any allusion to the experimental mechanism that made it possible, will enter into a state of even greater certainty. Atomic physicists will not even speak of it, will even stop writing it -- except in an introductory course or a popular article -- so obvious will it have become. (1999, p. 94)

What once required a number of alignments to be accepted, the neutron now stands on its own in the discourse. Therefore, nomological accounts and other accounts are in many ways the same, or at least in the sense that they are both made of the same 'stuff' in discourse: *facts* and *laws*.

Articulations need not necessarily be based on laws of physics or thermodynamics; and we can again look at the controversies to assess these points. In cryptography, there are practices and norms of the discipline and agreed goals and aims, that when practiced and agreed upon by many actors with different or similar interests who create and shape the technological actor, their norms and practices are also considered articulations. This is how cryptographic algorithms gain prominence, and applications become trusted.

A key point of the translation process is when the articulations change; when Joliot's consideration of research into the chain reaction began to mean 'looking out for Nazi spies' (Latour 1999, p.87); or more contemporarily, 'trust in e-commerce' begins to mean large prime numbers. This alteration of vocabulary is considered the *translation* of political terms into technical terms, and vice versa; and eventually we aim for alignment or some other type of resolution of these articulations. Therefore, the point that a 'political'/'social' expression becomes translated into a 'technological' statement is another interesting point of study, another moment of interest, as this tends to be an indicator of a point where the actors may begin discussion on the technological actors. This also indicates that the division of the social and the technological is artificial, and the points where we reduce the division are moments of interest (Latour 1999, p.206).

Although we have resolved that the interests may not be embedded by the creators, and that the technological actor can translate, this does not yet declare how technological actors act in their interests, however. Latour (1998) states that such a determination of a technology is not about what it is designed to do. Rather, we should look at the changing of properties with humans; "technical artefacts never simply transport a function, or play a role, they always modify our intentions, our roles, our interests." (Latour 1998)

3.4.3 On Discourse and Articulations

Similarly design constraints are merely articulations within a discourse. We must interrogate these articulations, possibly through intentionally incorporating opposing views (Sørensen and others 2001). This is not to say that the technological is merely social; rather once we have interrogated a negotiated settlement of *facts* and *laws*, we may have a situation where anti-essentialism leads to a form of objectivity. In effect, the technology hardens, and becomes more obdurate to interpretations. Divergent interpretations may always exist, however.

To understand the technological actors, therefore, we may listen to the articulations of others. Latour (1999, p.179) notes that there may be moments where the technology can in fact 'speak' for 'itself'. Latour recommends that we amass interpretations to see how actors agree about one another (what I call Latourian triangulation); anti-essentialists say that we should amass interpretations to see how interpretations differ (what I call anti-essentialist triangulation). Either moment is when our understanding of the technological may emerge.

Something may also be learned about the social in this process of articulating the technological. That is, as social actors speak on the technological actors, we learn something about the social actors' interests and strategies. Pouloudi and Whitley (2000) found that when the other actors spoke for the technological actor, the various human actors would seek to legitimize their view of the technological by undermining those of the alternative representatives. The articulations of the human actors are political acts, often, and political motivations may emerge.

We can learn from what actors say of themselves and what other actors are mobilised by using their statements. "Indeed, all statements have a reality, and this reality can be evaluated precisely by comparing, each time, what an actor says about another actor with what this actor says about itself." (Latour 1991, p.128)

We may also appeal to the epistemic community (Haas 1992), the community of specialists and experts, for their articulations (and even from within, they vary, e.g. Cypherpunks and

Denning). We may compare and contrast their articulations to the articulations of other actors. How each speaks on the technological in the least adds to our understandings of their interests; at best leads to a further understanding of the technological actor.

3.4.4 On Objections

A non-human does not immediately have something to say about itself, however. We may fall back upon articulations instead. These articulations, given by social actors are important to collect and analyse, but the technological actors are not just proxies, representing what is said about them; they are still objects, or at least have the ability to *object* to what is said about or done to them.

Rather than the common usage, Latour (2000) defines *objectivity* as the "presence of objects which have been rendered 'able' to object to what is told about them." This *recalcitrance* is a natural state for objects, as "the last thing that one scientist will say about them is that they are fully masterable." (Latour 2000) In fact they resist our attempts to control, unlike the human actors:

> Contrary to microbes and electrons who never abandon their capacity to object since they are not easily influenced by the interest of experiments, too remote from their own conatus (not to say interest), humans are so easily subjected to influence that they play the role of an idiotic object perfectly well, as soon as white coats ask them to sacrifice their recalcitrance in the name of higher scientific goals (...). (Latour 2000)

Humans can be mastered, but perhaps technologies are more reluctant; we can embed our interests into people, but not so easily into technologies. When we see these capacities of the technological, through objections, the anti-essentialist interpretive limit is reached: non-humans object to interpretations and alignments (an exploded laboratory is exploded (Latour 2000), a gun that we thought would work but that doesn't work (Fallows 1999)). Obduracy can be found, but it may require some pushing and prodding. This pushing and prodding may arise from the discourse naturally, or may require some intervention.

3.5 The Technological Actor and Moments of Interest

So we approach a situation where the technological actor is hardening. Determinism of any form has been abandoned, *moments of interest* have been recommended. The technological actor, in fact all actors, *may* resist interpretation, construction, and shaping. This actor can also object to being spoken for, and can object to being translated. These are all among the moments of interest within a discourse: points of interest to research and analyze in the formation of an understanding of the context and the actors (see table 3.1).

Issues from the literature on society and technology	Possible moments of interest for capture
Anti-essentialist view that technology is contingent, shaped and interpreted by humans.	Search for times of controversy, and look for varying interpretations of capacities. Interrogate notions of capacities, but there will be times when actors agree. When they disagree, each interpretation may say something about the actors.
Social constructivist view that there is always a discourse around a technology and its construction; open the black box.	Follow the actors and the discourse; notice the change in the actors, who gets included, who does not. Note when actors speak in detail regarding the technology, i.e. collect articulations.
Open the black box, and be specific on the technology to see how humans and non-humans 'make society durable', or how they fail. Politics of social affect the technological, e.g. M-16.	Be specific. Monitor discourse for articulations on capacities and how these become accepted, or refused. Analyze the content of the articulations, compare and contrast to identify sources of strain in the social. Watch how each technological actor works with others, and which social actors are involved.
The study of the process of alignment of heterogeneous actors. Successful and unsuccessful alignments, objections, and articulation-comparisons.	Monitor modifications over time of how goals change and unplanned uses and adapting to new environments. How do others speak of or use the technology, and how does the technology react? Document analysis of technological design, and monitoring of use and changes/adaptation. Collect statements of intentionalities and shifts in goals; including those of the epistemic community and their practices.
Stability is only contingent and temporary. Unintended consequences and uses, new conditions of use. Technologies can object to other technologies (bullets and gunpowder), but exogenous forces may also play a role, whether social or technological.	Monitor for changes introduced by other technological actors (that may be mediated by humans). Monitor for conditions where the technological objects to new uses, changes, or replacement. Identify the endogenous or exogenous factors that lead to recalcitrance or to alternative strategies.

Table 3.1 Summary of Moments of Interest

Later chapters will discuss cryptographic policy discourses in detail; and a number of actors, humans and non-humans, will emerge, alongside interests, mechanisms, and principles. In the process of capturing and representing a discourse, volumes of data can be compiled. Placing both the technological and the social in the foreground can lead to an unbearable amount of data (Walsham 1997). Specific points of interest need to be identified that are important for collection and analysis. Rather than looking only for capacities and intentions, we must monitor translations, interrogate interests and actions, particularly objection (Latour 2000), resistance to interpretation (Grint and Woolgar 1997, p.10), or obduracy (Bijker 1995, p.4).

The proposed moments of interest are among key points in the interaction between actors. The discourses tend to be centred on controversy or change (Bijker and Pinch 1987, p.27). Black boxes are opened and actors speak of one another, and actions occur, and objections arise. These statements by actors must be interrogated, regardless of the actors are social or technological.

Times of agreement and disagreement are among key moments. When actors agree and 'facts' arise, we can consider this *Latourian triangulation*. Examples include actors agreeing on one another, speaking similarly, perceiving interests similarly. When actors disagree, this is an *anti-essentialist triangulation*; varying perceptions of one another, differing statements and interests emerge, where we can learn more about the perceptions, interests, and actors accordingly.

From the point of view of the technological actor particularly, but may be generalised to all actors (Sørensen and others 2001), indications of recalcitrance are also moments of interest. This is when existing policies fail, the laboratory blows up (Latour 2000), computers break down, weaknesses in implementations exposed, and the actors resist consensual interpretation. This may lead us to question and investigate the actors who dominate other actors, who attempt to control the outcome of the process and act as key passage points (Callon 1986). These actors with the power may speak authoritatively, simplify articulations, speak of capacities (Grint and Woolgar 1997, p.33) and facts (Latour 2000).

The greatest benefit of this approach is that we can incorporate all accounts into such a framework; if people speak in deterministic ways or using constructivist terminology, we can incorporate their accounts as they try to give form to the social and the technological. If people ignore the technological, we may find it. If technological accounts ignore the social, we may identify it. After all, these moments of interest are the points of greatest contingency, controversy, disinterest, and conflict for not only the technological, but the social as well.

Some of the practical ideas concerning the technological actor, the human actors, and the network need to be tested, and Section II of this dissertation will apply these ideas within the cryptography policy discourses. Now that the moments of the discourses have been identified for capture, the next chapter will discuss the methodology used to study the discourses.

Chapter 4: A Methodology for Actors and Moments

> If a person were to try stripping the disguises from actors while they play a scene upon the stage, showing to the audience their real looks and the faces they were born with, would not such a one spoil the whole play? And would not the spectators think he deserved to be driven out of the theatre with brickbats, as a drunken disturber? (…) Now what else is the whole life of mortal but a sort of comedy, in which the various actors, disguised by various costumes and masks, walk on and play each one his part, until the manager waves them off the stage? Moreover, this manager frequently bids the same actor "Go back in a different costume", so that he who has but lately played the King in scarlet now acts the flunky in thatched clothes. Thus all things are presented by shadows.
>
> -- Erasmus, The Praise of Folly

Abstract

Section I outlined the research approach for this socio-technological study of technology policy discourse. This chapter describes the process through which I observed, recorded, and analysed cryptography policy discourses. Building on the *moments of interest*, the importance of understanding the context of the actors and their action will be outlined, as supported by epistemologies and methodologies from Information Systems research. Capturing and representing discourse remains challenging for a number of reasons, including the need to represent and interrogate technological actors. I will present the research process used to support my research argument: a set of qualitative intrinsic case studies incorporating interpretations from various actors, through the use of multiple methods of data collection.

4.0 Introduction and Summary

A cryptography policy discourse may involve many actors, some social and some technological, pursuing various programmes of action, with varying interests and goals. This chapter will present the epistemology and methodology for collecting data from, and means of representing, each discourse presented in chapters 5 and 6.

The previous section of this dissertation noted that both the Regulation literature and the Information Systems literature poorly reflected technology; and thus both domains are lacking in experience in collecting data of a socio-technological nature from discourse. Although an ontology emerged in both literature reviews of actors, both social and technological, interests, goals, and articulations; discussion of epistemology and methodology merits some consideration.

The discourse may naturally arise, but may require intervention of the researcher. Collecting socio-technological data from the discourse is no different. In my research I force a holistic

approach where I sometimes insert the technology into the foreground of data collection and representation to understand from a socio-technological perspective the challenges in establishing technology policy. I aim to understand how the social and the technological interact and enact realities (Orlikowski and Baroudi 1991), from the lowest levels of detail, e.g. cryptographic key sizes, up to the institutional transformations, e.g. national security (Latour 1991, p.124). This interpretive research is an attempt to understand socio-technological processes, and as a result I must try to get inside the world of the actors, with the intention "of understanding actors' views of their social world and their role in it" (Orlikowski and Baroudi 1991).

There are ways of researching and presenting discourse using positivist and critical research processes, as others have tried. Cryptography policy was one of the most contested technology debates in the 1990s, alongside copyright and free speech (in fact, in many ways cryptography policy envelopes both). Cryptography policy has been presented by others from the perspectives of politics, philosophy, criminology (Crowell 1997), technology (May 1994) and perseverance of technologists (Levy 2000), oppression and surveillance (Diffie and Landau 1998), fiction (Stephenson 1999), and pornography (as reported in Sullivan 1999), to name a few. The stories of cryptography policy can therefore be told in many ways. While trying to maintain a reasonable scope, an appropriate research perspective would try to incorporate, or listen to, the variety of interpretations that may emerge.

Drawing from Denzin and Lincoln's conceptualisation of the 'Research Process' (Denzin and Lincoln 1998, p.24), I will outline my own process within their five phases. These include the role of the researcher, theoretical paradigms and perspectives, research strategies, methods of collection and analysis, and the art of interpretation and representation.

The motivating goal to this research was to learn more about cryptography policy because I felt a compelling need to better understand the issues involved. There were no intentional research designs, or expected outcomes (Zmud 1999, p.23). Instead I was caught within a time when regulatory acts were being pursued; real events were occurring as policy regimes were transforming. My sense-making process was extensive, and took many years through many means of interaction; this immersion and resulting hermeneutic is explained in §4.1.

A consequence of this research approach is that both my understanding of the phenomenon and the eventual theoretical developments transformed in the process of this research. In a sense, my research approach aims for an 'understanding' of what happened through gaining an understanding of the perspectives, strategies, feasibilities, and capacities

(Braa and Vidgen 1999). This understanding is based on interpretations by the actors, and my own, in an attempt to capture the complexity of the issue, not to reduce it (Checkland 1981, p.245). A lengthy amount of time 'in the field' involved being subjected to many influences, observing many events and transformations, as I became immersed, trying to make sense of the events. This sense-making process is described in §4.2.

That is not to say that the research approach is *ad-hoc*. Aiming intentionally for a holistic analysis reflected my choices of data collection: pluralist (collecting competing interests and realities according to the actors), historical (seeing the evolution of ideas and action over a period of time), contextual (watching as many of the relationships between actors at different levels of analysis) (Pettigrew 1990, p.277). These did not just *emerge* from the data as I acted passively -- they required the act of research, sometimes as an academic-observer, sometimes *investigative* (e.g. to find relationships). The decision on the scope of the research approach is discussed in §4.3.

This approach also permitted the use of multiple methods (Mingers 2001b). These methods come from the interpretivist research traditions of ethnography, action research, and grounded theory coding. These will be reviewed in §4.4.

Finally, the presentation and analysis of the research results will be discussed in §4.5. Upon reaching an understanding of cryptography policy and the theories on technology and society, presenting these 'findings' again involved intentional intervention. I did not only 'let the data speak for itself', as this would have amounted to a simple chronological discussion of policy regimes. Rather the socio-technological approach called for interventions and specific presentations of *moments of interest* such as articulations, constructions, and the evolution of language.

4.1 The Researcher as a Multicultural Subject

Deciding on a research process within a politically charged topic is challenging. The amount of data and the disparate interests of actors are among the methodological challenges. A related challenge is discerning the role of the researcher, particularly whether the researcher is distant with regards to the actors and the data, or has a level of intimacy and interest in the issue. According to Denzin and Lincoln,

> the age of value-free inquiry for the human disciplines is over, and researchers now struggle to develop situational and transsituational ethics that apply to any given research act. (Denzin and Lincoln 1998, p.25)

Positivists require the researcher to play a passive neutral role so not to bias the results; below I will explain how I was neither passive nor neutral. I also note that my active and non-neutral role added to my hermeneutic understanding of the topic.

My interactions with the policy discourses were extensive. Prior to beginning my PhD-candidacy I was already interested in the discourse in the U.S., having written an undergraduate paper on the U.S. policy in 1994. In 1997, with some colleagues at the LSE and with a non-governmental organisation (NGO), Privacy International, we organised a conference on cryptography policy, *Scrambling for Safety*, to discuss policy developments in the United Kingdom. Through this conference I was able to develop relationships with NGOs and other conference attendees because of our shared interests. I also began to use cryptographic applications more frequently, sending encrypted messages between my new colleagues. I also submitted a response to a UK consultation process, also submitted as an MSc-level essay.

Even at that time I had not yet made up my mind regarding the validity of the claims of the U.S. and the UK governments regarding the dangers of cryptography -- in fact I was leaning more towards the pro-regulatory side of the debate; an opinion that I shared with some colleagues. The response was not as harsh as I had expected, but it is an important event in the story of this research: I did not begin this research with the assumption that I was going to show the faults in the understanding of my new colleagues. Nor did I begin this research by labelling the regulatory approach as invalid. I did realise, however, that I needed to develop a more thorough understanding of the contested issues.

A number of developments led to a deeper appreciation of the discourse. Through teaching at the LSE I felt the pressure to become authoritatively knowledgeable on the discourse, or at least enough to present to an audience of MSc students. Interactions with the NGO community led to interactions with the epistemic community of cryptographers and security experts, particularly as the two communities worked closely on a number of projects and positions. Again I felt the pressure to become more knowledgeable regarding the discourse, and the specific technology, if only to *hold my own* in conversation.

The interaction with these communities also led to greater access. I was included in more discussions, invited to conferences, given primary and secondary information, and given access to non-public on-line fora. Thousands of e-mail communications received and sent over the years were a result of this access.

Through the Foundation for Information Policy Research, Privacy International, the LSE, and a number of colleagues that I met over the years, I established a network of contacts. I

also interacted with government officials from a number of countries. The majority of these actors were aware of my status as a PhD research student (to my dismay at times).

As much as this affected our relationships in a number of ways, the interaction contributed positively to my research in two ways. First, through peer pressure and pressure of responsibilities, I had to learn a great deal in a short period of time regarding cryptography policy. Second, I had 'privileged seating'. When a new policy development occurred and was analysed by one of my colleagues, I was notified shortly thereafter. I was able to understand the contentious aspects of a policy, or a problem with a technology, through monitoring and participating in informal discussions. I was informed of places to look for more information and other actors to approach.

This testimony is describing, in effect, a hermeneutic process of my development of an understanding. Hermeneutics is the science of interpretation, and is concerned with the analysis of the meaning of a *text-analogue*, and the process of sense-making (Myers 1997, p.280). This gives rise to the idea of a hermeneutic circle -- a dialectic between understanding of a text as a whole and interpretation of its parts. When Myers applies this notion of a *text-as-an-organisation*, he argues that the

> more information we gather, the more we understand the organization as a whole and its constituent parts. This hermeneutic process continues until the apparent absurdities, contradictions and oppositions in the organization no longer appear strange, but make sense. (Myers 1997, p.281)

The more I discussed, lectured, wrote, and observed, my understanding grew. The interaction with the actors and the discourse added to this process. According the Boland,

> in the world we encounter a text of meanings already made and being made. All around us, mutually validated ways of seeing the world are being actualized through multiple language games. ... When a phenomenologist studies a person, she does not look at them, but with them in a dialogue searching for understanding. Understanding comes step by step, layer by layer as preconceptions, prejudices, and assumptions are recognized and seen through. (Boland 1985, p.195)

However, Myers does not see the prejudices as problematic in modern hermeneutics; rather I must become more aware of my 'historicality' (Myers 1997, p.282). In attempting to explain my development of an understanding, I had to become aware of the nature of this education and my role in the domain. Through this I can begin to understand the prejudices that I have developed.

It is fair to say that my understanding may be based more on my interaction with 'opponents' of the government policy; and one may assume that this leads to a biased

understanding. I actively solicited statements from supporters of the various government policies. Through discussion documents, consultation papers, testimonies and policy statements I was also able to provide a voice for their points of view. To generate the best understanding, I felt it necessary to incorporate as much 'data' as possible, particularly in accordance with the Latourian and anti-essentialist triangulatory methods, discussed in more detail below.

4.2 Theoretical Paradigms and Perspectives

My ontology for the purpose of this research is that the world is full of actors, social and technological; and activity may be purposeful to these actors, and may have meaning to them (Checkland 2000, p.s14-15). Reality is constructed by these actors, but this reality consists of interpretations (Denzin and Lincoln 1998, p.26). Trying to understand and express these interpretations involves interpreting the meaning of the actions, interests, and understandings of these actors and how they all interact (Checkland 1981, p.247).

This view of the world and of knowledge in this world is consistent with my mode of research, according to Checkland (2000, p.s39). First, it is situation-driven as opposed to methodology-driven. Second, it is interaction-oriented, as my understanding is supported by interactions with the people in the world.

My research process is derived from an interaction between theory and data. As the two developed, it became apparent that I would have to *create* a holistic story (Stake 1998, p.91) where perhaps there was not one before. While I could follow a technological or socially deterministic account, as many of the actors see the world, I chose to see the world as being socio-technological. This approach requires, however, adding this holistic socio-technological approach to the story while other researchers and actors do not necessarily see it in this way.

For a number of reasons, I can not solicit 'the truth', nor can I speak authoritatively on the issue of cryptography policy. One reason is the nature of the actors and interests: national security interests tend to be relatively opaque, and trying to explicate these interests is challenging. Another reason is based on the role of the researcher: it is arrogant to believe that in an interview an actor will tell me his understanding or a secret that has not been spoken before, particularly on an issue that affects trust, law enforcement, national security, and commerce. As a result, the stories told in this dissertation are not authoritative. Rather they are based on my understanding that has gone through iterations and credibility checks

to reduce the number of absurdities to a point where the story becomes viable for the purpose of analysis.

Lee (1991) provides another way of looking at the process of 'understanding' that involves some positivistic traits. Lee argues that there are a number of levels of understanding that occur within a research exercise, involving both interpretivism and positivism (p.351). The first level occurs as the observed subjects, the people and the technologies, establish the everyday common sense and meanings with which the 'subjects' see themselves, and in turn act. This is the world of action and speech. The second level of understanding involves the researcher's interpretation of the first level, and involves subjective interpretation and the hermeneutic circle. The third level of understanding is where the researcher creates and tests his understanding in order to explain the empirical reality that he is investigating, and is made up of constructs that belong exclusively to the researcher. At this level the researcher does not consider people, but rather 'puppets' (p.352). These puppets are endowed by the researcher with internally held values, opportunities, goals, and capacities. The researcher also specifies actions with which the puppets, given their internally held values, may respond to.

Lee's framework of understanding is useful for explaining the co-evolution of my data collection and theory development. The first phase involved watching and listening to the interpretive understanding of the actors involved in cryptography-policy -- who they are, and what things mean to them, and what they say are their interests. This early understanding led me to believe that the problem of study involved actors and interests, and this could be studied from the perspective of economics and regulation, focussing on the relationships between government, technology, and the market. This understanding also involved, separately, an understanding of the technological issues, but I could not sufficiently explain the role of the algorithms and the keys, nor sufficiently embrace the voices speaking on recalcitrance and risks. As I communicated further with the actors, followed more developments, and interacted with the discourse, the 'puppets' I had drawn of governments with law enforcement agendas, industry with market interests, and NGO-advocates as a united set of interests, no longer made sense to the actors in further discussions (Lee 1991, p.353). My understanding needed greater sophistication on all levels.

Neither the availability of policy-supporting products, i.e. key recovery software, nor recalcitrant technologies appeared to affect the views of 'success' of a given government policy. Simultaneously, subsidies and other economic incentives did not appear to be pushing the market in a deterministic direction. To resolve this conflict I looked deeper into

the arguments surrounding technology and society, as arose within the theory discussion in chapter 3.

Looking again at the actors, as the debates and policies evolved, I learned that there were many more actors, multiple interests, with multiple dimensions of action. I began to look at the larger picture of 'discourse' rather than a 'debate' between opposing sides, to see how technologies were being constructed and how they were translating. Issues such as e commerce, globalisation, and trust that I previously regarded merely as simple economic interests were included into the expanded notion of discourse. The data then began to make more sense, and the actions that followed in the 'field' could be better explained. I applied this line of thought to some of my other work on different technology policy processes (e.g. Hosein 2001) and it occurred to me that it was a reasonable way of viewing the issue of technology policy. At this point I felt comfortable enough with my understanding of the issues: my positivistic understanding based on the interpretive understanding derived on a reading of the subjective understanding held by the actors (Lee 1991, p.357).

4.3 Research Strategies

My field studies may qualify as intrinsic *case studies* (Stake 1998, p.88), the ideal settings for understanding human interpretations and meanings (Walsham 1995, p.74). The two policy processes are not strict 'cases'; Stake states that a case is specific, and is a 'bounded system'. Rather I am investigating what Checkland (1981, p.279) refers to as 'a situation' in which various actors perceive various aspects of the situation to be problematic. Rather than referring to a 'case', I use the term *discourse* as the field studies researched negotiations and other interactions within these situations.

The discourses of study follow not only the establishment of policy; as that would fail to acknowledge the role of the technological, and would also require looking at theories of criminology and crime control, issues of national security, signals intelligence, and economic theories of laissez-faire. Nor is it a discourse on the negotiation of interests in developing a set of technologies; I did not interview a number of cryptographers to understand their interests. The 'situation' that I am trying to understand is the evolution of the interaction between technology and policy, the interests and actors, some of the results and implications.

Establishing the scope of actors to be studied is non-trivial. The social constructivist approach of 'following the actors' with a 'rolling snowball' is one method (Bijker 1995,

p.95). This approach would let the discourse decide or announce the actors. A limitation of this scope is that those who initiate the discourse often decide the actors, through 'consultation'. Consultation processes may exist only around the regime-makers: governments set the technology policy; they then invite other actors to consult, speak, and advise. Some are then excluded; and these may be the voices of dissent. These voices can still rise and influence the government actors through the political process, or by speaking through those who are allowed to participate in the discussion. This has occurred in both the U.S. and the UK where individuals, NGOs, and industry appealed and spoke through their Congressmen and Lords, and through petitions and the media. These larger discourses, beyond consultations, are the focal units of my study.

The cryptography policy discourses in the U.S. and the United Kingdom were selected for study mostly because of the prevalence of field-based data (Zmud 1999, p.24). The two countries require consultation processes in order to establish policies, and both political systems have an active set of non-government actors and well-established media, both of which are technology-savvy. Language also played a role (Garfield and Watson 1998); where I had planned on looking also at France and Germany, it became easier to manage the load only of the U.S. and the UK.

The U.S. was selected for study as it was the first country to open up the cryptography policy debate to the public. Another reason for selecting the U.S. was that many of the world's software developers are in the U.S. As they are required to abide by U.S. policies, I felt that this would provide an interesting opportunity to see how U.S. technology is developed in accordance, or not, with these policies. Accordingly, for more detailed study I selected the largest software company, Microsoft; one of the first companies to gain export approval with almost full-strength cryptography, Lotus; and a company that specialises in commercial key recovery, Entrust Technologies. I also selected other technologies that were discussed at the time, including SSL and PGP, but did not interview developers.

The United Kingdom was selected because of my earlier activities, and my relationship with the interested actors. Also, the type of policy regime pursued in the United Kingdom was different from the U.S., as the UK discourse centred on regulating services rather than technologies; thus making the situation interesting for potential comparative purposes.

Within each discourse, however, massive amounts of data can be accumulated from a number of actors; the next section describes how the scope of collection was limited further.

4.4 Methods of Collection and Analysis

The number of developments and the amount of attention cryptography received over the years during the policy formation process only served to make the discourses even more difficult to capture and represent. For example, a review of FT-profile by Edgar Whitley in the period of August 1999 to August 2000 resulted in almost 500 articles relating to the Regulation of Investigatory Powers Bill (RIP), a particular piece of encryption policy in the UK.

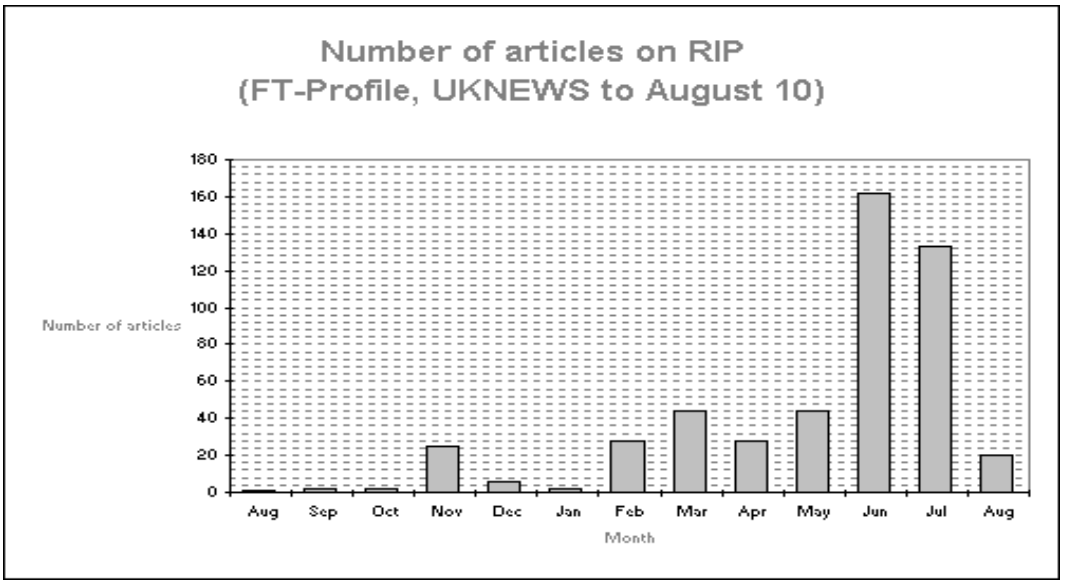

Figure 4.1 RIP News Articles analysis, by Edgar Whitley, 2000, unpublished

FIPR's RIP Information Centre (FIPR 2001) lists over 1000 world-wide news articles from December 1999 through to April 2001. Also consider the public discussion: *ukcrypto*, the public mailing list in the UK for discussion of cryptography policy had over 12,000 posts since 1997 when I subscribed. Articles and postings dealing with cryptography policy in the UK eventually subsided, most notably in the autumn of 2000, however.

By 1997, when cryptography policy was just becoming an issue in the UK, it was already a controversial topic in the U.S. A considerable amount of the U.S. discussions had already taken place; but many of the articles and reports were still available, or archived by NGOs, research centres, and even by interested individuals. Every day I visited archives[1], reviewed a number of media[2] and NGO[3] websites, monitored mailing lists,[4] and kept in regular contact with colleagues. When interesting issues arose, I would track down the documentation and save the files. I solicited as many interpretations as possible. For example, testimonies to the U.S. Congress committees are stored on the Congress servers -- I would collect all of the testimonies that were available in order to get the voices of as

many actors as possible. Eventually, however, the testimonies either stopped appearing (as Congress was no longer considering cryptography policy), or the testimonies became repetitive. This occurred most notably around the autumn of 2000, even though some discussion arose again following the events of September 2001.

To capture the discourses, I used multiple data collection methods, which is common within IS research (Baskerville and Pries-Heje 1999; Galliers 1991), and is argued to be non-problematic by Mingers (2001b), and viewed by Strauss and Corbin (1998, p.178) as inevitable, though some concerns do arise (c.f. Prasad 1997). Mingers (2001a) regards the barriers between methodologies are merely constructs of thought, and argues that we may detach research methods (and perhaps even methodologies) from a paradigm and use them, *critically and knowledgeably*, within a context that makes different assumptions (p.243), such as the presence of non-human actors (p.253).

Considering the research approach described above, and following from Mingers' arguments, I will review what form of methodologies and methods I used in my research to gather data, to observe action, and particularly to study non-human actors. Particularly, I made use of methods from ethnography, action research, and techniques from grounded theory.

4.4.1 As an Ethnographer?

In IS research, ethnography has led to the realization that information systems have a highly complex and constantly changing social context (Myers 1997). Ethnography involves the exploration of the social context in order to improve understanding of human thought and action through interpretation of human actions in context (Harvey and Myers 1995). This includes the investigation of how technology affects social interaction and creates shared meanings (Myers 1997).

In such studies, the observer plays a significant role. The result of an ethnography is a text that illustrates the researcher's interests and not simply a recording of a stream of events (Harvey 1997). A researcher selects from each situation those aspects of interest; affecting the entire research approach. While the interrogation of the capacities of technological actors occurs through focusing on moments of interest, I still select those moments, as I also selected the actors to investigate in detail.

I recognise that I cannot suspend my prejudices (Myers 1997). Ethnography supports enquiries in real world situations, particularly complex social, cultural, and political systems. In so doing, critical ethnographic analysis requires the investigation and interrogation of the

views of the various actors and the conflicts that arise (Harvey and Myers 1995). Prejudices, intimacy with the data, and interrogations may create awkward results. The actors in my research may know me through a number of affiliations, and their reaction to me may be affected by the myriad of ways that we may know each other, or have heard of each other; and they may have responded to this relationship.

Awkward results could have emerged from the interviews in particular. I was able to contact the relevant personnel in Microsoft because Microsoft Research in the UK had agreed to fund my research in part; through this relationship, the company gave me the contact details of those responsible for cryptography policy issues at Microsoft headquarters. Similarly, IBM Research Canada also provided funding resources; and then pointed me to the person responsible for export controls in IBM, who in turn pointed me to the appropriate person in Lotus (an IBM subsidiary). Communications with Entrust Technologies was established rather through *cold-calling* by e-mail that led eventually to the Vice-President; but initial conversations were buoyed by discussion of common acquaintances. Researching the technologies also involved document analysis and other data collection methods, particularly solicited from the epistemic community. Therefore, the interviewees and their responses could have been affected by a number of factors: that I was put in contact with Microsoft in Redmond by the head of Microsoft Research UK (hierarchical, or collegial), or because I was being funded (deontological), or that our discussions occurred from my e-mail account "gus@privacy.org" (political). Likewise, Lotus knew of my contacts with their critics, but also understood that I was an honest broker; but Lotus may have been trying to position itself as a 'good guy' knowing the harsh public responses it received previously. This self-questioning pushed me to consider how I, despite all my prejudices and prejudicing of the data, could try to introduce some form of reliability.

Latour notes that this is a common problem; one cannot easily step out of a situation, context, or data. He recommends the use of triangulation.

> (S)ince there no longer exists any external point of view to which we could ascribe the degree of reality or of success of an innovation, we can only obtain an evaluation by triangulating the many point of views of the actors. It is thus crucial to be able to shift easily from one observer to another. (Latour 1991, p.124)

I used the interviews as a form of triangulation, a verification of my understanding, rather than only as a means to get inside the world of the interviewees. Before the interviews I reviewed as much as I could regarding the technologies (articles, reviews, white papers). I then asked the interviewees to explain to me the nature of their technological solutions to resolve uncertainties and misunderstandings.

This form of triangulation, i.e. Latourian, was particularly important due to the amount of speculation in the field; not everything an actor says about another is necessarily important data, or 'true'. The discourses involve the highest levels of government and national security concerns; accordingly there are many ideas and stories particularly about who was responsible for which policies, what level of interaction there was between governments and industry, and what some technologies actually do. Statements of rumour and conspiracy, like "Blair was rubber-stamping the UK policy all along", or "the U.S. is driving the UK policy for *laundering* purposes", or "Lotus Notes sends mail to the NSA", were not necessarily discounted immediately, but were for the most part investigated. If supporting data or countering-evidence was found then the data considered further.

Triangulation need not lead to consensus, and sometimes leads to controversy. I was sometimes unable to corroborate data or to find differing interpretations. This turned out to be interesting for further study, consistent with the anti-essentialist 'triangulation'. If agreement was found, I noted it; if it was not, it was equally interesting.

In representation of the data, Prasad (1997) recommends that ethnographers try to understand the jargon and terminology of the people under study, and to incorporate this language into the reporting of the research "to convey a flavour of the situation to the readers" (p.107). Speech and articulations are essential to my work, as I believe they capture some of the essence of discourse. Prasad argues that this implies participant observation for lengthy periods of time 'in the site', and sometimes even taking on the roles of inhabitants. That is, "using an ethnographic approach calls for the cultivation of some degree of informal intimacy with the people being studied" (p.108). Accordingly, being seen as an 'inhabitant' of the policy discourse gave me credibility with the actors. This credibility increased in informal settings; over drinks and dinner some of the most interesting ideas, discussions, and references would arise, as Trauth (1997) also discovered with beer and public houses. Some of this 'data' was surely lost, or poorly represented in my research; but I always tried to maintain email communications with these individuals, which in turn increased our iterations of Lee's cycle, to further my understanding of their subjective meanings.

The research is not strictly ethnographic, however. I am more intimate with the 'field' than with its ethnographic subjects; I did not have an 'informant' (Schultze 2000) nor did I have to rely on 'trust' and confidence in order to gain insight. That is, my discussions with the human actors did not involve a solicitation of their subjective meanings in the sense that I was trying to find out the 'truth' they are trying to conceal (Pettigrew 1990, p.277).

Moreover, I was not reporting the work of the human actors alone (Harvey 1997). With regards to the technological actor, ethnography sees technology as systems of meaning, holding multiple meanings for different people. Ethnography becomes inconsistent with my theoretical developments as it views the technology becoming active only when located within a broader cultural system of meaning, when humans attribute symbolic value to its already functional properties (Prasad 1997).

Therefore, my work is slightly ethnographic in that I was intimate with the actors, sometimes on an informal basis; I also looked for the development of shared meanings and articulations. I use similar methods such as discourse-observation (conference presentations, and debates on-line, in the media, in testimonies to Congress and in Hansard); semi-formal interviews (Janson and others 1997; Matenlaers 1997) with Microsoft (5 hours), Lotus (2 hours), Entrust Technologies (4 hours); document collection including reports, testimonies, statements, whitepapers; informal social contact (Myers 1997) with advocates, cryptographers, lawyers, civil servants, industry representatives; with a subordinate use of quantification (Atkinson and Hammersley 1998, p.110).

The essential similarity between my research process and that of ethnography is the evolution of the hermeneutic. Ethnographers approach the culture over time; I was trying to increase my credibility with the actors while also increasing my understanding to work towards a theory that could be reflected back to the actors, the discourse, and academia. Using thick description, providing multiple interpretations, searching for Latourian (agreement) and anti-essentialist (disagreement) triangulations, and weaving the contradictions and complexities into a form that can be analysed (Prasad 1997, p.106), I am able to capture and represent an understanding of the discourse.

4.4.2 As an Action Researcher?

Often there is some confusion between ethnography and action research; in a survey of the literature, Lau (1997) found that a number of cases of action research actually appeared as ethnographic accounts. Action research is a process that depends on the social interaction between observers and those in their surroundings. The main contention of action research is that complex social processes can be studied best by introducing changes into these processes and observing the effects of these changes (Baskerville 1999). As the researcher and the subjects interact, a shared meaning develops, and in some ways the world-view of the researcher approaches that of the subjects.

Relative to the other actors, my interventions were limited. My interventions in the discourses were usually about creating more discourse: organising conferences and speaking

publicly regarding the status of the various proposals. If I spoke as an academic I offered analysis on the regulatory issues; if I spoke as an advocate, I discussed the privacy and human rights implications. These interventions situate my research process beyond the 'boundaries' of action research (Baskerville and Wood-Harper 1998). Although I was involved as a participatory observer, I did not determine the nature of the interventions to a significant extent.

The interventions were not part of some intended and articulated research design. I did not have a methodology prior to entering the problem situation, as required by action research (Braa and Vidgen 1999), mostly because my approach evolved with the theory and the data. Therefore my research process is more 'organic' than 'action and change' in orientation (Baskerville 1999).

The challenge of identifying my research process as action research is quite common; Baskerville and Wood-Harper (1998) recommend that a solution is to separate the data collection technique, participatory observation, from the method, participant observation. Participatory observation, in their eyes, requires asking the question: 'how do they respond to me?' I accept that the actors that I observed necessarily reacted to me due to my interaction with the field, and I have two responses to this challenge. First, the actors, are not the focal units of analysis; I am studying the discourses. As my actions did not affect the discourse notably, the discourse has no notable response to me. Second, my interaction with, or participation within, the discourse gave me further access. This access assisted in the feedback loop of my hermeneutic understanding, and also provided even more data. This wealth of data is the next challenge of my methodology, and will be discussed in the next section.

4.4.3 As a Grounded Theorist and Coder?

The data collection process also incorporated some techniques from grounded theory. Grounded theory involves the gathering of the perspectives of multiple actors, which in turn give rise to analytical interpretations (Strauss and Corbin 1998, p.172), using thick description (p.169). Researchers are interested in patterns of action and interaction between and among these actors; and also in discovering *process*, i.e. "reciprocal changes in patterns of action/interaction and in the relationship with changes of conditions either internal or external to the process itself." (Strauss and Corbin 1998, p.169) The data is collected and then coded for analysis to establish these patterns.

Although grounded theories are normally generated from the data, theory can also be generated through existing theories that are "then elaborated and modified as the incoming

data are meticulously played against them." (Strauss and Corbin 1998, p.159) Such theoretical 'sensitivity' enhances the coding of data; and this sensitivity is also based on research and personal experiences of the researcher (Strauss and Corbin 1998, p.173). As my data and theory interacted in a way similar to Lee's framework on understanding, my 'coding' capabilities also evolved. This can be seen particularly with my file-structure of the documents that I collected.

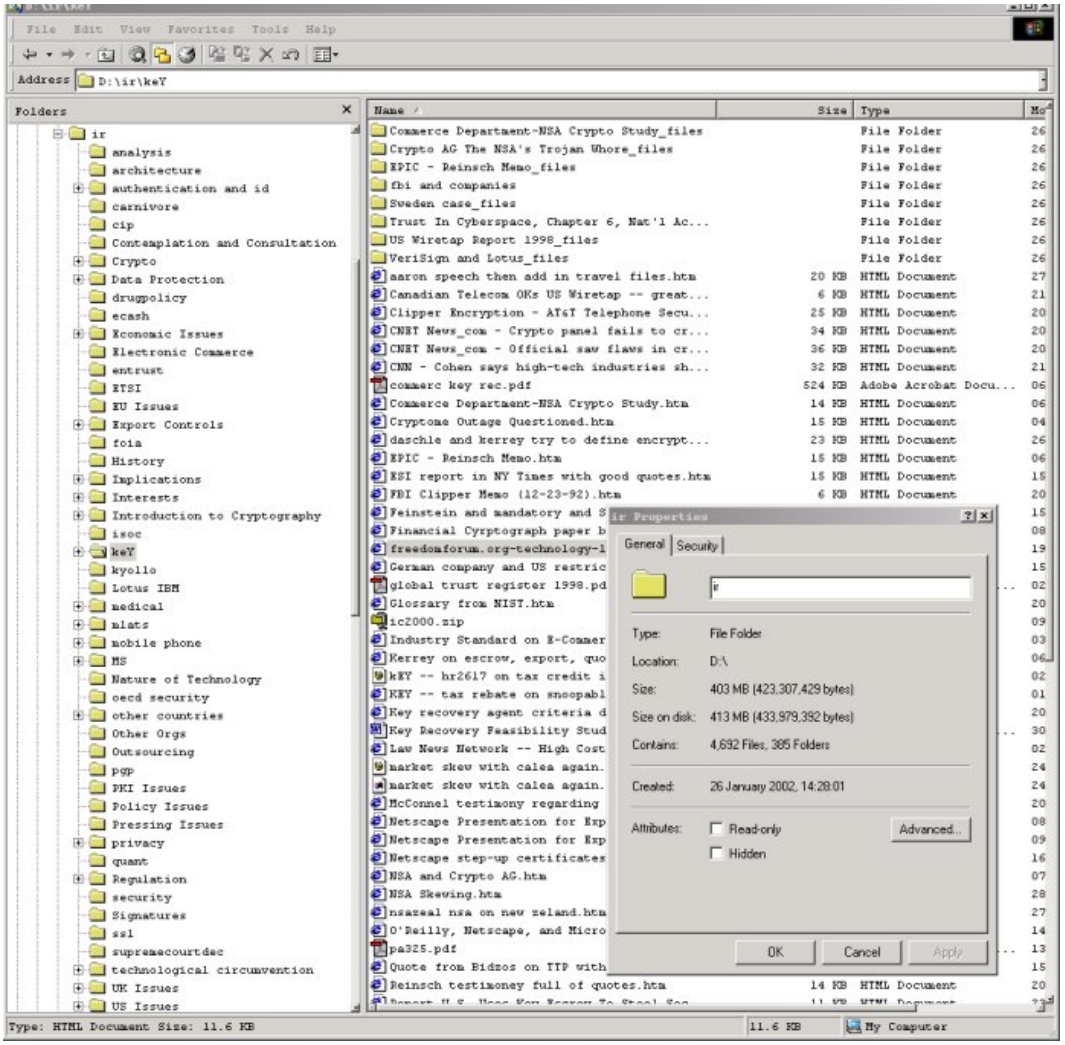

Figure 4.2 File System snapshot as of September 2002

The file system of over 350 folders and 400 MB began with a basic structure that grew more complicated quickly, in parallel with my appreciation for the issues that my theories would have to include. I do not think it is possible to trace back whether it was the folder-names or the theory that came first. The interaction of the two led to the file system, and lead to my theoretical foundations, and suggested ideas for analysis and possible contributions.

This is a deviation from standard practice of grounded theorists, as it is less a substantive coding (a mechanical noting of keywords using a software application), and more theoretical (Strauss and Corbin 1998, p.166) and conceptual classification system of the contents of an article or report and its relevance to my intended description and theory development. My file system of over 4500 reports, articles, consultation documents, and other such files evolved as the data 'arrived'. With links sent by colleagues, found from mailing lists, from my review of the various news sites daily, or upon research to triangulate other findings, by the third year of collecting these files the folder structure stabilised. Upon downloading a file and reviewing its contents the files were classified into the file structure; when I felt that there was something of interest but without a folder, a folder was created. As time went on, the number of new files decreased, and the number of new folders also decreased; while other folders were found to belong in subfolders, and others still were no longer considered relevant. The point of data saturation and boredom with the constant data collection occurred almost simultaneously.

A problem with a conceptual classification system of this relatively flat nature is that in some cases documents would have a number of possible classifications. These files would be saved multiple times in different folders. Often the file names were different, depending on the issue that was being highlighted. For example, the Business Software Alliance, an industry association, released a report, written by security and cryptography experts, on recommended minimal key-lengths. This report was downloaded and saved twice, in *\crypto\minimal_keylengths.pdf* and *\interests\techact\crypto\bsa-final-report.pdf*; the first representing cryptography, the other representing the epistemic community's articulation (in a folder with other articulations). Documents with cross-categorical importance and relevance were saved also in a folder entitled *\keY* (sic), and this folder was repeatedly consulted.

Another deviation from traditional grounded theory encoding was noted by the audience at IFIP 8.2 2001 Conference where Edgar Whitley and I presented a related paper (Whitley and Hosein 2001). We were asked if we used grounded theory methods to analyse the primary source of empirical data in the paper, UK Parliament Hansard. The response from Whitley, was 'no'; rather he indicated that I had read the entire set of Hansard notes surrounding the policy. Having learned and understood some of the contentious issues through my work with FIPR, Privacy International, and my involvement in the BCC report, and in discussions with Whitley regarding some of the more interesting issues, while also considering the state of my theory development at the time of writing that paper; as I read Hansard I carved out the 'interesting' quotations and discussion. This data was then filed into a set of text files, yet another filing system, classified by whether it was speech

regarding industry, the media, the technology (articulations), previous policies, notable quotations (noted by the media, colleagues, etc.), specific amendment language, and specific issues (key revocation, tipping off, burden of proof, etc.). Although I may have missed some notable 'data' in my review due to exhaustion; I cross-checked my findings, in most cases, with the findings of colleagues who attended the debates or who also read the Hansard and had decided to pull out the text that they found most relevant. Our findings overlapped sufficiently; only mine were often more extensive due to my broader academic interests.

4.4.4 Other Methods?

My research approach involved elements of ethnography, without an interest in the culture of the actors; action research, without wishing to intervene only to monitor the effects of my intervention; and grounded theory in order to develop both theory and data collection practices for the purpose of analysis, without using a strict regime of coding and analysis.

Mingers (2001a) notes that there is a level of convergence in these methods. Ethnographers and grounded theorists both tend to use interviews and qualitative content analysis. Ethnography and hermeneutics both involve immersion into language, practices, values, and meaning; hermeneutics and action research can both involve participatory observation.

Many researchers who have conducted similar research also used multiple methods of collection. Garfield and Watson used secondary interview and document analysis in their comparative review of national policies, but did not do any coding as their goal was a 'broad understanding' (1998, p.321).

Trauth (1991; 1997) used multiple methods including interview data, ethnography, and internal and publicly available documentation. She noticed that she became self-conscious while among the actors, yet still valued 'getting close to people'; although she found that she was always working with the subjects.

> (A)s an observer, I can never be totally objective and judgment free. What I can do, however, is attempt to make observations without reading in my own biases and answers. Additionally, I can record my own introspection along with my interview and observational data. In my qualitative studies I accomplish this through journal writing. (...) When I embarked upon the research project, I had not expected my personal journal to be relevant to the research effort. But, then, I also didn't expect to be engaged in my "research" day and night either! (1997, p.242)

I had two such *journals*. One journal was a text file that I codified with categories of data relating to what I believed my structure was at the time, and filled with thoughts,

quotations, relevant links, and conversations that I held on both field- and theory-related issues. The second journal was my e-mail, as much of my interactive work was conducted by electronically. If I needed to remember the date or context of something that was discussed, I only had to search for a specific e-mail within the over 230 MB of e-mails that I have collected.

I only use data that is publicly available or attributable. If it is interview-based I try to triangulate this data. Some of the 'knowledge' that I have developed can not be attributed, however; sometimes the source is unknown or not remembered, or other times it is the product of a lengthy discussion on mailing lists, unattributable to a single individual.

These methods are used to collect as much data surrounding the *moment of interests*. Through this extensive data gathering and the capacity to file and search through this data, and also because I interacted with the discourses, I am able to identify a sufficient amount of these moments, and enrich the descriptions of these moments with sufficient data to tell a story leading to analysis.

4.5 The Art of Interpretation and Presentation

While qualitative studies allow for the amassing of information to construct an interpretation of a situation, devising a way of writing up the data is not easy (Denzin and Lincoln 1998, p.29). Consequently, the presentations of chapters 5 and 6 vary. These chapters are presented in such a way that will bring out the *moments of interests* in each technology policy discourse, while also providing sufficient data for analysis in chapter 7 involving regulation theory. Holism and the *moments of interest* are my intentional research acts, and therefore involve necessarily an intervention to the 'letting the data speak for itself' method of presentation.

Chapter 5 presents a story of the evolution of the U.S. cryptography policy discourse. Rather than providing a chronological representation of the transformation of policies, the data is presented in such a way that highlights the interplay between technology and policy. While specific policy proposals are discussed in detail along with the interpretations according to industry and civil society representatives, the interpretations of the technologies are also presented. While forms of triangulation are used as methods, triangulation is also used as an analytical device, where voices are added that were not necessarily heard at the time in the discourse.

Chapter 6 presents a story of the evolution of the UK discourse. I made more use of consultation documents, responses from a number of companies and organisations and

individuals, and less so of interviews. My interaction and participation in this discourse was greater and so my ability to make sense out of the events was aided, but my bias in data collection is more likely. Much of the data is centred around the consultation responses that I solicited, and is also based significantly on the issues raised by the main opponents of the RIP Bill, being FIPR, Privacy International, some advisors to the House of Lords who were also on *ukcrypto* listserv, and the individuals with whom I worked on the BCC report. The order of presentation reflects more of a chronology of events, although the presence of translations regarding the technology is notable, particularly within Hansard.

4.6 Integrity of this Research

I still need to make the case that this research process has integrity, and qualifies as legitimate interpretive field work (Klein and Myers 1999). Natural questions arise, regarding the credibility, transferability, dependability/validity, and confirmability of the findings (Denzin and Lincoln 1998, p.27).

The credibility (Janesick 1998, p.50) of these stories remains to be assessed by the reader (e.g. too technology focused, or critical social theory oriented). My immersion in the field also aids my credibility, as I advised government, industry, and civil society on issues relating to technology policy over the years; and I believe I maintained the ability to act in all of these capacities by not appearing to support one too strongly over the other, while still being analytical and critical.

The stories and findings have been reviewed by a number of experts in the field. Chapter 5 was reviewed by David Banisar, who worked within civil society throughout the U.S. discourse, and published and edited some of key analyses, e.g. (Banisar and Schneier 1997; EPIC 1994). While he made some recommendations, he made no substantive corrections at the presentation stage. The stories and results of Chapter 6 were similarly discussed with individuals on the FIPR advisory council, particularly in the preparation of two publications (Hosein and Whitley 2002; Whitley and Hosein 2001). This supports the confirmability of the data; as it was confirmed by the actors. Also the majority of the data is publicly accessible or referenced to provide a sufficient audit trail (Morse 1998, p.76), unlike many case studies that rely on internal-documentation and interviews.

The theory development and data analysis have benefited from credibility checks of academic peers. First, the LSE's Short Course on Regulation supported a literature review of regulation. Secondly, similar conclusions that are reached in Section III have been presented in a law and regulation peer-reviewed journal (Hosein 2001), with supportive

comments by the reviewer. Third, a paper co-written with Edgar Whitley was presented at an IFIP conference where we received some comments and feedback regarding methodology. Fourth, another paper co-written with Edgar Whitley (Hosein and Whitley 2002) was reviewed extensively by the Journal of Strategic Information Systems where we went through three iterations of comments and review; when this paper was published, the editors acknowledged that my dual role as a researcher and active participant added to the credibility of the interpretations (Galliers and Jarvenpaa 2002). Finally, I discussed these ideas extensively with my academic colleagues and supervisors within and beyond the LSE.

The research process inevitably excluded and ignored some of the actors and the events. It can be said that this was minimised with my continual interaction with the actors in the field; though this interaction could have increased the errors, or 'bias'. While the data comes from two public discourses, and most of the data is verifiable, the more compelling response to such concerns is that other 'stories' representing the events of these discourses draw similar chronologies and actors. Although some concentrate less on technology, concentrate more on the technologists (e.g. Levy 2000), or on what is hidden from public view (e.g. Bamford 1982), or only on portions of the debate (e.g. Regan 2001), they all contain similar actors and events, or at least as is consistent with their ontologies. I did limit the scope of presentation and intentionally excluded actors and processes (such as the OECD cryptography policy guidelines, developments in other countries) due to time, relevance, and space. This does detract from the study, but I feel that I still provide a fair representation of the events.

Assessing the value of this interpretive work, in accordance with agreed principles (Klein and Myers 1999) can only be left until the final section of this dissertation. While many of these principles have been visited and discussed above such as hermeneutics, the role of the researcher, contextualization, multiple interpretations, dialogical reasoning, and suspicion; the test of validity remains. Validity will be assessed particularly in chapter 7 when the reader can judge whether the explanation of the moments of interests are compared with the description given in the remaining chapters of Section II.

Endnotes

1. Archives most visited include: www.cryptome.org, www.politechbot.com, eff.org and crypto.org.
2. News sites most visited include: news.com, cnn.com, wired.com, msnbc, news.bbcco.uk, techweb.com.
3. NGO sites most visited include: www.epic.org, www.eff.org, www.cdt.org, www.gilc.org, www.privacyinternational.org, www.fipr.org.
4. Mailing lists most used were: *ukcrypto*, *politech*, *gilc*, *cyber-rights*, *fipr-ac*, *rre*, *cypherpunks*.

Chapter 5: Domestic and Foreign Policies and Recalcitrance in the U.S.

Abstract

Using the approach and methodology presented in earlier chapters, I will present a socio-technological story of how the U.S. policies transformed throughout the discourse (particularly between 1993 and 2000). I will also investigate some specific implementations of cryptography that are affected by policy. The resistance, objection, accordance, or ignorance of the technologies are noted.

5.0 Introduction

The United States has a rich regulatory history involving the development, use, and proliferation of cryptography, having attempted a number of policies, of different policy types, as presented in chapter 1. This chapter will present a number of these policies, focusing briefly on the early application of type I policies, followed by the more detailed interactions with a number of actors emerging from type II and type III policies.

The *story* of cryptography policy in the U.S. is an anthology: many short-stories with many strategies and tactics. This chapter is therefore presented not only as a chronological account; many of these short-stories overlap, many of the actors represent multiple interests and have too much to say, that would otherwise be confusing for presentation or analysis. For example, the domestic story and the export controls stories are separate in many ways but were very much part of the same strategy. As a result, §5.1 discusses algorithmic and export restrictions based key sizes, introduced prior to the 1990s but altered subsequently; §5.2 introduces the Clipper Chip, the hardware key escrow policy beginning in 1993, followed by software key escrow and key recovery in §5.3. In §5.4 the next generation of export controls are discussed, particularly their use as domestic controls. Finally §5.5 describes the process of policy liberalisation.

The added dimension of the technological will also be presented. Distributed throughout I present in detail some of the technological solutions that were constructed in compliance, rejection, opposition, or ignorance of the regimes of regulation. In §5.1 I present the standard algorithms and their design processes, to determine their capabilities and capacities, both being results of intervention. §5.2 reviews the details and flaws of the Clipper Chip. The epistemic community of researchers and technologists responded to software key escrow requirements, arguing that there are large risks and costs, if not

impracticalities, as outlined in §5.3. The government counter-argued that some software solutions had been developed, such as Entrust Technologies' Public Key Infrastructure (PKI) solutions; Entrust's approach to key recovery is also reviewed in §5.3. The community later found flaws in a version of Pretty Good Privacy (PGP), a popular cryptographic application; this version was altered to reflect government policy; also investigated in §5.3. In §5.4 I present a number of technologies that were developed in accordance with export policy requirements, including Secure Sockets Layer (SSL), Microsoft Cryptographic Application Program Interface (CAPI), and Lotus Workfactor Reduction (WFR), and the discourses surrounding these. The purpose of this exposition is to view the discourse as socio-technological, to allow for the detailed comments of the epistemic community, and to compare and contrast articulations, as discussed in section I of this dissertation.

5.1 The Story of *Strong* Cryptography

Up until the 1990s the U.S. Government practiced type I policies, regulating the development of algorithms. The regulator in this case was the National Security Agency (NSA), as it regulated the release of algorithms for public review. In 1979, the Director of the NSA stated publicly (Inman 1979) that open publication of cryptography research was harmful to national security, and sought statutory authority to limit the publication of cryptographic research (USACM 1994). Previously, by secretly patenting processes and algorithms, the NSA prevented the academic community from publishing results under the threat of patent infringement.

The regimes of regulation proposed in the U.S. throughout the 1990s revolved around the choice of algorithms and the keys. Early policies concentrated on controlling the form and length of the keys. This is the issue of *strong* cryptography.[1] If encrypted data (messages, files, etc.) need to be decrypted for national security and law enforcement purposes, without the keys necessarily being at the disposal of the government agencies, then the keys will have to be guessed. This gives rise to the discourse surrounding key lengths, brute force cracking, and strong cryptography.

5.1.1 Key Lengths and Brute Force Cracking

Guessing a key, i.e. *brute force cracking* a key, is supposed to be non-trivial in modern cryptography. In the case of the *RSA* algorithm, it involves factorising large numbers into large co-prime numbers. The larger the keys in size, i.e. their length in bits, the more difficult this factorisation becomes; therefore a short key length can be *brute forced* faster

than a longer key. For example, in 1999 researchers managed to factor a 140-digit key-pair over four weeks using a sum total of 185 computers (Cavallar and others 1999; RSA Laboratories 1999).

Meanwhile, for symmetrical cryptography, such as the Data Encryption Standard (*DES*), the challenge is to guess the key within the keyspace. *DES* by design has a maximum key length of 56-bits; guessing the key involves searching through the space of numbers between 1 and 2^{56}. Traditionally, the strength of these systems has been based on the inability of computers to guess the key in a sufficient amount of time. In the 1970s when *DES* was negotiated, relative to resources at the time, 56 bits was generally sufficient. With the advent of cheaper resources such as processing power and networking the technological environment has transformed cryptography.

The capacity to brute-force keys is interpretively flexible. In 1997, Judge Louis Freeh, then-Director of the U.S. Federal Bureau of Investigations (FBI) testified to a House of Representatives committee with regards to *DES*, arguing that

> If we hooked together thousands of computers and worked together over 4 months we might, as was recently demonstrated decrypt one message bit. That is not going to make a difference in a kidnapping case, it is not going to make a difference in a national security case. We don't have the technology or the brute force capability to get this information. (Freeh, Crowell, and Reinsch 1997a)

The then-director of the NSA, William Crowell supported this statement.

> There is no brute force solution for law enforcement. (REDACTED) A group of students -- not students -- the Internet gang last week broke a single message using 56-bit DES. It took 78,000 computers 96 days to break one message, and the headline was, DES has weak encryption. If that had been 64-bit encryption, which is available for export today, and is available freely for domestic use, that same effort would have taken 7,000 years. And if it had been 128-bit cryptography, which is what PGP is, pretty good privacy, it would have taken 8.6 trillion times the age of the universe. (Freeh, Crowell, and Reinsch 1997b)

These claims are contentious, however. In 1993, Michael Wiener, then at Nortel Labs, wrote a paper presenting the specifications of a machine that could be built for 1 million USD that could perform an exhaustive *DES* key search, finding a key on average in 3.5 hours (Wiener 1993). While the machine was never built, the research indicated that someone with sufficient interest and funds could develop a machine that would render much of the world's secured data able for decryption.

There are frequent competitions among the security and cryptography community to test brute forcing methods, as new resources and techniques are discovered. The next section describes one such method.

5.1.2 Interrogating Articulations with Technologies: Cracking Machines

In 1998 the Electronic Frontier Foundation (EFF), a civil liberties organisation in the U.S., developed a system, costing 210,000 USD, that searched 92,160,000,000 keys in 4.524 days. They discovered something even more alarming, however: economies of scale could be developed. Through parallelizing this process just slightly in their tests, EFF managed to speed up the process by a factor of 36,000. The EFF wrote a detailed report on how to construct such a machine.

> This book describes a machine which we actually built to crack DES. The machine exists, and its existence can easily be verified. You can buy one yourself, in the U.S.; or you can build one yourself if you desire. (...) We have published its details so that other scientists and engineers can review, reproduce, and build on our network. There can be no more doubt. DES is not secure. (Electronic Frontier Foundation 1998)

In 1999, the EFF used this technology, *DESCracker*, in conjunction with networked computers and set a new record by cracking a *DES* key in under 23 hours. The network, provided by Distributed.Net consisted of 100,000 personal computers on the Internet trying keys in background processes, tested 245 billion keys per second (Clark 1999). It is believed that the NSA computing capabilities are significantly greater than the resources of EFF and Distributed.Net (Federation of American Scientists 1998). Moreover, the design of DESCracker was not particularly advanced; as a result the supporting claim by the head of the NSA to Mr. Freeh's statement is questionable.

In 1996, a committee of cryptographers concerned with the problem of brute force attacks was convened by the Business Software Alliance (BSA), an industry organisation consisting of leading high-tech companies. The committee released an influential report on the advised length of keys for adequate security (Blaze and others 1996). Finding *DES* to be inadequate because of the 56-bit key-length limitation, the committee advised that an adequate challenge to adversaries would be a 75-bit key. The committee estimated that an adversary would have to spend $10 million in order to search out the larger keyspace over six years.

The expert committee concluded that to protect information adequately for the next 20 years in the face of expected advances in computing power, keys in newly deployed systems should be at least 90-bits (Blaze and others 1996, p.3). The most interesting conclusion is in

line with the economy of scale finding of the DESCracker: encrypting information with stronger keys (e.g. 128-bit keys) requires little more in computing resources than encrypting using weaker keys (e.g. with 40-bit keys).

> There is no practical or economic reason to design computer hardware or software to provide differing levels of encryption for different messages. It is simplest, most prudent, and thus fundamentally most economical to employ a uniformly high level of encryption: the strongest encryption required for any information that might be stored or transmitted by a secure system. (Blaze and others 1996, p.4)

The duality of modern computing is this: as increasing computing power becomes more ubiquitous, the processing problems related to increasing the key length are mitigated; and as computing and networking power increases, there is a pressing need to increase the key lengths.

There were objectors to these findings, although anonymous. Shortly after the release of the BSA report, a four-page document was circulated to members of Congress, presumably from the NSA although there was no supporting documentation (Blaze and Diffie 1996). The document argued that parallel key searches suffered from 'physical realities', such as interconnections, heat dissipation, input/output bandwidth, etc. making it difficult to divide the task of key searches. Two of the authors of the BSA report responded to this critique that "while these factors do limit the scalability of more general purpose multiprocessor computers (...) , they do not apply at all to specialized exhaustive key search machines" (Blaze and Diffie 1996). Another objection was that the BSA report underestimated the costs of chips by an order of 1000. The two authors responded that

> our $10.00 per chip estimate is based on an actual price quote from a commercial chip fabrication vendor for a moderate-size order for an exhaustive search ASIC designed in 1993 by Michael Wiener. Perhaps NSA could reduce its own costs by changing vendors. (Blaze and Diffie 1996)

These techniques were implemented in DESCracker, supporting the articulations of the expert committee over the articulations of the NSA.

5.1.3 Algorithms and Abilities -- *DES, DSA*, and NSA

From the above discourse on brute force capabilities, it may be assumed that the NSA's specialty is in obfuscation, and limiting the strength of cryptosystems. The NSA's interests are more complex, however. The NSA's role in the standards process is an interesting exemplar of its complex goals and interests.

The key length constraint of *DES* was dictated by the NSA. *DES* was designed originally by IBM to have key sizes up to 128-bit; some experts argued at the time for 256-bit keys. Upon submission to the U.S. Government for consideration as the national standard, the U.S. Government made two significant alterations. Interestingly, the first alteration was favourable for *DES* security (Ellison 1994); it involved modest changes that were later found to make the algorithm stronger to very advanced attacks, differential cryptanalysis, of which little was known publicly at the time. The other alteration was the restriction of the key size to 56-bits. In a committee review, the NSA articulated that the key-size needed to be limited because of parity checks and engineering constraints (Levy 2001).

In 1978 the Senate Intelligence Committee uncovered that the NSA had made these alterations (Banisar and Schneier 1997, p. 294). Some users of *DES* became concerned the NSA also included some back doors to the algorithm that only the NSA could take advantage of. However, over 25 years of open review and analysis of *DES* has only shown that its greatest weakness is not in the algorithm per se, but in its restriction of key size. The NSA had performed awkwardly in this situation, and Kahn hypothesises that it was due to the internal conflict within the NSA:

> a miniature debate seems to have broken out in secret between the two halves of the NSA. (...) The code-breaking side wanted to make sure that the cipher was weak enough for the NSA to solve it when used by foreign nations and companies. The code-making side wanted any cipher it was certifying for use by Americans to be truly good. The upshot was a bureaucratic compromise. (Kahn 1979)

This is an indication that the national security interests of government are not as monolithic and simple as often assumed.

When the U.S. National Institute for Science and Technology (NIST) decided to create a public key cryptography standard, a similar process ensued. The process began with the intention of using *RSA* as the algorithm for the standard, but the NSA intervened (Banisar and Schneier 1997, p.304-307). As Diffie and Landau propose, the decision to prevent *RSA* from being the standard lay "presumably in its flexibility, which allowed it to be used for purposes of confidentiality as well as authenticity" (1998, p.72).

What had started as a standard for digital signatures and secret key distribution for confidentiality, ended with the NSA submitting an alternative algorithm, the *Digital Signature Algorithm*, that only allowed for signatures (Banisar and Schneier 1997, p.305). NIST originally resisted, and based on a consultation process, concluded that there would be problems with general acceptance of *DSA* including the lack of privacy protection, incompatibility with the industry standard *RSA* algorithm, the NSA role in designing the

algorithm, and among several technical problems (Rotenberg 1993). The Department of Treasury and the Internal Revenue Service even threatened to adopt *RSA* (Banisar and Schneier 1997, p.306). In May 1994, NIST announced the adoption of the (now) Digital Signature Standard (*DSS*), even after the overwhelmingly negative comments from the public; the identified failure of the hashing algorithm (Diffie 1997); and patent conflicts (Diffie and Landau 1998).

Strong cryptography as a result is represented by a non-static issue of key length: larger keys in a trusted algorithm means that a system is strong, shorter keys infer *weak* cryptography. The classification of strong vs. weak is not without controversy; actors speak of each differently.

5.2 Hardcoding *Escrow*: The Clipper Policies

The public history of domestic use controls in the U.S. formally began in 1993. Previously, the controls were limited to export and the associated control on publication of cryptographic research. The first type III policy that was proposed for domestic users was a technology, the *Clipper Chip*.

Clipper was a solution to what had seemed inevitable: the eventual diffusion of cryptographic products for use over telephone lines by the general public. When AT&T began developing a new secure telephone to replace the ageing previous model, STU III, with a new version, the TSD 3600, implementing *DES*, the U.S. Government grew concerned. Various government agencies decided that they needed to find a solution.

The Clinton Administration entered this situation fresh from an election, inheriting a set, but unannounced, policy in 1993. In a letter to the National Computer System Security and Privacy Advisory Board and copied to the Attorney General, the Secretary of Commerce, the OMB, and NIST, in 1992, the NSA Director, Admiral McConnell noted,

> The National Security Agency has serious reservations about a public debate on cryptography. We do, however, support the need to ensure that government decision-makers are made aware of the oft-conflicting interests of the various stakeholders who seek to influence cryptographic policy. (McConnell 1992a)

In another letter, this time to the Attorney General (and copied to the Secretary of Defense), the Director of the NSA pointed to the initiation of a process of co-operation:

> Regarding your request of the 7th October 1992, we are prepared to provide the Department of Justice (DOJ) and the (FBI) technical advice and assistance in addressing the challenges to law enforcement

> posed by the sale and use of products to encrypt voice communications. (McConnell 1992b)

In 1992, a letter addressed to the FBI from the Attorney General outlined concerns about the timing and implementation of Clipper, based on the shifting administration from Bush to Clinton.

> We also believe that going forward with the installation of the Clipper chip based on the approval of the current Administration has some potential pitfalls. The most serious concern is that the scenario regarding the use of the "exploitable" chip could surface publicly during the transition period or shortly after the Clinton administration arrives, but before they approve the proposed overall solution. If that happened, it might result in their being pushed toward disavowing the prior Bush Administration approach in order to avoid the controversy, rather than the Clinton administration moving forward with us in a consolidated effort to convince Congress and the public of the merits of our position. (Davis 1992)

The actors were preparing for controversy, and hoped for a carefully planned and executed programme.

George Tenet, then Senior Director for Intelligence Programs (and later director of the CIA), was also mobilised. In a memo to Leon Fuerth, Assistant to Vice President Gore for National Security Affairs, he stated

> We need to get together for purposes of devising an action strategy to bring the encryption issue to closure. … We need to sit down, review the bidding, identify the issues that may need additional work, figure out what we need to do for the Vice President to get him fully fluent, engage lawyers, etc. to address the privacy issues, construct a package, and then bring it forward to the President. (Tenet 1993b)

Tenet later organised the meeting with the Vice President, a month before the eventual release of the policy, sending a memo entitled: *HELP HELP HELP*, stating

> We need to schedule some time for Admiral Studeman (CIA) and Admiral McConnel (NSA) to brief the Vice President next week, preferably early next week on encryption. (...) Leon, I think I know what the VP wants to hear McConnel/Studeman talk about. Can we have a discrete discussion to further help me in my tasking. (Tenet 1993a)

On March 31st, that meeting occurred with Vice President Al Gore, who at the time was responsible for affairs relating to information technology. The *Who's Who* of the executive government was there: Attorney General, Secretary of Commerce, CIA Director, Director of Office of Management and Budget, Presidential Assistant for Economic Policy, FBI Director, NSA Director, Under Secretary of Defense for Acquisition, and two Directors for Intelligence Programs (Gore 1993).

Over the subsequent years, the Clinton Administration articulated the concerns of these agencies, even though the strategy involved aligned interests that predated the Administration's involvement.

> Press Secretary: While encryption technology can help Americans protect business secrets and the unauthorized release of personal information, it also can be used by terrorists, drug dealers, and other criminals. (The White House 1993)

> Vice President: Our policy is designed to provide better encryption to individuals and businesses while ensuring that the needs of law enforcement and national security are met. Encryption is a law and order issue since it can be used by criminals to thwart wiretaps and avoid detection and prosecution. It also has huge strategic value. (Gore 1994b)

> Attorney General: Encryption as a practical matter decreases the power of law enforcement and all we endeavour to do is maintain the status quo. (Reno 1996)

> Under-Secretary of Commerce: The President has decided on an encryption policy, and we are well on our way to implementing it. It balances all of the competing interests in this issue: privacy, electronic commerce, law enforcement, and national security. (Reinsch 1997)

The solution advocated was *key escrow*, a means of depositing keys so that they are within surreptitious reach of law enforcement agencies (Gladman 1998b).

On April 16, 1993 the Clipper Policy was officially announced by the Clinton Administration. As argued within the original declaration,

> Rather than use technology to accommodate the sometimes competing interests of economic growth, privacy and law enforcement, previous policies have pitted government against industry and the rights of privacy against law enforcement. (...) The President today announced a new initiative that will bring the Federal Government together with industry in a voluntary program to improve the security and privacy of telephone communications while meeting the legitimate needs of law enforcement. (The White House 1993)

Clipper was the name of a microchip that could be embedded within telephones that would permit for secure communications sessions, while still maintaining law enforcement access to communications. The keys that are used for establishing the secure session could be accessed by law enforcement under warrant; the keys would be escrowed in a third party for that eventuality.

Choosing Clipper allowed the Clinton Administration to appease the concerns of law enforcement, and hopefully appease the public concerns for security.

> The Administration is not saying, "since encryption threatens the public safety and effective law enforcement, we will prohibit it outright" as some countries have effectively done; nor is the U.S. saying that "every American, as a matter of right, is entitled to an unbreakable commercial encryption product." There is a false "tension" created in the assessment that this issue is an "either-or" proposition. Rather, both concerns can be, and in fact are, harmoniously balanced through a reasoned, balanced approach such as is proposed with the "Clipper Chip" and similar encryption techniques. (The White House 1993)

This articulated settlement of interests of public security was two-fold: unabated law enforcement access and the subsequent security from this level of surveillance over criminals, and the strength of the algorithm preventing illegal surveillance.

The government was attempting to enrol the public and corporate users with the idea of *stronger* encryption with increased key lengths. The claim that "(i)t scrambles telephone communications using an encryption algorithm that is more powerful than many in commercial use today" (The White House 1993) is accurate, but not quite precise because it also involved key escrow, the representation of law enforcement interests. According to the then-Director of the FBI,

> Clipper employs an algorithm which is based upon an 80-bit key. Although only 24 bits longer, "Clipper" encryption provides for 16 million times as many permutations which makes it geometrically more difficult to decrypt. (Sessions 1993, p.7)

The NRC report clarified 'strong' and 'escrowed' encryption.

> The relationship between strong encryption and escrowed encryption should be noted. Escrowed encryption refers to an approach to encryption that enables access to plaintext without requiring a third party to perform a cryptanalytic attack. At the same time, escrowed encryption can involve cryptographic algorithms that are strong or weak and keys that are long or short. (NRC 1996, p.169)

By confusing the two, the government position could be labelled as 'supporting strong cryptography'.

Another detracting feature to the strong cryptography claim was the use of the *Skipjack* algorithm. It was developed by the NSA but not released for public review, thus increasing uncertainty regarding the integrity of Clipper.

In order to promote interest and confidence in the scheme, the Clinton Administration promised to purchase 'several thousand of the new devices' (The White House 1993). This market intervention by the government was in direct reference to the AT&T TSD 3600 device. By offering to create a market for the secure phones, the U.S. government was

hoping to create an economy of scale, and through network effects, to get as many people using Clipper.

In 1994, the ideas behind Clipper became a national standard, the Escrowed Encryption Standard (*EES*); not without a controversial consultation however (c.f. Department of Commerce 1994). The process included responses from 22 government agencies, 22 industry organizations and 276 individuals. The results included concerns about the banning of non-escrowed cryptography, a lack of technical details in the consultation process, infringements on individual rights, concerns about the secret algorithm, to name a few. Costs of the key escrow agencies were a concern; NIST responded with an estimated cost of establishing the escrow system of $14 million, while the cost of operating the key escrow facility was estimated at $16 million annually.

The *EES* applied beyond voice telephony, however. While Clipper was designed for voice encryption on telephone lines, the *Capstone chip*[2] on the *Fortezza card* were designed to support escrowed encryption for data storage and digital communications. These all became government standards; companies wishing to sell security products to the government had to implement these standards. For example, the NSA issued a solicitation for over 750,000 Fortezza cards (NRC 1996, p.177).

The *EES* was designed with access in mind. Within each communication transmission a law enforcement access field (LEAF) is included. This 128-bit field consists of a copy of the session key (80-bits) for that given transmission, and information that identifies the chip that created the key (32 bits); and a checksum (16 bits). The copy of the session key is encrypted to the LEAF using the unit key, assigned to the chip at the time of manufacturing. This same unit key is stored in escrow, for law enforcement access (Blaze 1994). Finally, all 128-bits are encrypted using a global/family key (see figure 5.1).

The purpose of this LEAF is to allow law enforcement agencies to use the information in the LEAF to identify (once decrypted using the family key) the particular device of interest (Unit ID), solicit its unit key components from the escrow agencies, decrypt the session key using the escrowed unit key, to decrypt the traffic (NRC 1996, p.171). The chip would be protected against reverse engineering and other attempts to access its technical details.

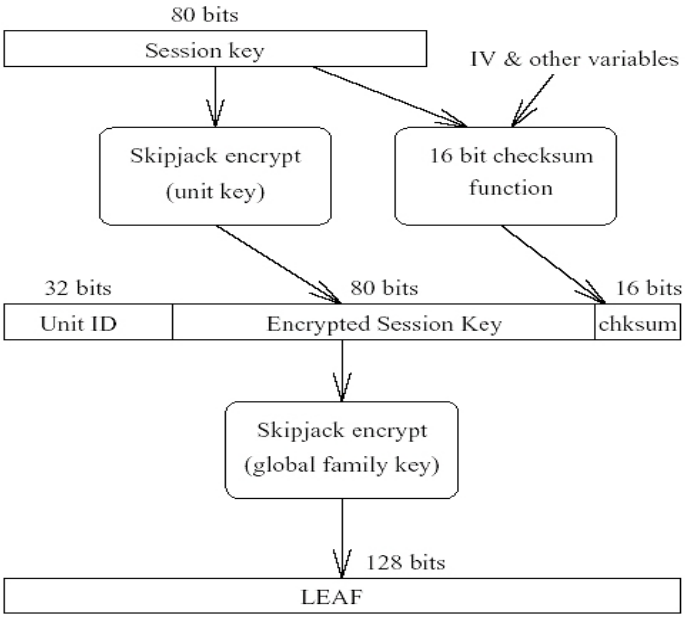

Figure 5.1 The EES' Law Enforcement Access Field (LEAF), from (Blaze 1994)

As often occurs with security systems (Anderson 2001), the system could be forced to behave in manners other than intended. A report written by Matt Blaze (1994), a security engineer at AT&T Bell laboratories described how the LEAF could be circumvented on the Capstone implementation, thus preventing lawful access to the session keys.

> The system is intended to be difficult to deploy without also sending a valid LEAF and thereby exposing the traffic to the possibility of government monitoring. (...) To force applications to send the LEAF on the same channel as the traffic, EES devices will not decrypt data until they have received a valid LEAF for the current session key.

Blaze found that this is not always the case, and identified a weakness in that very protocol of requiring the LEAF prior to decryption, "by using that interface in unexpected ways". Taking advantage of the relatively small checksum (16 bits, which can be searched exhaustively within a relatively small period of time), Blaze reverse engineered the factors involved in creating the checksum, and with that knowledge, describes a method to construct applications use *Skipjack* while preventing law enforcement access through the LEAF. He describes two classes of "rogue" *EES* applications: those that can communicate only with other rogue systems and those that can successfully interoperate with *EES* "legal" systems as well. "The latter category especially threatens the goals of the *EES* program, since such rogue applications would be operationally equivalent to their legal counterparts without being subject to government access." (Blaze 1994)

The solution to this predicament is to increase the size of the checksum to make an exhaustive search infeasible (to 32 or 64 bits), which requires increasing the size of the LEAF, or reducing the size of other fields (session key length or unique ID). That is,

> (i)ncreasing the size of the LEAF package to, say, 192 bits would provide room for an additional 64 bits of checksum redundancy but would likely require significant re-engineering of many existing EES components, from the processors themselves to the protocols and applications that use them. Within the constraints of the 128 bit package, checksum size can increase only at the expense of either the unit ID or encrypted session key fields. The 32 bit unit ID field appears to be at the minimum possible size given the intended scope of the EES program (a previous version of the LEAF with a 25 bit unit ID was considered inadequate. It may be possible to use bits from the encrypted session key field to increase the checksum size, at some expense in law enforcement wiretap access performance. If only 64 bits of the encrypted session key were included in the LEAF, the wiretapper could exhaustively search for the remaining 16 bits at decrypt time. Such a search, with properly optimized hardware, would likely add at most a few seconds to the decrypt time and would enable 32 bit LEAF checksums within the existing LEAF size constraints. (Blaze 1994)

Blaze is describing the balancing act and potential tradeoffs to consider in order to rectify the fault. The system can not be changed arbitrarily; every small shift of data within the LEAF has impacts on the intentionality of the design and the outcomes. According to Levy (2001), the wireless telephone companies warned that the LEAF had to be small for practical purposes. It was later discovered that the NSA wished to design a larger checksum into the field, but the FBI had insisted on using 80 bits so that the full session key would be transmitted (Levy 2001, p.258).

Blaze also predicted the diffusion of the method of circumvention.

> (I)t is likely that little or no special skill would be required to install and operate the modified software. In particular, one can imagine "patches" to defeat key escrow in EES-based systems being distributed over networks such as the Internet in much the same way that other software is distributed today. (Blaze 1994)

The reception to the publication was curious. The NSA had even reviewed the paper, correcting errors of transcription and grammar (Levy 2001, p.258). AT&T had millions of dollars riding on the phones but allowed for its publication as well. Blaze's findings were reported on the front page of the New York Times, to the surprise of many including Blaze. Public awareness and concern thus grew.

As with *DSS* and *DES*, there were also public confidence concerns with *Skipjack*. Being designed by the NSA, the algorithm was not to be released to the general public for review. Memories of *DES*-tampering articulations reappeared in the discourse, but exacerbated due

to the lack of open review; at least *DES* was reviewed publicly. Some believed that an additional backdoor had been introduced, others believed that the choice of keys was further limited, i.e. the keyspace was *flat* (Schneier 1996), thus making it more likely that secured communications could be decrypted without a warrant. Even the NSA recommended a review by *outside* mathematicians (Brooks 1993). This review occurred eventually under high security, concluding that *Skipjack* was secure: there are no secret backdoors, and the secrecy of the algorithm did not affect its security (Brickell and others 1993). This did not increase public confidence however (Blaze 1994).

The idea of the keys being stored within the government also raised concerns. These *third party* escrow agents were proposed initially to be the Department of Treasury and Department of Commerce. These were later proposed to be non-governmental organisations that were not as likely to be coerced by government agencies into handing over keys without proper authorisation.

The market for these telephones and devices diminished rapidly, as the devices were lambasted in the media, by advocacy groups and civil libertarians. Those on the political right and left aligned to protect the right of use. Massive campaigns began, posters and t-shirts were sold, particularly the following:

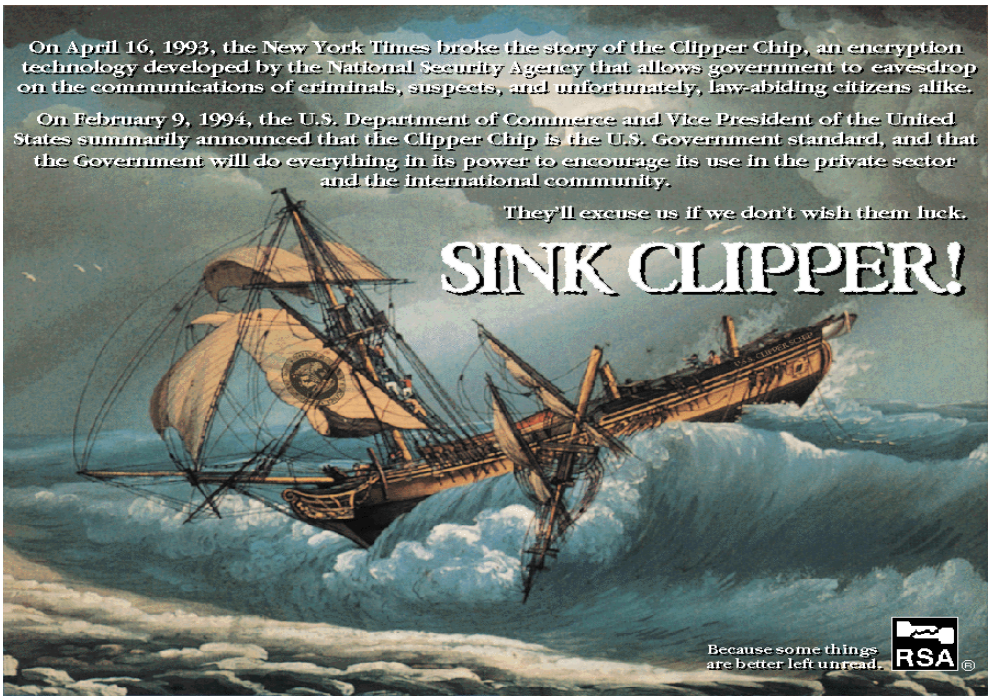

Figure 5.2 Sink Clipper Campaign poster, from EPIC website

Further reports were written, testimonies given, comments submitted, articles published, many of them disagreeing with the idea of designing a technology specifically for surveillance. As Whitfield Diffie stated in Congressional testimony,

> In the month that has elapsed since the announcement, we have studied the Clipper chip proposal as carefully as the available information permits. We conclude that such a proposal is at best premature and at worst will have a damaging effect on both business security and civil rights without making any improvement in law enforcement. (Diffie 1993)

Other speakers testified on repressive regimes, and the importance of privacy. The concern extended to politicians. According to Marc Rotenberg, director of the Electronic Privacy Information Center (EPIC), arguably the most active civil society organisation in this discourse,

> Congressman Markey, after hearing the testimony presented, noted that the Clipper proposal had raised an "arched eyebrow among the whole committee" and that the committee viewed the proposal skeptically. This statement was the latest indication that the Clipper proposal has not been well received by policy makers. (Rotenberg 1993)

Within this environment, civil liberties advocates and industry organised a petition and a letter sent to the President, stating

> The private sector and the public have expressed nearly unanimous opposition to Clipper. In the formal request for comments conducted by the Department of Commerce last year, less than a handful of respondents supported the plan. Several hundred opposed it. Some have proposed that Clipper be adopted on a voluntary basis and suggest that other technical approaches will remain viable. The government, however, exerts enormous influence in the marketplace, and the likelihood that competing standards would survive is small. Few in the user community believe that the proposal would be truly voluntary. The Clipper proposal should not be adopted. (Computer Professionals for Social Responsibility 1994)

The petition eventually had 50,000 signatories.[3]

The U.S. government continued to try to create a market for *EES*. Companies were approached to implement the Fortezza cards within their systems software: Netscape and Oracle supposedly received over five million USD each to implement it in their applications, Qualcomm received two million USD to implement it into digital cellular phones (Banisar and Schneier 1997, p.318-9). By early 1996, AT&T reportedly sold 10,000 to 15,000 secure phones, but only some of those had the Clipper chip inside (NRC 1996, p.174). Some accounts claim that only 9000 of these phones were actually Clipper-enabled and were sold mostly to the FBI (Diffie and Landau 1998, p. 215).

The private sector continued to be critical of the proposal, and the government began to listen. Without a solid market incentive, Clipper was bound to be restricted to a segment of the market driven mostly by mandatory government requirements (Walker and others 1995).

As a result, throughout 1994 and 1995, the policy shifted away from hardware enforced *EES* and towards software key escrow, with trusted third parties being companies themselves. The result, however, is that the market for voice encryption devices disappeared, and even today, apart from mobile telephony, telephone conversations remain generally unencrypted and unprotected (Diffie and Landau 1998, p.215).

5.3 The Story of *Soft* Key Escrow

Contrary to the wishes of the NSA, cryptography policy became an issue of great discussion in Congress, with a number of proposed bills by Senators and Representatives, pushing for decreased controls e.g. (105th Congress 1997a; 105th Congress 1997b; 105th Congress 1997c; 105th Congress 1997d; 105th Congress 1997e; 105th Congress 1997f; Kerrey and McCain 1997; Leahy 1998).

> A few years ago, only a small number of people knew about encryption. Today, virtually everyone who is familiar with the Internet recognizes that encryption is critical to the growth of the on-line economy, and the protection of privacy and security. Encryption is not just good for business and the economy. It is necessary for the growth of the Internet and the safety of consumers in the twenty-first century. (Rotenberg 1996)

The policies were changing, but the interests and goals remained the same.

> It is a critical to understand that the White House continues to believe that encryption should only be available if it is can easily be broken. There have been several proposals all based on this same premise. Each has a new name. The White House will promote "Voluntary Key Escrow." They will endorse "Commercial Key Escrow." They will support "Escrow Encryption Standard." And they will back a new plan for "Key Management Infrastructure." Call it what you will, it is still Clipper. (Rotenberg 1996)

In the policy initiatives following the Clipper Chip, the technology was disembodied from the chip, but the philosophy remained: escrow was essential.

Rather than a government-developed solution, the subsequent policies attempted to convince industry that it was their responsibility, and in their interests, to develop technological solutions.

5.3.1 Key Management Infrastructure

In 1994, Vice President Al Gore wrote a response to a critical letter he received from Congressional Representative Cantwell. Gore acknowledged that there was a significant amount of criticism within industry regarding the Clipper Chip,

> We welcome the opportunity to work with industry to design a more versatile, less expensive system. Such a key escrow system would be implementable in software, firmware, hardware, or any combination thereof, would not rely upon a classified algorithm, would be voluntary, and would be exportable. While there are many severe challenges to developing such a system, we are committed to a diligent effort with industry and academia to create such a system. (Gore 1994a)

While many believed that Gore was essentially claiming the death of Clipper, he was only beginning the next programme of action.

Clipper was only the first articulation of escrow policy, embedded within government-developed hardware. The subsequent proposal included embedding the policy within software, developed by the market. NIST was called to provide the criteria for software key escrow, the Ten Criteria. This policy change involved some learning from earlier failures, and some new strategies.

1. The product will use an unclassified encryption algorithm with a key length not to exceed 64 bits.
2. The product shall be designed to prevent multiple encryption.
3. The key required to decrypt (...) shall be accessible through a key escrow mechanism in the product, and such keys will be escrowed during manufacture in accordance with #10. (...)
4. The key escrow mechanism shall be designed to include with each encrypted message or file (...) information sufficient for the escrow agent(s) (...) to decrypt.
5. The product shall be resistant to any alteration that would disable or circumvent the key escrow mechanism (...).
6. The product shall not decrypt messages or files encrypted by non-escrowed products (...).
7. The key escrow mechanism allows access (...) regardless of whether that user is the sender or the intended recipient (...).
8. The key escrow mechanism shall not require repeated involvement by the escrow agents for the recovery of multiple decryption keys (...)
9. In the event any such product is or may be available in the U.S., each production copy of the software shall either have a unique key required for decrypting (...) that is escrowed in accordance with #10, or have the capability for its escrow mechanism to be rekeyed and any new key to be escrowed (...).
10. The product shall accept escrow of its key(s) only with escrow agents certified by the U.S. Government or by foreign governments with which the U.S. Government has formal agreements (...).

(National Institute of Standards and Technology 1995, redacted)

Industry was not immediately opposed to the idea of software key escrow, but concern arose regarding the requirements. As the BSA noted in Congressional testimony, the criteria

> continue to reflect a misunderstanding of the marketplace and, if implemented in anything like their current form, will prevent key escrow encryption from ever being commercially adopted. (...) But what the government fails to recognize is that key escrow encryption approaches must be commercially desirable and voluntarily adopted. Computer users must want to buy programs with such features. America's software companies can't sell what users won't buy -- they have not become as successful as they are by trying to force their customers to purchase products with unwanted features. Therefore, unless there is market demand for key escrow encryption, software companies are not likely to produce programs with such features. (Holleyman 1995)

The method of government intervention into the marketplace was also of concern.

> Perhaps government officials believe that they know more than American industry about what computer users worldwide are demanding by way of information security. If that is so, then we must strongly disagree. (...) Is the Administration really going to pick winners and losers in the computing industries when it comes to providing information security? (...) How so? Clearly the government is trying to force America's software companies to include government sought key escrow features in its software as the "price" for export approval. (Holleyman 1995)

This was indeed part of the government's strategy.

The U.S. Government then began discussing the notion of a *Key Management Infrastructure* (KMI), 'the Son of Clipper' (Holleyman 1995), or 'Clipper with a Happy Face' (Banisar and Schneier 1997, p.320). The strategy was to embed key escrow into the key management infrastructure, which in itself is perceived as necessary by some in industry, and further intertwining this strategy with export controls. The interest of industry was piqued, naturally; the language of policy included references to the *lead* of industry, and *voluntary participation* in a required infrastructure, and *relaxation of export controls* (McConnel and Appel 1996, p.3).

Another translation was the change of terminology used by government, as *key escrow* had become a popular derogatory term. Proponents of key escrow began using the term *key recovery*, particularly to enrol the interests of business. This new term was used to convince businesses that they needed to develop and implement such systems for their own uses. If businesses found a need for key recovery (due to a loss of keys, or rogue employees, as examples), then the market would have to respond with key recovery products.

Similarly, a government sponsored standards committee, the Technical Advisory Committee to Develop a Federal Information Processing Standard for the Federal Key Management Infrastructure (TACDFIPSFKMI) convened to articulate key recovery as being motivated by three primary scenarios,

1. Recovery of stored data on behalf of an organisation (or individual) e.g., in response to the accidental loss of keys;
2. Recovery of stored or communicated data on behalf of an organisation (e.g. for the purposes of monitoring or auditing activities); and
3. Recovery of communicated or stored data by authorised authorities.

(TACFIPSFKMI 1995)

The third requirement reveals the nature of key recovery **as a government policy** as being key escrow using new terminology, however (Gladman 1998b).

The market responded to the policy. Various products, including Entrust's applications and Pretty Good Privacy enable a level of key recovery or data recovery. The presence of these products today does not reconcile the conflict between commercial and government requirements. That is, the requirements of government, the commercial world, and individual users are very different; so different that there is little overlap between systems that address these two problems (Abelson and others 1998). While the market did respond, whether these products were a response to a call from the marketplace or government policy, requires interrogation.

5.3.2 Risks of Key Recovery

There have been a number of articulations of the policy of access to keys presented thus far. First there was *EES* and Clipper, followed by software key escrow in accordance to the Ten Criteria, and then the TACFIPSFKMI articulation of 'key recovery'. Each policy evolution involved learning from earlier policy failures.

In a seminal report, a group of leading cryptographers and security specialists studied the *Risks of Key Recovery*, arguing that all the proposed policies suffered from similar flaws. Their conclusions were that the costs, risks, and the complexity of a key recovery infrastructure were too significant. The following subsections outline some of their issues and ideas.

Being Specific on the Requirements

The report's first argument was that key recovery was not a marketplace need; or at least not as it was defined by government. As government officials tried to convince industry that users needed key recovery, the report in turn argued, in accordance with others (e.g.

Gladman 1998b; Rubinstein 1997), that users have very different requirements. Users, they argued, are not interested in communications recovery; while this is the main purpose of the policies.

Second, the application of cryptography within e-commerce was very different from what the policies envisioned. Cryptography's role in e-commerce, the report argues, is to support binding commitments. The problem then arises that some key recovery schemes archive authentication keys along with confidentiality keys -- thus destroying the non-repudiation property that supports binding commitments. The archiving of signature keys is a dangerous practice, and unnecessary to meet the interests of government surveillance. Even if the policies changed so as to not require the escrow of signature keys (as permitted by *DSS*), and requiring only the escrow of encryption keys, this would still be problematic, particularly with algorithms like *RSA* that do not separate signature and encryption keys.

> (I)t is difficult to exclude authentication and signature keys from a key recovery infrastructure of the kind proposed by the government, because some keys are used for both signature and encryption. Nor is it sufficient to exclude from the recovery system keys used only to protect financial transactions, since many electronic commerce schemes use keys that are general in scope. The same key might be used, for example, to encrypt personal electronic mail as well as to electronically sign contracts or authorize funds transfers. (Abelson and others 1998)

The report argues that the policies involve a misunderstanding of key *granularity*: how keys are specifically used, implemented, destroyed, and interpreted.

Third, the report argues that a key is always most secure when it resides only with the user. If users and businesses are concerned with the loss of keys, death of employees, the destruction of files, and the need to gain access to secured data, the report claims that key recovery involves a very different form than the key recovery infrastructure proposed by the government policy. Key recovery, according to government policy, proposes a centralised infrastructure of surveillance allowing surreptitious warranted access to keys; an ideal key recovery infrastructure for industry and individual use would only allow localised access, without any surreptitious access requirements. These are different infrastructures.

Finally they argued that the confusion between authentication services and recovery services at the infrastructure level leads to further problems. Combining key recovery with the Key Management Infrastructure transforms Certification Authorities (CAs) from trust management organisations, vouching for users identities and privileges, into Key Recovery Authorities, vastly increasing their risks and costs of operation. CAs are involved in signing public keys; the policy proposed that they collect private keys as well.

> (T)he operation of a certification authority does not require handling sensitive user data; a CA generally handles only users' public keys and never learns the associated secret keys. If a CA's (own) secret key is compromised or revealed, the only direct damage is that the certificates from it can be forged. On the other hand, if a key recovery agent's secrets are compromised, the damage can be far greater and more direct: every user of that recovery agent might have its own secrets compromised.

The report warns against such a translation of an authentication institution into a key depository; and argues further that the technology, the infrastructure, and the market will object to higher costs, risks, and complexity.

Complexity as Recalcitrance?

The report imagines that each Internet user will own a keypair. Many, if not most, users will have several public key pairs for various purposes, and others may choose to create key pairs every time that they are required. Additionally, there will be hundreds of billions of recoverable session keys, linked with every encrypted telephone call, every stored file, every email message, and every secure web session. This could involve billions of keys.

A key recovery infrastructure would then have to accommodate the over 17,000 local, state, and federal law enforcement agencies in the U.S. alone that may seek key information, and then other countries' law enforcement agencies. Then, they argue, we are left with a severely complex scenario.

Costs as Recalcitrance?

With complexity comes cost. The experts claimed that the operational and design costs for implementing such an infrastructure would be inordinately high. The U.S. Government's TACFIPSFKMI committee had the duty of developing a standard for a key recovery infrastructure. Two years later they abandoned their work. According to the Under-Secretary of Commerce, as quoted in the Washington Post (Pressman 1998), "(i)t clearly has turned out to be a difficult task (...) This one was a hard one."

With their collective expertise, the authors of the Risks report warned that such design considerations are difficult to accommodate.

> Non-key recovery systems have rather simple requirements and yet exploitable flaws are still often discovered in fielded systems. Our experiences designing, analyzing and implementing encryption systems convince us that adding key recovery makes it much more difficult to assure that such systems work as intended. It is possible, even likely, that lurking in any key recovery system are one or more design, implementation, or operational weaknesses that allow recovery of data by unauthorized parties. The commercial and

> academic world simply does not have the tools to properly analyze or design the complex systems that arise from key recovery. (Abelson and others 1998)

The report writers recalled the flaws in the Clipper initiative,

> The reason the Escrowed Encryption Standard had flaws is that good security is an extremely difficult technical problem to start with, and key recovery adds enormous complications with requirements unlike anything previously encountered.

Bruce Schneier, one of the authors of the Risks report later commented that the reason that the TACFIPSFKMI committee encountered troubles is that designing a system to meet both the interests of the market and those of law enforcement is practically 'impossible' (Pressman 1998).

Risk as Recalcitrance?

As the development of standards and systems proves to be challenging, no system can be proven to be entirely secure. These risks can also introduce additional problems, according to the report.

Through the existence of *key recovery centres* or *trusted third parties*, cryptography's central usefulness to the cause of security is circumvented. The new paths to plaintext outside the control of the intended users, as keys are no longer in their possession alone, creates unnecessary risks.

Lastly, the risk of storing all the keys within Key Recovery Authorities raises the risk that these stores will be susceptible to attack. The NSA agreed in its own report, stating that these centres will be heavily targeted (National Security Agency 1998). The threats were outlined as arising from four adversaries: rogue users, various espionage adversaries, rogue key recovery personnel, and rogue law enforcement agents.

The policy also hampered traditional cryptography risk management practices. The report argues that the policy would require a shift in security design away from *perfect forward secrecy*.

> A system with forward secrecy is one in which compromising the keys for decrypting one communication does not reduce the security of other communications. For example, in an encrypted telephone call, the keys for encrypting a call can be established as the call is set up. If these keys are destroyed when the call is over, the participants can be assured that no one can later decrypt that conversation -- even if the keys to some subsequent conversation are compromised. The result is that once the call is over, the information required to decrypt it ceases to exist; not even the parties to the call store the keys. Typically, keys are created and destroyed on a per-call basis, or even many times per call. This makes it possible to limit the costs and risks

> of secure processing and storage to the period of the call itself. (Abelson and others 1998)

Forward secrecy is considered desirable because of the simplification of design, and increases security while decreasing costs of a system.

> Key recovery destroys the forward secrecy property, since the ability to recover traffic continues to exist long after the original communication has occurred. It requires that the relevant keys be stored instead of destroyed, so that later government requests for the plaintext can succeed. If the keys are stored, they can be compromised; if they are destroyed, the threat of compromise ceases at that moment.

This is again the issue of *key granularity*: as there are many keys, there are keys with different purposes and tasks. The report calls on the policy to reflect granularity.

> Various systems have been proposed in which the recovery agent produces "master" keys that can decrypt all traffic to or from individual users or hardware devices. In other systems, only the keys for particular sessions are recovered. Coarse granularity (e.g., the master key of the targeted user) allows only limited control over what can be recovered (e.g., all data from a particular individual) but requires few interactions between law enforcement and the recovery center. Finer granularity (e.g., individual session keys), on the other hand, allows greater control (e.g., the key for a particular file or session, or only sessions that occurred within a particular time frame), but requires more frequent interaction with the recovery center (and increased design complexity).

Combining this with the previous articulation of granularity of signature keys and confidentiality keys, if a coarse granular key is lawfully accessed, no future or past signature can be trusted, defeating the primary goal of authentication services. If signature keys are separated from decryption keys, and only coarse decryption keys are accessed lawfully, then all past and future communications of that individual may be accessed, regardless of the limitations of the warrant. The experts main point, however, is that designing a more accountable system increases costs; designing a course granularity system also increases the risks.

From the above discussion, the report's conclusions are that

> (k)ey recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature. The massive deployment of key-recovery-based infrastructures to meet law enforcement's specifications will require significant sacrifices in security and convenience and substantially increased costs to all users of encryption. Furthermore, building the secure infrastructure of the breathtaking scale and complexity that would be required for such a scheme is beyond the experience and current competency of the field, and may well introduce ultimately unacceptable risks and costs.

These conclusions were supported by the findings of other researchers, including a report commissioned by the Canadian Government to Entrust Technologies (Lloyd and Oorschot 1998), and even a report from the NSA (National Security Agency 1998).

The U.S. cryptography policy forced industry to find solutions regardless. Some did develop key recovery, through interpreting the requirements differently.

5.3.3 Entrust

Entrust Technologies is an Ottawa-based provider of Internet security solutions and services. Because they have a U.S. office in Texas, however, the firm is subject to U.S. regulations.

Entrust is famous in the field of cryptographic technologies and services because of two particular product developments. First, it is one of the leading developers of Public Key Infrastructure solutions. Secondly, while Entrust defines PKI to also includes key recovery as an essential component (Curry 1997), unlike other contemporary definitions.

> An organization must be able to retrieve encrypted data when users can no longer access their decryption keys. This means that the organization to which the user belongs requires a system for backing up and recovering the decryption keys. There are two reasons why key backup and recovery are important to organizations. The first reason is that users forget passwords. (...) The second reason is that users may lose, break, or corrupt the devices in which their decryption keys are stored. (Curry 1998, p.3)

Entrust's interest in key recovery predates the U.S. policy discourse, however. Entrust began developing key recovery applications in 1994. As stated in an interview with the Vice President, Brian O'Higgins, Entrust supports the Gladman (1998b) differentiation between commercial and law enforcement key recovery, and in turn supports commercial key recovery. "We follow the market."

Key recovery within Entrust applications relies on the use of two key pairs for each user. One key pair is created for encryption/decryption, and the second keypair is for signature/verification. Entrust articulates the use of separate keypairs as 'business requirements', being

> ? support for key backup and non-repudiation
> ? support of different algorithms for encryption and digital signature
> ? support for updating encryption key pairs and managing decryption key histories, and updating signing key pairs and destroying signing keys
>
> (Curry 1998, p.1)

Signature keys are never backed up (Curry 1998, p.5), while decryption keys may be.

> Unlike encryption key pairs, there is no technical or business requirement to restore previous signing key pairs when users forget their passwords or lose access to their keys. In these situations, the secure solution is to generate new signing key pairs for users. (Curry 1998, p.7)

Entrust draws a careful separation between key recovery and key escrow within their documentation.

> (... C)ommercial requirements for key backup and recovery can be completely separated from law enforcement requirements for "key escrow"(...). Key backup and recovery requirements (...) focus on fundamental commercial needs that exist regardless of law enforcement requirements. (Entrust Technologies 1998b)

Entrust is very careful in its wording: key recovery is not key escrow. They do not say whether their version of key recovery is in law enforcement's interests necessarily.

Looking specifically at their solution, their claims are supported. Session keys are not collected, and key backup is a localised phenomenon.

> Flexible key recovery policy - Provides a secure and flexible per-operator policy to control which administrators can recover users, which users can be recovered by whom, and whether multiple authorizations are required to initiate key recovery. (Entrust Technologies 2001)

The Entrust solution is stated to be designed for the enterprise environment.

> Entrust's Enterprise Key Recovery gives corporations the ability to deliver only the relevant decrypted data to law enforcement officials or other third parties. Additionally, this feature provides protection to employees since corporations define the number of system administrators required to set users up for key recovery. (Entrust Technologies 2001)

The design also allows for keys to be identified as *compromised*.

The recovery administration service requires a senior security officer of the organisation to log in using two passwords -- the keys are multiply encrypted in an archive and under the administrator's key, in accordance with the local policy settings (Curry 1998, p.3). Importantly, this recovery/backup feature may be turned off.

The process model is such that the user is always alerted to alterations and administrative access to keys. O'Higgins did acknowledge that it is possible to access keys surreptitiously when they are stored on a backup server, but is not common practice. Also, session keys are

not stored, O'Higgins argued, as there are no commercial requirements for session key recovery. As a result, Entrust key recovery applications are not useful for intelligence purposes; as access requires localised intervention through the security administrator, it cannot be done surreptitiously. For law enforcement purposes it is not useful as the user will be notified of the key being accessed, unless it is accessed over the backup server.

There is some controversy within the discourse whether the Entrust solution to key recovery is actually a system that meets the interests of law enforcement. Gladman argues that

> Companies offering key recovery products should adopt the (commercial key recovery) model (...) in place of the (domestic key recovery or export key recovery) model (...). That this is possible has been demonstrated by both Entrust Technologies (Canada) and PGP Inc. (U.S.), both of which appear to offer products of this form (...). Of course these products may have other desirable (or undesirable) security features but they do appear to have adopted a key recovery strategy. (Gladman 1998b)

Denning and Branstad (1997), in their report on the growing market acceptance of the government policies, see it differently, however. "(Entrust's) commercial product archives user's private encryption keys as part of the certificate authority function and public-key infrastructure support." As a result, they classify, favourably, the Entrust model as "recovery of communications, files and other stored data", but accept that session keys can not be recovered. While key recovery may be possible and law enforcement may be able to access the keys, this is because it was seen as a commercial requirement, and not designed specifically because of policy issues.

5.3.4 PGP and its ADK

The story of Pretty Good Privacy (PGP) is long and dramatic, and covered elsewhere (Garfinkel 1994; Levy 2001; McCullagh 2001). In short, PGP was developed by Phil Zimmerman in the early 1990s. It is an encryption application created ideally for email but also applies to file and disk encryption, originally using a hybrid cryptosystem based on *RSA* and *IDEA* (a 128-bit symmetric algorithm). Zimmerman's stated intention for creating the application was so that human rights workers could communicate in privacy without being illegally wiretapped and persecuted (McCullagh 2001).

In the early 1990s someone placed a copy of PGP on the Internet and it was free for download anywhere in the world with access. One of the reasons for this action, according to Levy's research (2001, p.197) was to invalidate a U.S. Senate bill that required backdoors to be built into all encryption programs. The source code was exported on paper and

scanned into computers to recreate the software outside of the U.S., and thus making its distribution legal. Some speculate that close to a million copies of the various versions of PGP have been downloaded world-wide, to the discontent of law enforcement officials (Freeh 1998).

Zimmerman decided to sell the application for profit, but when that failed he sold the company to Network Associates (NAI). At first this was heralded: a company as large as NAI could distribute the application even more widely, and possibly on commercial scale (Markoff 1998).

Network Associates at that time was working with other companies within the *Key Recovery Alliance* (KRA) to come up with key recovery solutions to meet government policy requirements. NAI had also recently purchased Trusted Information Systems, a company known for key recovery solutions. The fact that a company that was a member of the KRA also owned PGP eventually generated concern in the community of opponents to the existing policy. Zimmerman responded to these concerns.

> NAI has no plans to incorporate TIS's key recovery technology in any version of PGP, including our business versions. I have discussed this point with NAI management. (Zimmerman 1998)

NAI shortly thereafter left the KRA, but later rejoined (Wired News 1998), until the KRA itself disappeared.

Before the sale of PGP, data recovery was introduced by Zimmerman (and not NAI, as opposed to popular belief (Zimmerman 2000)). Versions 5.5 through to version 6.5.3 included the option for *Additional Decryption Keys* (ADKs) that permitted authorized extra decryption keys to be added to a user's public key certificate. This would allow companies to add another key to an employee's certificate in order to maintain the ability to access all communications. As Zimmerman later commented,

> The ADK feature was designed in 1997 to be a kinder, gentler alternative to key escrow for companies to use for employee's keys. (...) This satisfied a major requirement from our corporate customers for a mechanism of handling what happens when an employee is not available to decrypt the file, perhaps because he's on vacation, or died in a plane crash, or simply forgot his passphrase. It is so much better than key escrow because it requires the consent of both the sender and receiver to use the feature. It is highly visible to the sender, and asks his consent before proceeding with the encryption.

A different interpretation was presented by critics.

> (N)o access to the user's secret key was needed to recover the plaintext by decrypting the message with the ADK, a key which was

> clearly meant not to be in control of the user. Criticism has focussed on the fact that the link between a user's key and a third-party-ADK creates a perfect means of surveillance of the user's encrypted communication and data, which would effectively result in third-party-access to plaintext as had been pursued previously by key escrow. Same effect but presented to the user in a nicer way. (Senderek 2000)

The community opposing U.S. cryptography policy was enraged, foreseeing government policy changes that would require all individuals to include law enforcement agencies keys as ADKs. This did not happen.

A fault was later discovered in the way that the ADK option was implemented.

> The attacker who modifie(s) the certificate can obtain the plaintext from this ciphertext. PGP does not correctly detect this form of certificate modification because it fails to check if the ADK is stored in the signed (hashed) portion of the public certificate. As a result, normal methods for evaluating the legitimacy of a public certificate (fingerprint verification) are not sufficient for users of vulnerable versions of PGP. (CERT 2000)

Zimmerman was again requested to respond to this situation.

> Some of the postings on the Internet about this subject have portrayed this bug as a back door in PGP. Let me assure you, it is nothing of the sort. It is a bug (and we have now fixed it). An especially embarrassing bug, because it is in a feature that some people have objected to even when everyone thought it was working correctly. (Zimmerman 2000)

PGP was patched soon thereafter. As Bruce Schneier commented,

> Way back in 1998 a bunch of us cryptographers predicted that adding key escrow would make system design harder, and would result in even more security problems. This is an example of that prediction coming true. (in McCullagh 2000)

Schneier, and other in the epistemic community, interpret the fault as the technology objecting; others may see it as intentional design by the NSA; others may see it as a mistake. Regardless, the technology was faulty, and for an application that is designed for security, this is problematic.

5.4 Enrolling Industry and Export Controls

Efforts to generate domestic controls through the Clipper chip, software key escrow, and then through key recovery solutions generally proved to be failures. Subsequently, the government tried to make it in the interests of industry to develop cryptographic systems and infrastructure that will still in some way meet the interests of national security and law

enforcement agencies. A sophisticated regulatory regime was selected as the means to achieve both domestic (law enforcement) and foreign (national security) policy goals.

5.4.1 Background to Export Controls

Export controls in theory are an extension of foreign policy (Heinz 1991). Export controls of cryptography have been supported in order to maintain the ability of intelligence gathering worldwide (Campbell 1999a). As with all export controls, the purpose of controlling the export of cryptography was to prevent or delay the possession of capabilities of secure communications by adversaries or even prospective adversaries (Olmer 1984). This tactic changed in the cryptography policy discourse, as the traditionally foreign policy-oriented export controls were designed to serve domestic interests.

There are costs to export controls. A report from the Center for Strategic and International Studies (1994, p.39-45), while not dealing specifically with cryptography, outlines three forms of costs: transaction, administrative, and opportunity. Transaction costs relate to the burden, penalties, and time delays involved in applying for export licenses. Administrative costs are related to the investments that business make in new administrative or business processes, procedures, or systems to assure that their exports comply with the export regulations. Finally, the opportunity costs involve loss of sales due to delays, sales not pursued due to uncertainty of gaining licenses, sales lost to foreign competitors who have fewer regulatory barriers, and a depletion of long-term reinvestment into research and development of future technologies. As we will see below, these concerns were raised particularly by software companies and industry alliances.

5.4.2 The Legal Environment for Export Controls

In controlling the export of arms and munitions from the U.S., there are two key items of legislation: the Export Control Act of 1949 (ECA) intended to regulate munitions, and the Export Administration Act (EAA), intended to regulate so-called *dual-use products*, i.e. products with both military and commercial applications. Cryptography was controlled within each of these. From the ECA came the International Traffic in Arms Regulations (ITAR (1992)), in which the U.S. Munitions List (USML) is defined and specified, and administered by the Department of State. The EAA meanwhile, is the legislative basis for the Export Administrative Regulations (EAR), which define dual-use items on a list administered by the Department of Commerce.

The ITAR was traditionally the regulatory act that controlled exports of

> all cryptographic systems, equipment, assemblies, modules, integrated circuits, components or software with the capability of maintaining secrecy of confidentiality of information or information systems. (ITAR (1992))

ITAR also regulates information *about* cryptography, such as algorithms and research papers, under *technical data* (NRC 1996, p.115).

Created in the 1940s, export controls were used to protect the economy, i.e. to prohibit the export of scarce resources. In 1948, ITAR became an instrument of national security; and was formally instituted when the Department of Commerce placed most exports to the Soviet bloc under mandatory licensing control as the USSR withdrew from the Marshall Plan conference (Heinz 1991, p.11). The intentions behind export controls were thus extended from the protection of domestic economy from excessive drain of scarce materials; to furthering the foreign policy of the U.S. to aid in fulfilling its international responsibilities. Even at that time, however, the ECA had a sunset clause set for 1953, but was extended periodically until 1969, when the act was transformed: the protection of scarce resources had virtually disappeared, and national security became the motivating factor (Heinz 1991, p.11).

As trade-related issues grew, particularly due to the Cold War, however, a strain appeared in the mission of the Department of Commerce, between the promotion of *strategic trade* and the controlling of exports (Heinz 1991, p.13). The resolution of this conflict was attempted in 1985 through the creation of the Bureau of Export Administration (BXA), to separate the Department of Commerce's export control function from its trade promotion function (Heinz 1991, p.21). The ITAR munitions list continued to be managed by the Department of State. According to Heinz, with reference to all export controls,

> A system that builds in mutually incompatible missions within the principal agencies responsible for carrying out export control policies, rendering them unable to balance --much less manage -- the natural tension between national and economic security interests. The Department of Commerce is commercially unable to balance and manage trade promotion and trade controls. (...)The Department of State is diplomatically unable to balance foreign policy goals and technology transfer programs. The National Security Council staff is conceptually unable to balance policy coordination and policy leadership. U.S. Customs and Commerce cannot agree on enforcement cooperation abroad. (1991, p.39)

This is an indication of the conflicting interests of government agencies. The resulting question of who is to regulate is non-trivial.

The ECA was updated again in 1979, the new act called for a better understanding of 'foreign availability' as a burden to U.S. industry (Heinz 1991, p.20). This was a result of the

realisation that new centres of excellence have challenged U.S. superiority in research and development.

> (A)s foreign industry has become more capable, the flow of technology has become more bidirectional, with the U.S. steadily increasing its consumption of foreign technologies and engineering know-how through imports, license agreements, and foreign direct investment. (...) The largest U.S.-based firms, with operations around the world, have taken this process of integration even further, conducting business on a global scale and seeking out new technologies and opportunities wherever they may be, irrespective of borders. (...) As a result, technology, often in the form of pure information, has become increasingly difficult to contain within a nation's frontiers. (Irwin 1993, p.67)

In 1977 this resulted in a change to the regulations allowing the President to manage controls extraterritorially, i.e. "subject to the jurisdiction of the U.S. or exported by any person subject to the jurisdiction of the U.S." (Irwin 1993, p.112).

Conflicting jurisdictions and interests gave rise to a conflicting legal regime. Concerns often arise about free speech and other such rights and freedoms and their conflict with export controls. According to Irwin, the issue of 'technical data' seemed a likely conflict.

> For the purposes of the EAA, an export of technology occurs not only when there is a shipment of technical data out of the U.S., but when technical data is imparted to a foreign national by means of oral exchanges of information and provision of services, training, or visual inspection. Thus, where a foreign national is involved, a transmission of information wholly within the U.S. may constitute a prohibited export. (Irwin 1993, p.120)

In jurisprudence, such as *New York Times vs. the U.S. Government*, the Supreme Court made its conclusions based on the seriousness and the immediacy of the danger, whether the information was otherwise available, and whether an injunction would have been effective (Irwin 1993, footnote 741).

Prior restraint of speech is unconstitutional, but according to an Assistant Attorney General in 1981,

> dissemination of technical data for the purpose of promoting the sale of a defense article or service would appear to be commercial speech, and the constitutional barriers to prior restraints may well have a diminished applicability to the dissemination of technical data in that context. (Olson 1981)

This principle was brought up in *Bernstein v. United States Government* where Daniel Bernstein sought to post source code (human readable) of a cryptographic algorithm on the Internet, without any commercial intent (Patel 1999). Among the interesting questions raised were: is

code speech? are programs speech? are algorithms speech? The response from the court in a 1999 ruling was that code is in fact a form of speech (McCullagh 1999).

5.4.3 Software Export Controls

If a software company wished to export a product that fell under the regulations in the 1990s, the company was obliged to apply for a license from the U.S. Government. According to the special report of the Association of Computing Machinery,

> Quantifying lost sales is difficult. One can count the number of export-license applications denied or withdrawn, but that misses the mark. Foreign customers who know that the products they want will not receive U.S. export approval are unlikely to waste time approaching American companies. At the same time, export controls are sometimes cited as the reason for a lost sale when the facts are otherwise. The Department of State export-license statistics give only a partial picture of the situation. (USACM 1994, p. 57-58)

Meanwhile the NRC Report states that the export control regime is an increasing impediment to the information security efforts of U.S. firms competing and operating in world markets, developing strategic alliances internationally, and forming closer ties with foreign customers and suppliers (NRC 1996, p.8).

There is always the option, as Netscape and Microsoft have pursued in their browsing software, to provide two different applications for the two geographic markets (domestic vs. foreign). However, the ACM committee states a case where this caused the early death of a product. Digital Equipment Computer developed a *DES*-based application, *DESNC*.

> (G)overnment policy did not permit the general export of DESNC. There was still a domestic market. But Digital Equipment marketing managers feared that publicizing DESNC, without the availability of a comparable product for export would alienate Digital Equipment's foreign customers by suggesting that unencrypted Ethernet technology is vulnerable (...), but without providing a solution for non-U.S. customers. A high-cost item, DESNC was unlikely to be a big seller in either foreign or domestic markets, but an inability to offer this product on a global basis posed a critical customer relations problem. These concerns, in combination with the negative publicity it would bring to Ethernet technology, were deemed unacceptable trade-offs. (USACM 1994, p. 59)

The NSA agreed that export controls may be a *hindrance* to the incorporation of strong encryption algorithms in *domestic* applications due to this problem of dual versions (National Security Agency and US Department of Commerce 1995, p. ES5). Consequently, export controls are also dual-use: they inhibit the growth of cryptographic software applications in both foreign and domestic markets, in turn meeting the interests of law enforcement agencies by reducing the domestic availability of strong cryptography.

In October 1996, Vice President Al Gore announced the *liberalisation* of export controls on cryptographic products. The previous controls restricted export of cryptography any stronger than 40-bit key lengths; the new policy permitted export of 56-bit products upon receiving a license.

These licenses were to be updated every six months, however; and the only way that the licenses would be updated after two years is if the companies developed key recovery into their products by then. That is, after a two-year period of allowing the export of 56-bit products, no product would be allowed for export that does not incorporate key recovery. An additional incentive was that "no key length limits or algorithm restrictions will apply to exported key recovery products" (Office of the Vice President 1996).

In November of that same year, President Clinton removed encryption from the ITAR, and placed cryptography export controls generally under the jurisdiction of the Department of Commerce (DoC), in order to promote the cause of e-commerce (The White House 1996b). The Department of Commerce and its BXA then became active players in the discourse. Some within industry were sceptical, however. According to the BSA and Microsoft,

> (W)hile this transfer of jurisdiction should have resulted in easier exporting, the Administration continued to impose many of the same stringent national security and foreign policy controls traditionally applied to munitions! For example, the provisions minimizing export controls when U.S. companies demonstrate the availability of similar products from foreign sources, or the publicly availability of such products, are deemed inapplicable for encryption items. In short, the forum changed, but not the substance. (Rubinstein 1997)

In a further announcement, the position of a special envoy for cryptography, or *crypto-tsar* was formed. This person would be responsible to "promote the growth of international electronic commerce and robust, secure global communications in a manner that protects the public safety and national security" (The White House 1996c). Critics viewed the appointee, Ambassador David Aaron, as someone who would force other countries to implement domestic key recovery policies, thus ensuring a market for U.S. products, in a procedure that Banisar and Schneier (1997) refer to as *policy laundering*.

Industry was thus provided with incentives to develop key recovery products; the transaction, administrative, and opportunity costs would act as an incentive to deploy these products domestically. Now, companies were forced to develop key recovery systems for export, and in turn, due to the dual-version dilemma for foreign and domestic markets, they would probably be marketed for use within the U.S. In 1997, Louis Freeh of the FBI supported this move claiming it to be

> from our point of view, a very positive development in the sense that it begins to create incentives, incentives which are being taken advantage of particularly by the financial community and institutions to get their products distributed where they want them distributed, but also give us the commitment, although not really an enforceable commitment, but a commitment nevertheless, that they will also construct and develop key recovery products. (...) (T)his policy overall (...) is the incentive which is moving toward an infrastructure which we can take advantage of. (Freeh 1997)

Almost all interests were being met, to some extent. Companies could now export products; national security interests were not disturbed, since 56-bit encryption is still weak enough to be brute-forced by the NSA and key recovery could possibly include key recovery for access by intelligence agencies; and the FBI was content that domestic application seemed imminent; all while the DoC, through Aaron, was pushing for the key recovery market abroad.

Industry's scepticism continued. Microsoft's lawyer, representing the BSA stated that

> (t)he Administration's policy is an attempt to use export policy to control the domestic use of encryption. (...)As I explained earlier, the domestic software industry makes approximately one-half of its revenues through exports, and customers are increasingly demanding uniform encryption capabilities; therefore, most mass-market software and hardware is designed to offer the same encryption capabilities both domestically and abroad. Thus, this new policy effectively forces domestic encryption hardware and software into the Hobson's choice of maintaining separate products lines for the domestic and international markets or complying with the Administration's export restrictions. (Rubinstein 1997)

The results of this policy can be seen in two particular technologies discussed in detail below, being Lotus WFR and Microsoft CAPI.

There was also a further development in the 1996 policy shift: strong cryptography without key recovery was liberalised immediately for use only within the specific industry sectors of health and finance (The White House 1996a). The next subsection will look at the sectoral liberalisation, which will lead to §5.4.5 and §5.4.6 that look specifically at two policy-constructed cryptography implementations.

5.4.4 SSL -- Intended and Unintended Step-Up

With liberalisation of strong cryptography for specific sectoral, solutions needed to be developed that permitted strong cryptography for specific use while preventing general use. One solution, developed by both Microsoft and Netscape for use in their browsers and with Secure Sockets Layer (SSL, c.f. Rescorla 1999) was *server gated cryptography* (SGC)

(Microsoft Security Advisor 1998a) or *step-up crypto* (Netscape 1999). For the sake of simplicity, I will use the term *step-up crypto*.

Traditionally SSL would set up a session between a client and a server using either 40-bit or 128-bit session keys.[4] If a user was in the U.S. and had a strong-cryptography-enabled browser, and the server was also in the U.S. with a strong-cryptography-enabled server software, only then is a 128-bit session key be established. If either of the parties had an 'export'-version of the software, or both simultaneously, then the established session key is 40-bit.

Through digital certificate design and issuance, these companies managed to create a certification infrastructure that would allow for differentiable-strength cryptography depending on the form of the certificate, in turn depending on the industrial sector. For example, Verisign, a certification services company, received approval for the export of services that would issue *Global Server IDs* that would allow **only** financial institutions to communicate with their clients world-wide who are using Netscape and Microsoft browsers using 128-bit encryption (Verisign 1997). That is, a 128-bit session will be established under the following conditions,

- servers located in the U.S. and browsers located globally, when the servers have a VeriSign Global Server ID
- browsers located in the U.S. and servers located overseas, when the servers have a VeriSign Global Server ID
- browsers and servers located overseas, when the servers have a VeriSign Global Server ID

(Verisign 1997)

The determination of which institutions receive these IDs is up to the service provider (e.g. Verisign), the technology, and the U.S. Government.

- Global Server IDs will only be granted to legitimate businesses that meet the necessary U.S. government qualifications
- Global Server IDs can not be obtained under false pretenses
- The full lifecycle services offered by VeriSign, including 24 hour, 7 day a week revocation, will ensure the integrity of the program

(Verisign 1997)

This scheme ensures that privileges can be endowed and removed at the request of the U.S. Government (Verisign 1998). To receive such a certificate, the institution usually has to present a Dun&Bradstreet DUNS number or an American Banking Association number, or

through state, provincial, or national governments requesting approval from the Department of Commerce (Microsoft Security Advisor 1998b).

Microsoft, Netscape, and Verisign, among other companies, were quick to market this capability. Believing that end-users were concerned with key lengths, step-up crypto became part of the marketing range. Barclays Bank was one of the first UK institutions to receive the step-up enabled server certificate.

> We recognise that in the past some people had concerns with the security of on-line services. That's why Internet Banking uses the latest encryption technology licensed from the U.S. Government to prevent unauthorised access to your records. (Barclays Bank 1999)

Step-up crypto and the resulting *cartelisation* (Lash 1997) of cryptographic products and service providers were rendered moot as foreign availability increased, however. Two such cases are worth mentioning in the scope of strong-SSL, *SSLEAY* and *Fortify*.

SSLEAY is a SSL-compatible protocol developed by two security experts, operating from Australia, using publicly available documentation (Hudson and Young 1998). Interpreting international policies on cryptography and intellectual property rules, the developers created a *legal* strong crypto-enabled implementation of SSL that is available for free. The implementation was made available on-line and mirrored on servers around the world. Some of the more popular web servers at the time, such as Stronghold, implemented SSLEAY instead of SSL (to the envy of the BSA (Rubinstein 1997)). This eroded the privilege of the banks in allowing for strongly encrypted commercial transactions for all.

Commercial providers also began to make stronger implementations available. Baltimore Technologies, an Irish cryptography and security firm, began making a software patch, *Fortify*, available for download worldwide that allowed for Netscape browsers to be upgraded to strong encryption (Cryptix 1998), "redressing the security hole" in U.S. products (Baltimore Technologies 1997). While I am aware of the Baltimore patch due to personal experience, I am less able to confirm Gladman's claim on *ukcrypto* listserv (1998a) that a similar patch for Microsoft's browser could be downloaded from an FTP site in the Netherlands. Baltimore also created their own implementation of SSL that enabled strong cryptography (IDG.net 1997).

While foreign availability increased, the regulations also became more careful: methods needed to be devised to ensure that patches could not be distributed by hackers, enthusiasts, or other companies. This arose particularly in the Microsoft CAPI solution.

5.4.5 Extra-jurisdictional Microsoft and CAPI

Microsoft develops the most widely sold operating systems available, and in turn has an interest in developing security solutions. These solutions, according to a George Spix, a senior solutions architect in Microsoft, are created because there is a market incentive. Building products to meet government interests may collide with this market-facing ideal. Moreover, building the same product differently for each jurisdiction is already difficult and costly -- language translations are hard enough, but coding changes are even more difficult. According to Spix, Microsoft tried to 'remove ourselves' from the challenge of developing policy-specific solutions by developing Crypto API, which helped to 'cover (our) liability'.

Microsoft has been active in the cryptography policy discourse, by generally opposing key escrow. As articulated to its consumers,

> Key escrow encryption is not a market-driven solution and it raises serious privacy concerns for many customers. It is also new, undeveloped, untested, and uncosted, and it will take a long time to be worked out. Additionally, customers have expressed hesitation about mandatory key escrow, especially if they have to give the keys to the government or a government-selected third party. Therefore, we are not actively adding support for key escrow in our products and technologies. (Microsoft Corporation 1996)

Microsoft supports the work of the BSA and other industry organisations, and was active in the U.S. Congress (e.g. Rubinstein 1997).

Siding with the results of the NRC report, Microsoft's legal counsel testified that the current controls were problematic due to the weak keys, and the challenges of foreign availability.

> (O)ur U.S. customers need to operate globally, and foreign customers are not satisfied with "crypto lite." Therefore, we need export relief so that we can sell a single product worldwide. (...) We still need 128-bit relief for Internet financial applications. This is not a future need -- customers today reject (DES) and demand 128-bit protection for financial data. If we cannot supply these products, foreign vendors will (...). (Microsoft Corporation 1996)

Developing multiple software distributions for the same software application was difficult. As explained to me in one example, two French-language editions of software had to be developed: one that met the Canadian regulations on cryptography (no domestic controls), and another that met France's controls (no crypto allowed at first, then 40-bit). Testing costs increased; because testing must be done for all configurations, e.g. Win98 40-bit, Win98 128-bit, Win98+IE5 128-bit, Win98FrenchCanadian, Win98 France, etc. and likewise for SSL, including the additional issues relating to server gated cryptography. According to Brian LaMacchia, the team developer of cryptography solutions at Microsoft,

the test "matrix is blowing up", and as a result, "guys in the NT build don't like us. (...) We complicate their lives." Even at the time of interview, it was seven months after the December 1998 changes to export controls where 56-bit encryption could be exported freely, the latest updates to the software had not yet included the changes. Although the code was ready in January 1999, it was past the company's development deadlines. "Government approval came too late for our processes. (...) If (the regulation changes) came out in October 1998, fine, but they didn't." Testing would have taken too long, and would have delayed the entire product. "I ended up pissing off a lot of customers" who wanted 56-bit encryption, said LaMacchia.

This situation was affecting domestic use of strong cryptography as well. Microsoft could not develop the software first, and then localise, i.e. reduce, the key-lengths afterwards. This is because of the agreements with the Original Equipment Manufacturers (OEMs), as it would require the OEMs to know exactly where their computers were going to be sold prior to software installation, which was infeasible. The result, rather, is that all initial implementations would have 40-bit key lengths, and then upgrades occur once domestic customers become aware of the weak strength and download patches. That is, by default all users were using weak cryptography, and only those who took the initiative could upgrade.

On CAPI

Developing an Application-Program-Interface (API) was another solution to managing regulatory challenges. An API is "between the application software and the application platform, across which all services are provided" (NSACOCAPI 1996). The purpose is to support interoperability, and Crypto-API, or CAPI supports cryptographic applications so that they can be embedded within Microsoft operating systems. According to the NSA,

> Until recently, the integration of cryptographic functionality into application software has required that developers tightly couple the application to the cryptographic module. This approach forces each new combination of application and cryptography to be treated as a distinct development effort, and does not provide the modularity and maintainability expected of commercial products. An approach that can provide flexibility and cost savings is the use of a standardized Cryptographic Application Program Interface (CAPI) suite. (NSACOCAPI 1996)

Microsoft's CAPI accomplishes this using cryptographic modules, or Cryptographic Service Providers (CSPs; see figure 5.3).

> CryptoAPI provides an abstraction layer that isolates you from the algorithm used to protect the data. An (CSP) will refer to contexts and keys and make calls to special functions that act as drivers for the encryption servers installed on the machine. (Esposito 1997)

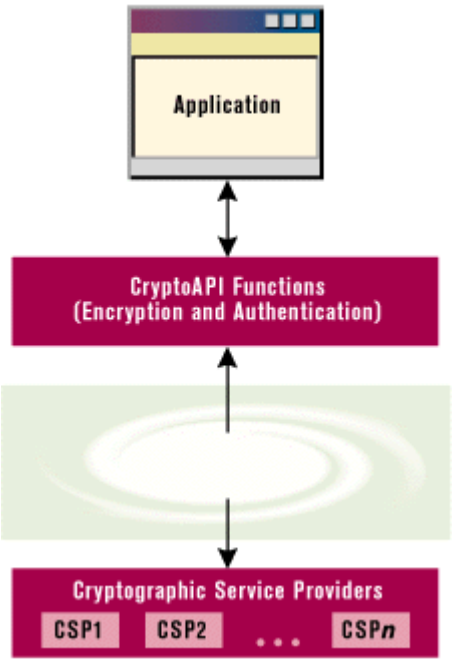

Figure 5.3 Abstraction as presented in (Esposito 1997)

Comparing design articulations from LaMacchia, a review of the development documentation, and associated research leads to the conclusion that it was designed specifically for export. LaMacchia argued that the benefit of this design was that one set of base code could be implemented for every implementation worldwide, and then localisation based on national policy was possible through the CSPs.

The design was not so simple as to allow any CSP to plug in to the API -- a specific design constraint existed. According to Gladman (1996), a poorly understood component of U.S. export controls prohibits 'crypto-with-a-hole'. Crypto-with-a-hole is a design where applications that lack cryptography at the time of export but feature a hole that can be easily loaded with components at a later date (Kerstetter 1998).

> (E)xport control laws not only constrain cryptographic and related products but also any products which are specifically designed to interface to, or integrate with, cryptographic products. In effect, therefore, the very principle of openly available Cryptographic Application Programming Interfaces (CAPI) is in direct conflict with the existing export control provisions in many countries. (Gladman 1996)

Crypto-with-a-hole is not exportable, and so Microsoft had to design a more complex system.

> It is important to recognise that this situation is not of Microsoft's making. In publishing and promoting a CAPI for use with their products Microsoft has gone as far as it can under U.S. law to establish an improved basis for the provision of cryptographic

> information security when using their products. The procedures (...) are the provisions which the United States administration has imposed in order that Microsoft can offer their operating systems in world markets without being subject to U.S. export controls. (Gladman 1996)

Microsoft designed CAPI so that it would only work with CSPs approved for export by the U.S. Government.

For export versions of such a solution, the API would still be there, but the algorithms and key-lengths components would be missing. It would be trivial for someone outside of U.S. to create these components, and thus make Microsoft applications operable with strong cryptography, enabled by the work of Microsoft in developing the API (see figure 5.4). Such an API contravenes U.S. law.

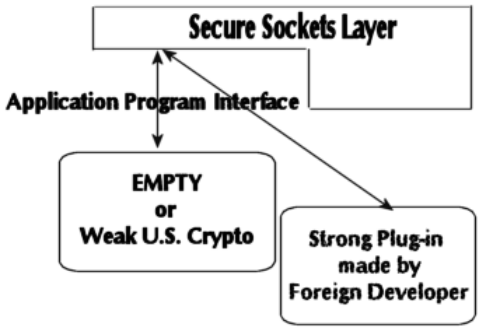

Figure 5.4 API with a hole

Microsoft's solution was to design CAPI in such a way that it required that the components CSPs would have to be signed digitally by Microsoft. Without the signature, the CSP would not work (see figure 5.5).

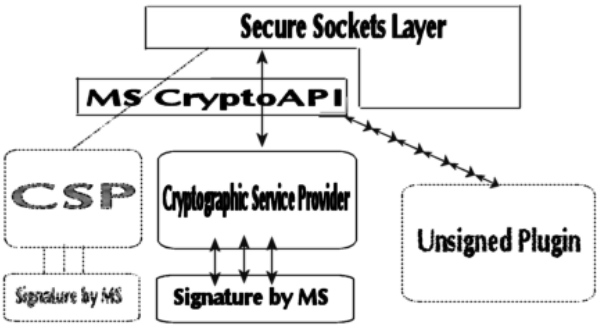

Figure 5.5 CAPI with Signed CSPs

There were two reasons for this, according to Gladman,

> Microsoft has announced its intention to digitally sign supplier provided CSP modules for two reasons:
>
> - To allow the integrity of supplied CSP modules to be checked by the operating system;
> - To ensure that CSP modules comply with United States export controls on cryptography and cryptographic interfaces.
>
> (Gladman 1996)

Each CSP would have to be designed to work in 128-bit mode for domestic use, and 40/56-bit mode for export (depending on the export regime in place).

All of these considerations were no longer an issue for Microsoft: each CSP developer would have to get approval for export from the DoC BXA, and only then would Microsoft digitally sign the CSP.

The signing process is by no means simple, however. According to LaMacchia, it is a two-man operation, using a highly controlled signing key stored in a vault with 24-hour protection. LaMacchia commented that there was a large cost associated with this operation, and maintaining records was also challenging. The content of the CSP is irrelevant to Microsoft: "we don't want to know." Rather, the signing protocol involves verifying the approval of the U.S. government for a given CSP.

Developing CSPs was not easy, though. LaMacchia claims, "CSP Developer Kits (CSPDK) distribution is a real pain", as each distribution had to be checked against the "bad persons list", and this was still managed by the Department of State.

Even after the new policy removing cryptography from ITAR, the CSPDK remained on the munitions list, and signing of CSPs for export is considered a 'defense service'; both regulated by ITAR (Microsoft Corporation 1996). The rest of CAPI is regulated by the Department of Commerce Bureau of Export Administration.

CSP developers first need to get a CSPDK, which could be challenging if they are outside of the U.S. Then signing the CSP is a challenge, particularly for foreign CSP developers, but Microsoft claims that it will sign them if allowed under law (Microsoft Corporation 1996).

Gladman (1996) summarises this situation

> (...) CSPs Produced in the United States and Canada for Domestic Use
>
> - The CSP Software Development Kit (SDK) is freely available without export control.
> - Microsoft will sign a CSP module without U.S. (or other) government involvement.
>
> CSPs Produced in the United States and Canada for Export
>
> - The SDK is freely available without export control.
> - Microsoft will sign a CSP module given evidence of United States government export approval.
>
> CSPs Produced Outside the United States and Canada
>
> - The SDK is subject to U.S. government export control.
> - The Microsoft signature on a CSP is deemed to be a 'defense service' provided by Microsoft to an overseas supplier and as such it is subject to the provisions of United States export control laws.

This last case is most interesting: export controls in the U.S. apply to all CSPs, regardless of the country within which they are developed. This type of extra-jurisdictional power is a design implication CAPI, inviting the U.S. government into the functional loop of authorising applications. To defend against any accusations of crypto-with-a-hole, maintaining the integrity of CAPI was essential; even if it meant creating additional burdens and extra-jurisdictional reach for U.S. policy.

The NSAKey Controversy

Within CAPI, there is a key that verifies the signature of the CSP in order to ensure that a CSP has been signed by Microsoft, thus asserting that there was approval from the U.S. government. Any tampering with this signature key would result in CAPI failing to operate. In 1999 a researcher in Canada reverse-engineered the code of Microsoft NT 4.0 and found that within CAPI there were two such verification keys, one entitled "KEY", the other entitled "NSAKEY". The name of the key caused an uproar with significant media attention, and growing concerns of a potential backdoor in CAPI made for the NSA.

The key does not allow for a backdoor, necessarily. Rather, the key is only a secondary key for verification of signatures of CSPs. After the media uproar, Microsoft came public with why this key existed. When CAPI had to be reviewed by the NSA prior to export, in accordance with export controls, the NSA apparently suggested that having only one signature verification key could be hazardous if that one key is lost. As a result, Microsoft

implemented a secondary key, and entitled it NSAKEY to represent where the idea had come from.

> This is simply an unfortunate name. (...) The keys in question are the ones that allow us to ensure compliance with the NSA's technical review. Therefore, they came to be known within Microsoft as "the NSA keys", and this was used as a variable name for one of the keys. However, Microsoft holds these keys and does not share them with anyone, including the NSA. (Microsoft Security Advisor 1999)

Experts weighed in and argued that because of the functionality of the key, it is unlikely that it can cause any harm.

> I see two possibilities. One, that the backup key is just as Microsoft says, a backup key. It's called "NSAKEY" for some dumb reason, and that's that. Two, that it is actually an NSA key. If the NSA is going to use Microsoft products for classified traffic, they're going to install their own cryptography. They're not going to want to show it to anyone, not even Microsoft. They are going to want to sign their own modules. So the backup key could also be an NSA internal key, so that they could install strong cryptography on Microsoft products for their own internal use. (Schneier 1999)

While some worried that the NSA could surreptitiously place CSPs on a computer that would work with CAPI but would disclose your keys, again experts responded with some doubt.

> Once a well-motivated adversary has gained control over a target machine, there are many more attacks - both more vicious and more subtle - than the replacement of a CSP module. (Zaba 1999)

Arguably, the key was not intended, by design, to reduce security.

A more interesting issue, however, was that the second key could be modified. The first key, KEY, could not be modified manually because CSPs would refuse to work with CAPI.

> The replaceability of the secondary key does appear to defeat the narrow security goal apparently represented by the requirement to gain export approval for cryptographic APIs. If we accept the aim of this U.S. government policy is to limit the usage of "strong" cryptography worldwide, then the ability to add arbitrary CSPs to so widespread a platform as Microsoft Windows would indeed undermine this goal. (Zaba 1999)

The effect is that all the controls within CAPI for only accepting signed CSPs upon receiving export approval are moot: the secondary key could be replaced with another signature verification key to work with CSPs that have not been signed by Microsoft (and presumably not received a license from the U.S. Government). This is crypto-with-a-hole

and in contravention with the export controls requirements. The response from Microsoft, according to a News.com article,

> (Microsoft) did not deny someone could replace the second key, but dismissed the significance. "If he wants to run his own crypto program under Windows NT, there is a far simpler way to do it -- write a higher level software program. (Wilcox 1999)

Zaba's analysis (1999) supports this view.

> Since the initial launch of the Microsoft CryptoAPI there have been three significant liberalisations of the export control regime.(...) One can therefore imagine that a replaceable secondary key might have been suggested to Microsoft during the technical review for export, and presented as a mechanism with advantages to both sides. A further advantage to Microsoft might be that, under suitable non-disclosure, they could share the information about the replaceability of the secondary key with other major customers who might want CSP signing capabilities under their exclusive control. Such an arrangement would both explain the name of the variable, and be consistent with Microsoft's vigorously stated position that neither the primary nor the secondary signing keys had been disclosed. (Zaba 1999)

In a sense, Microsoft was adhering to the regulations, and as the export controls changed and the knowledge regarding the second key grew, the effects became negligible.

5.4.6 Designing for the NSA -- Lotus Workfactor Reduction

Lotus, a subsidiary of IBM, has also been active throughout the cryptography-policy discourse. In Congressional testimony, the legal counsel, Melinda Brown, echoed the reservations of Rubinstein and Microsoft regarding the export controls regimes in the U.S.

> One of the most important features computer users are demanding is the ability to protect their electronic information and to securely interact worldwide. American companies have innovative products which can meet this demand and compete internationally. But there is one thing in our way - the continued application of outdated, unilateral, "munitions" export controls by the U.S. Government. (Brown 1996)

Her testimony articulated Lotus' problems with the 40-bit key length limits for export. Lotus called for policy that would

> ? permit the export under a Department of Commerce general license of software programs using the DES algorithm with 56-bit keys and other algorithms (...) at comparable strengths (with unlimited key lengths for key management);
> ? automatically increase key lengths two bits every three years given the reality of "Moore's Law" (...) (i.e., institute a Cost of Cracking Adjustment or "COCA");

> ? broaden existing licensing for programs using even stronger encryption (e.g. 128-bit encryption for financial applications);
> ? permit the export of software with "hooks," or Application Programming Interfaces, enabling foreign customers to "plug in" whatever encryption they may obtain and use in other countries; and
> ? remove remaining export control restrictions on non-confidentiality uses of cryptography (i.e. key management, authorization, integrity, signatures), on the personal use of cryptographic programs abroad by American citizens, and by U.S. multinational corporations.
>
> (Brown 1996)

There was no demand for complete liberalisation.

In a speech at the 1996 RSA Data Security conference, the president of Iris Associates, a subsidiary of Lotus responsible for security development within Lotus Notes/Domino, the Lotus flagship product, commented on the U.S. policy, and the technological options for implementing security.

> We talked to our customers about the administration's proposal, and the answer was very clear: our customers have said a resounding "no" to key escrow in Lotus Notes. They simply don't like the notion that they can't compute the additional risk and liability introduced by a third party holding the keys to unlock their data. Well, that left us in a bind. We need to provide better security for our international customers, but the government's proposal was clearly unacceptable to them. And because I didn't see a "silver bullet" solution -- or general export relief -- in the cards, I began looking for an interim solution that might allow us to ship a more secure product in the short term, while we continued to argue for substantial revision of national cryptography policy. (Ozzie 1996)

The solution was Workfactor Reduction (WFR), and gained approval of the U.S. Government, and since version 4.0 in 1994, was implemented in Notes.

In an interview with the team leader for the development of WFR in Lotus Notes, presented in (Kosheff 1997), Charlie Kaufman noted the challenge.

> (W)e had to go to great lengths to satisfy export criteria, while maintaining Notes' own 64-bit key scheme. They wanted us to implement a backdoor fix so the government could get in, but we didn't much like that idea, so we came up with an interesting alternative. We use 64-bits within the United States, which is considered fairly strong. In the exportable Edition, we also use 64-bits, but make 24 of those bits available to the U.S. government. (Kosheff 1997)

Every time a key is generated for batch encryption, it is a 64-bit key. If the application is operating outside of the United States and Canada, 24-bits of this 64-bit key is encrypted

with a public key and appended to the message. The private key component to that public key belongs to the NSA, and is kept secure at their facilities (Ozzie 1996). The result is that for the U.S. government (NSA specifically), the effort to decrypt ciphertext is reduced to the problems in brute forcing 40-bit keys, but for any other opponent, the effort requires the *workfactor* of 64-bits (see figure 5.6).

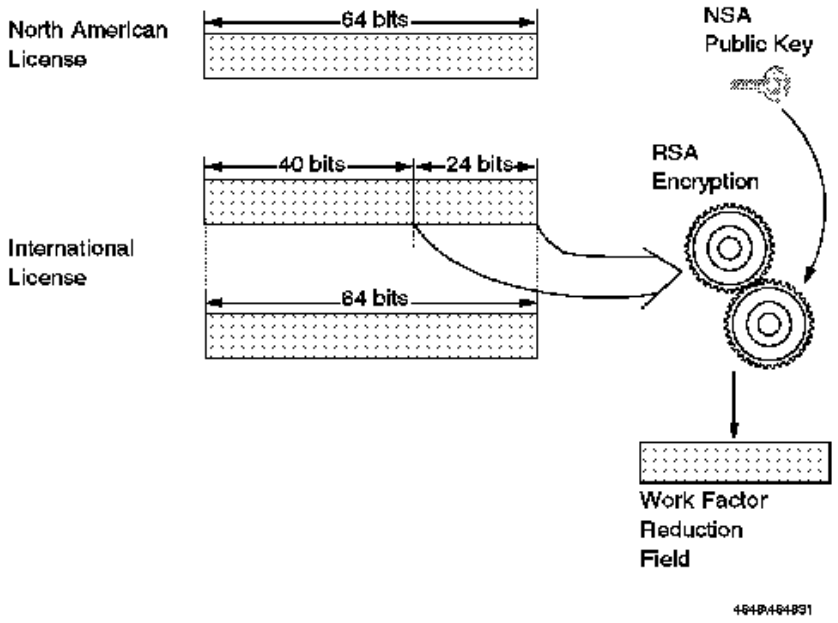

Figure 5.6 Lotus work factor reduction, as appeared in (Macgregor and others 1997)

According to Kaufman,

> This is sort of the best of both worlds -- it doesn't make the product any less secure against the U.S. government, but it makes it substantially more secure against all other attackers. We still wish the U.S. government would let us do better, but this solution satisfies more customers than either of the other available alternatives. (Kosheff 1997)

The jurisdictional problems still continue, however, particularly with France. Lotus still had to develop three implementations of Notes security: domestic, foreign, and French (Nielsen and others 1999). An article by a Lotus employee notes that

> The government of France, however, found the International edition unacceptable. To comply with French law, we created the French edition, which uses a plain 40-bit encryption key and can therefore be "broken" by attackers willing to apply considerable computing power (presumably, including the French government). (Swedeen 1998)

Apparently the French government also wanted the same power as the NSA, but the WFR solution only gave the power of access to the NSA.

While much of this was public information, presented at various conferences and information available on Lotus' web site, in 1997 an uproar occurred, and was repeated again in 1999, raised mostly by the media. In 1997 a journalist in Sweden found that Lotus Notes and its NSA-supporting security was being used by 400,000 to 500,000 Swedish users, including

> ...349 parliament members, 15,000 tax agency employees, as well as employees in large businesses and the defense department.
>
> "I didn't know that our Notes keys were deposited (with the U.S.). It was interesting to learn this," says Data Security Chief Jan Karlsson at the (Swedish) defense department.
>
> Gunnar Grenfors, Parliament director and daily e-mail user, says, "I didn't know about this--here we handle sensitive information concerning Sweden's interests, and we should not leave the keys to this information to the U.S. government or anyone else. This must be a basic requirement." (Laurin 1997)

Rumours arose about backdoors, and secret access. In 1999 furore arose again as information regarding the Echelon surveillance infrastructure developed by the U.S. intelligence agencies became public, and the capacity of the NSA to perform intelligence gathering on European governments began to be discussed openly. Lotus Notes was raised as an example of how U.S. industry helps the NSA in achieving its goals (Campbell 1999a; Campbell 1999b; Madsen 1998).

This did not help matters for Lotus. At the time of my interview with Kevin Lynch, the Security Product Manager, the controversy was nearing its peak. With 39 million clients, and 40-45% of these clients being considered 'foreign', such controversy was not welcome, particularly as some of the commentary included misunderstandings of the solutions. Lynch admitted that their solution was not ideal. With U.S. regulations "spawning foreign availability", regulations constantly changing and creating uncertainty, the WFR solution is determinately "fixed". "All we want to do is sell to customers worldwide", but the regulations created a climate that was hurting e-commerce, and leaving Lotus in a "difficult position". Lynch believed that without the regulations, the foreign availability of cryptography would disappear: international developers only existed because of the regulations.

As the president of IRIS commented on the WFR solution,

> But please make no mistake about it: We fully recognize that this is a compromise solution. This is not a panacea. This is not the "silver bullet" that addresses all needs. (...) But we relish the fact that, in today's highly-charged political climate surrounding the issue of cryptography, we were able to negotiate a solution that increases information security for our worldwide customers. By throwing another potential solution into the mix -- by leading the way for others by clearing its export approval -- we hope that this stirs debate related to national cryptography policy. (Ozzie 1996)

The debate was stirred, and regulatory relaxation did occur eventually. The WFR solution was a design for the interests of the NSA, not that of law enforcement neither in the U.S., nor internationally.

5.5 Liberalisation and Conclusions

This chapter presented a story of the cryptography-policy discourse within the U.S., and some examples of the implications for technology, but also the implications of technology on policies through recalcitrance. The three types of policy, from intervening in the algorithms, managing access to keys, and controlling the form and nature of the keys were implemented in concert, or in solo, until liberalisation occurred.

Throughout these years where the policies shifted and transformed, it was difficult to separate the policy from the technology, and the technology from the policy. Black boxes were opened to find weak cryptography existed, based not on engineering decisions, but political ones. Black boxes of hardware (Clipper and Capstone), and standards (*EES*), were built to provide a stable solution to a political discourse that had not yet occurred publicly. These technologies, embedded with the interests of political actors, were confronted by other actors who mobilised the media, testified to Congress, and addressed petitions to the President. Blaze found recalcitrance within the design of *EES* itself: the design could not accommodate the interests entirely. The technique of escrow was then disembodied from the standard and the chips, into industry designs through shifts in the regulatory regime, attempting to enrol industry to develop solutions to meet the same interests. The policy was given to the market to sort out the technology of key recovery, transforming the perceived needs and interests of e-commerce.

With the influential report on the Risks of Key Recovery (Abelson and others 1998), scepticism peaked regarding the feasibility of key recovery, and the risks introduced by these systems. These arguments were supported by other researchers and specialists, including from Entrust (Lloyd and Oorschot 1998), and the National Security Agency (1998).

Such systems were built, however. Denning (1997) outlines 34 such implementations, according a taxonomy developed by herself and Branstad (1997). There were disagreements regarding the capacities of these technologies. Entrust developed key recovery, but as we have seen, this was very different from the policy defined as key escrow, nor was it developed necessarily because of policy. PGP was developed to confront government policy, and faced the full brunt of it; and when PGPADK was implemented, faced the full brunt of public concern, and eventually even technological objection.

Industry had more interests than creating a system that was difficult to build and that introduced new risks and liabilities. To enrol these interests, domestic policy, market policy and foreign policy were merged into one: export controls were re-engineered to satisfy national security interests, law enforcement concerns, and market creation for key recovery products. Liberalisation occurred for specific markets only if the interpretive flexibility and application of cryptography could be limited; and such solutions were developed, but circumvented eventually by foreign availability. Microsoft CAPI was developed, in accordance to the policy, and regulated foreign availability; but in doing so created extra-jurisdictional power for the regulators. Lotus WFR created with the interest of strong cryptography actually carried with it the interests of the NSA wherever implemented; except for France where the government's interests were met to some extent, but not to the same as the extraterritorial powers granted to the U.S. through its design.

Even the technology and the policy can be excluded, or circumvented. Criticism of the government policy did not cease, as protests and concerns from industry and civil society continued to arise. Foreign availability of products were documented and found to be increasing (Trusted Information Systems and Network Associates 1997), including studies done by the U.S. Government (National Security Agency and US Department of Commerce 1995), and even documented by members of the House of Representatives (Campbell and others 1996).

Foreign availability places North American companies at a competitive disadvantage. With estimates of costs and risks of losing out to foreign cryptography providers while the solutions required by domestic controls are either ineffective, risky, or commercially unviable, and the loss of interest and protection in e-commerce due to privacy and security concerns, and increasing pressure from industry lobby groups and civil society organisations, the U.S. policy was set for change.

Liberalisation did occur, grown from seeds of concern planted within the government as early as 1996. Under the U.S. FOI procedures, EPIC managed to review some of the BXA

internal documentation regarding the rules at that time. In one memorandum between the Under-Secretary of Commerce (and head of the BXA) and his colleagues, William Reinsch states that in considering the 1996 decision to allow export so long as key recovery is eventually built-in, the policy would do significant damage to the U.S. economy.

> Market forces are more reliable and more politically stable than new restrictions. (...) The effect will be not only to damage U.S. firms but to subsidize (by ceding market share and revenue) the foreign production of non-key recovery products, thus undercutting our efforts to win international support for key recovery. (...) There is also a real risk that multinational corporations will move production of these non-key recovery products offshore to avoid new U.S. restrictions.(...) There is also the real risk that by encouraging the development of non-key recovery manufacturing outside of the U.S., we would see more non-key products available domestically as the new foreign producers do not face any restrictions on imports into the U.S. (...) (Reinsch 1996)

Reinsch was voicing what can be perceived as the eventual policy outcome: foreign availability increased, general mistrust arose surrounding U.S. technologies, and companies did indeed move offshore (both Sun (Clark and Lash 1997) and RSA (Messmer 1999; RSA Data Security 1999) did, amongst others (Wayner 1998)).

Other regulatory strategies were considered. One included a tax subsidy bill, entitled "Tax Relief for Responsible Encryption Act 1999" (1999), which was to give companies a 15 percent tax break on the costs of developing key recovery technology. Another strategy was to require that any interaction with government would only occur between communications system using key recovery. This revisited the Clipper strategy, using interoperability and network effects as the incentive. These strategies were not taken forward.

Announced in September 1998 and circulated in December 1998, new rules were released that allowed companies to sell cryptographic applications abroad with a key-length limit of 56-bits, without the obligation to develop key recovery solutions. It is worth noting that this was before DESCracker was developed, and perhaps DESCracker was developed specifically to show the futility of such limited protection.

In September 1999 more changes were announced when liberalisation applied to all strengths of cryptography sold to individuals, commercial firms, and non-government end-users in all countries short of the embargoed terrorist-supporting states. A one-time review was required by the U.S. Government, to review exactly what form of cryptography was being exported (Bureau of Export Administration 2000).

In January 2000 new rules were released that also dealt with the issue of public availability of source code, thus considering some of the results of the Bernstein case, while

maintaining the one-time review. This was a curious development: cryptography posted on the web, newsgroups, and possibly emails would be regulated according to the new rules. That is, according to an interpretation from the BXA,

> a) If you post encryption source code to a site on the net and anyone can access it, you do not need to have it reviewed by BXA or obtain a license.
>
> b) Simply posting this "publicly available" encryption source code does not count as an export and does not trigger all the terrorist sanctions and other requirements created by various Federal sanctions laws. (what this means is that if you post some code and Saddam Hussein downloads it, you are not liable. If Saddam calls you up and asks you to e-mail him the code, and you send the e-mail without applying for and receiving a license, you are liable).
>
> c) You do need to send BXA an E-mail with the internet location of the posted source code and you are prohibited from sending (as opposed to posting) the encryption source code to a terrorist country or an individual on one of our denial lists.
>
> d) if a foreign person makes a new product with the source code you've posted, there are no review or licensing requirements for that foreign product. If they pay you a royalty or licensing fee for a product they've developed for commercial sale, however, you may have to report some information to BXA. (Lewis 2000)

What followed was further confusion and comedy. Cypherpunks (alluded to in chapter 3) who earlier had devised perl script code of a *RSA* implementation began to include these scripts in their signatures of emails, and thus every email they would send they would carbon copy to the BXA. Likewise, people would begin posting source code on their websites just to notify the BXA.

What began in a situation where public discussion was dissuaded, and export of technologies unlikely (ITAR), and government-sponsored solutions for the market (Clipper), was transformed into market incentives and controlled liberalisation, and ended with simple reporting schemes reduced in some situations to comedy.

In reviewing the data presented here, it is noticeable that regimes of regulation changed drastically throughout the discourse, while the technology itself, though implemented differently at points in time, returned very much to its original design in the 1970s, or its scientific progression as argued by cryptographers. Years from now, the 1990s crypto-wars, as they are known, may be erased from history; as Joliot was separated from his nucleus. Cryptography may be considered without the policy; and it would be easy to claim that an otherwise *natural* progression occurred between the 1960s (*DES*) through to 2000 (liberalisation). Such a narrative would not explain why cryptography is not widely used, why *DSS* exists, amongst other issues.

Moreover, we would miss the opportunity to learn about the policy landscape of cryptography, and how it may be similar to other policy discourses, with similar interests and ideas. In chapter 7 I will review this landscape, and attempt to understand the implications and lessons for regulation theory.

Endnotes

1. The term *strong cryptography*, in dealing with key sizes, presupposes that effective algorithms are used. I left this detail out for the time being for simplicity.
2. Some refer to Capstone as Tessera; the two are the same: Tessera was the original name of Capstone, until it was discovered that there was a previous trademark (NRC 1996, p.176 footnote 15).
3. According to http://epic.org/crypto/clipper/.
4. In some implementations, each case involved 128-bit keys, except that in the export version, 88 bits of the session key would not be encrypted.

References

"International Traffic in Arms Regulations (as of April 1, 1992)." In *Code of Federal Regulations*, Title 22 (Foreign Relations), Chapter I (Department of State), Subchapter M, 1992.

"To amend the Internal Revenue Code of 1986 to allow a tax credit for development costs of encryption products with plaintext capability without the user's knowledge." 1999.

105th Congress. *Electronic Data Security Act of 1997*. Washington, DC: U.S. Congress, 1997a.

105th Congress. *H.R. 695, en Bloc Ammendments by the Subcommittee on International Economic Policy and Trade of the Committee on International Relations*. Washington: U.S. Congress, 1997b.

105th Congress. *Promotion of Commerce On-Line in the Digital Era (Pro-CODE) Act of 1997*. Washington, DC: U.S. Government, 1997c.

105th Congress. *S.909: Secure Public Networks Act (Introduced in the Senate)*. Washington, DC: U.S. Government, 1997d.

105th Congress. *S.2067: Encryption Protects the Rights of Individuals from Violation and Abuse in CYberspace (E-PRIVACY) Act (Introduced in the Senate)*. Washington, DC: U.S. Government, 1997e.

105th Congress. *S. 376: Encrypted Communications Privacy Act of 1997*. Washington, DC: U.S. Congress, 1997f.

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L., Schiller, J. I., and Schneier, B. *Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption*. Washington: Center for Democracy and Technology, 1998, 2.

Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*: John Wiley & Sons, 2001.

Baltimore Technologies. *Demonstrates Integrated Solutions for Secure E-Mail, Web Browsing & Certification at Infosecurity '97*. London: Infosecurity '97, 1997.

Banisar, D., and Schneier, B. *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*. New York: John Wiley and Sons, 1997.

Barclays Bank. *Barclays Internet Banking: Security*. Barclays Bank, 1999. Accessed January 29 1999. WWW. Available from http://www.personal.barclays.co.uk/online/homepage/internet/security.htm.

Blaze, M. "Protocol Failure in the Escrowed Encryption Standard." A paper delivered at the Second ACM Conference on Computer and Communications Security, Fairfax, VA, November 1994.

Blaze, M., and Diffie, W. *Open Letter and attached Transcription of BRUTE-FORCE CRYPTANALYTIC ATTACKS*. www.crypto.com, 1996.

Blaze, M., Diffie, W., Rivest, R. L., Schneier, B., Shimomura, T., Thompson, E., and Wiener, M. *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security: A report by an ad hoc group of cryptographers and computer scientists.* Business Software Alliance, 1996.

Brickell, E. F., Denning, D., Kent, S., Maher, D., and Tuchman, W. *Skipjack Review: Interim Report*. 1993.

Brooks, C. *Decision Memorandum: Outside Crypt-mathematicians to Examine Clipper*. National Security Agency, 1993.

Brown, M. *Statement on HR3011 by Vice President and General Counsel of Lotus Development Corp and on Behalf of the Business Software Alliance to House Committee on the Judiciary*. U.S. House of Representatives, 1996.

Bureau of Export Administration. *Revisions to Encryption Items; Interim Final Rule*. U.S. Department of Commerce, 2000.

Campbell, D. *DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION (An appraisal of technologies for political control): The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition.* European Parliament Directorate for General Research, Directorate A, The STOA Programme, 1999a, Part 4/4.

Campbell, D. "Only NSA can listen, so that's OK." *Telepolis*, June 1 1999b.

Campbell, T., Goodlatte, B., Eshoo, A., Engel, E., Lofgren, Z., Barr, B., Moorhead, C., Schroeder, P., Frank, B., Gejdenson, S., Coble, H., Boucher, R., Heineman, F., Bono, S., Ehlers, V., Cunningham, R., Norwood, C., Tate, R., Manzullo, D., Chenoweth, H., Davis, T., Bartlett, R., Farr, S., Calvert, K., Smith, L., Moakley, J., and Woolsey, L. *Dear Mr. President*. Washington, D.C.: U.S. Congress, 1996.

Cavallar, S., Dodson, B., Lenstra, A. K., Leyland, P. C., Lioen, W. M., Montgomery, P. L., and Murphy, B. *Factorization of RSA-140 using the number field sieve*. Centrum voor Wiskunde en Informatica, 1999.

Center for Strategic and International Studies. *Breaking Down the Barricades: Reforming Export Controls to Increase U.S. Competitiveness*. Washington, D.C., 1994.

CERT. *CERT Advisory CA-2000-18 PGP May Encrypt Data With Unauthorized ADKs*. Computer Emergency Response Team, 2000.

Clark, T. "Record set in cracking 56-bit crypto." *CNet News.com*, January 19 1999.

Clark, T., and Lash, A. "Sun dodges crypto export limits." *CNet News.com*, May 19 1997.

Computer Professionals for Social Responsibility. *Electronic Petition to Oppose Clipper to the President of the United States*. Washington, D.C.: CPSR, 1994.

Cryptix. *Cryptix Frequently Asked Questions*. Cryptix Development Team, 1998, 1.18.

Curry, I. *Trusted Public-Key Infrastructure*. Entrust Technologies, 1997.

Curry, I. *Key Update and the Complete Story on the Need for Two Key Pairs*. Entrust Technologies, 1998.

Davis, J. R. *Letter to Director Sessions of the National Security Agency RE: Use of the Clipper Chip in AT&T TSD 3600 During Phase II of Production*. National Security Agency, 1992.

Denning, D. *Descriptions of Key Escrow Systems*. Georgetown University, February 1997.

Denning, D., and Branstad, D. K. *A Taxonomy of Key Recovery Encryption Systems*. Georgetown University and Trusted Information Systems, 1997.

Department of Commerce. *Federal Register: February 9, 1994 (VOL. 59, No. 27), Approval of Federal Information Processing Standards Publication 185, Escrowed Encryption Standard (EES)*. National Institute of Standards and Technology (NIST), 1994, RIN 0693-AB19.

Diffie, W. "The impact of secret cryptographic standard on encryption, privacy, law enforcement and technology." A paper delivered at the Testimony to The Subcommittee on Telecommunications and Finance of the Committee on Energy and Commerce of the U.S. House of Representatives, Washington, DC, 11 May 1993.

Diffie, W. *Comments on the Computer Security Enhancement Act of 1997 before the House Science Committee, Subcommittee on Technology*. U.S. House of Representatives, 1997.

Diffie, W., and Landau, S. *Privacy on the line: the politics of wiretapping and encryption*. Cambridge, Mass.: MIT Press, 1998.

Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics and Chip Design -- how federal agencies subvert privacy*. Sebastopol, CA: O'Reilly and Associates, Inc., 1998.

Ellison, C. *Who Owns Cryptography*. Glennwood, MD: Trusted Information Systems, 1994.

Entrust Technologies. *Businesses Require Key Backup and Recovery System For Effective Implementation of Security Solutions*. Dallas, Texas, 1998a.

Entrust Technologies. *Guide to the Business Impact of PKIs*. 1998b.

Entrust Technologies. *Entrust Authority*. 2001. Accessed September 27 2001. Available from http://www.entrust.com/authority/features.htm#a3.

Esposito, D. "Supporting CryptoApi in Real-World Applications." *Microsoft Interactive Developer*, Volume 2, Number June, 1997.

Federation of American Scientists. *FAS Intelligence Resource Program: Intelligence Agency Budget and Personnel*. July 31 7:04:21 AM 1998. Accessed December 14 1998. WWW. Available from http://www.fas.org/irp/agency/budget1.htm.

Freeh, L. *Threats to U.S. National Security, Statement for the record before the Senate Select Committee on Intelligence*. Washington: U.S. Senate, 1998.

Freeh, L., Crowell, W., and Reinsch, W. *Members Briefing Regarding Encryption, House of Representatives 10 Committee on International Relations*. Washington: Federal Bureau of Investigations, the National Security Agency, Bureau of Export Administration, 1997a.

Freeh, L., Crowell, W. P., and Reinsch, W. *Members Briefing Regarding Encryption: House International Relations Committee*. U.S. House of Representatives, 1997b.

Freeh, L. J. *House International Relations Committee: Statement of Louis J. Freeh, Director, Federal Bureau of Investigation*. Washington, DC: Members Briefing Regarding Encryption, Committee Hearings of the U.S. House of Representatives, 1997.

Garfinkel, S. *PGP: Pretty Good Privacy*: O'Reilly & Associates, 1994.

Gladman, B. *U.S. Government Controls on the Microsoft Cryptographic Application Programming Interface: A Paper for the ICE Workshop.* International Cryptography Experiment, The Third Workshop, 1996, 7th Draft.

Gladman, B. "IE4 Security Features." ed. UKCrypto Mailing List: UKCrypto Mailing List Archive, 1998a.

Gladman, B. "Key Recovery -- meeting the needs of users or key escrow in disguise?" In *EPIC Cryptography and Privacy Sourcebook 1998*, ed. David Banisar. Washington, DC: Electronic Privacy Information Center, 1998b.

Gore, A. *Meeting on Encryption Policy, Wednesday March 31, 1993, at 6:00pm*. Washington D.C.: Office of the Vice President, 1993.

Gore, A. "Dear Representative Cantwell." To the Honorable Maria Cantwell from the Office of the Vice President, 1994a.

Gore, A. *Statement of the Vice President*. The White House, Office of the Vice President, 1994b.

Heinz, J. *U.S. Strategic Trade: an export control system for the 1990s*. Boulder, Colorado: Westview Press, 1991.

Holleyman, R. W. *Testimony of Robert W. Holleyman, President, Business Software Alliance On The Export of Software with Encryption Capabilities.* Gaithersburg, MD: National Institute of Standards and Technology, 1995.

Hudson, T. J., and Young, E. A. *SSLeay and SSLapps FAQ*. Mozilla Crypto Team, 1998.

IDG.net. *News and New Product Briefs (12/15/97): Baltimore Technologies J/SSL can be used for e-commerce security*. 1997.

Inman, B. "The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector." Republished in *Electronic Privacy Papers*, ed. David Banisar and Bruce Schneier, 347-355, 1997. Original 1979.

Irwin, S. M. *Technology Policy and America's Future.* New York: Henry L. Stimson Center, St. Martin's Press, 1993.

Kahn, D. "Cryptology goes public." *Foreign Affairs*, Volume 58, Number Fall, 1979.

Kerrey, J., and John McCain. *The Secure Public Networks Act*. Washington, DC: U.S. Senate, 1997. Congressional Record, cr18my97-111.

Kerstetter, J. *Crypto holes slow export adoption.* PC Week, 1998. Accessed October 7, 1998. WWW. Available from http://www.zdnet.com/pcweek/news/0601/01crypto.html.

Kosheff, B. *Charlie Kaufman: Security Status.* Iris Notes.net, 10/01/97 1997. Accessed December 7 1998. WWW. Available from http://notes.net/today.nsf/8a6d147cf55a7fd385256658007aacf1/5c32705b58a3bd6d85256522005eaede?OpenDocument.

Lash, A. "Feds OK 128-bit crypto amid protests." *CNET News.com*, February 13, 1997.

Laurin, F. "Secret Swedish E-Mail Can Be Read by the USA." *Svenska Dagbladet*, 18 November 1997.

Leahy, P. S. *Introduction of the E-PRIVACY Act*. Washington: U.S. Senate, 1998.

Levy, S. *Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age*. New York: Viking Press, 2001.

Lewis, J. "Re: FC: Is this man a crypto-criminal? The Feds won't say..." ed. Declan McCullagh: Politech Mailing list, 2000.

Lloyd, S., and Oorschot, P. v. *Key Recovery Feasibility Study*. Entrust Technologies, 1998.

Macgregor, R., Sadtler, C., Zhe, W. X., and Yamamoto, H. *The Domino Defense: Security in Lotus Notes and Internet*. IBM, 1997, SF24-4848-00.

Madsen, W. *Crypto AG: The NSA's Trojan Whore?* 1998. Accessed March 17 2003. Available from http://mediafilter.org/CAQ/caq63/caq63madsen.html.

Markoff, J. "Export Law Tested by Sale of Privacy Software." *The New York Times*, March 20 1998.

McConnel, B. W., and Appel, E. J. *Interagency Working Group on Cryptography Policy Draft Paper: Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure*. Washington, DC: Executive Office of the President of the United States, 1996.

McConnell, J. M. "Dear Dr. Ware." FOIA release from the Electronic Privacy Information Center, 1992a.

McConnell, J. M. "Dear Mr. Barr." FOIA release from the Electronic Privacy Information Center, 1992b.

McCullagh, D. "Landmark Ruling on Encryption." *Wired News*, May 6 1999.

McCullagh, D. "Pretty Good Bug Found in PGP." *Wired News*, August 25 2000.

McCullagh, D. "PGP: Happy Birthday to You." *Wired News*, June 5 2001.

Messmer, E. "RSA tries Australian end-run around U.S. encryption laws." *IDG on CNN.com*, January 8 1999.

Microsoft Corporation. *Government Regulation of Cryptography*. 1996. WWW. Available from http://www. microsoft. com/technet/treeview/default. asp?url=/technet/security/prodtech/mailexch/cryptreg.asp.

Microsoft Security Advisor. *Server Gated Cryptography*. Microsoft, 13 April 1998a. Accessed February 23 1999. WWW. Available from http://www.microsoft.com/security/tech/sgc/whitepaper.asp.

Microsoft Security Advisor. *Server Gated Cryptography: Information on Regulations Concerning SGC*. Microsoft, 1998b.

Microsoft Security Advisor. *There is no "Back Door" in Windows*. Microsoft, 1999.

National Institute of Standards and Technology. *Key Escrow Issues Meeting: Discussion Paper #3 -- Draft Export Criteria for Software Key Escrow Encryption*. 1995.

National Security Agency. *Threat and Vulnerability Model for Key Recovery*. U.S. Government, 1998.

National Security Agency, and U.S. Department of Commerce. *A Study of the International Market for Computer Software with Encryption: Executive Summary and Introduction*. U.S. Government, 1995.

Neshevich, C. "Industry debates encryption policy." *NetworkWorld*, April 24 1998.

Netscape. *International Step-Up Encryption*. Netscape Communications Corporation, 1999.

Nielsen, S. P., Dahm, F., Luscher, M., Yamamoto, H., Collins, F., Denholm, B., Kumar, S., and Softley, J. *Lotus Notes and Domino R5.0 Security Infrastructure Revealed*. International Technical Support Organization, IBM Lotus, 1999, SG24-5341-00.

NRC. *Cryptography's Role in Securing the Information Society* Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, National Research Council, ed. Kenneth W. Dam and Herbert S. Lin. Washington, D.C.: National Academy Press, 1996.

NSACOCAPI (NSA Cross Organization CAPI) Team. *Security Service API: Cryptographic API Recommendation, Second Edition*. Fort Meade: National Security Agency, 1996.

Office of the Vice President. *Statement of the Vice President*. Washington DC: The White House, 1996.

Olmer, L. "Objectives and Goals of U.S. Export Control Policy." In *Building Reasonable Commercial Ties with Political Adversaries*, ed. Michael R. Czinkota, 40-49. New York: Praeger Publishers, 1984.

Olson, T. B. *Memorandum to William B. Robinson, Office of Munitions Control*. Assistant Attorney General, Office of Legal Counsel, 1981.

Ozzie, R. *Opening speech of the RSA Data Conference 1996*. President of Iris Associates, and affiliate of Lotus Development Corporation, 1996.

Patel, M. H. "Daniel J. Bernstein v. United States Department of Justice; United States Department of Commerce; Department of State; United States Department of Defense; United States Arms Control and Disarmament Agency; National Security Agency, United States Department of Energy; Central Intelligence Agency; Madeline E. Albright, United States Secretary of State; William M. Daley, United States Secretary of Commerce; William Cohen, United States Secretary of Defense; Kenneth A. Minihan, Director, United States National Security Agency; John B. Holum, Director, United States Arms Control Agency; William G. Robinson; Gary M. Oncale; Ambassador Michael Newlin; Charles Ray; Mark Koro; Greg Stark." In *Appeal from the United States District Court for the Northern District of California*, ed. Marilyn Hall Patel: Office of the Circuit Executive, 1999.

Pressman, A. "Attempt to Design 'Backdoors' Fails." *Washington Post*, June 26 1998.

Reinsch, W. *Administration Encryption Policy: Senate Commerce Committæ Testimony*. Washington DC: Under Secretary of Commerce, U.S. Department of Commerce, 1997.

Reinsch, W. A. "Memorandum for Deputies Subgroup on Cryptography: Non-Key Recovery Export After Two Years." Washington, DC: United States Department of Commerce, 1996.

Reno, J. *Law Enforcement In Cyberspace, presented to The Commonwealth Club of California*. San Francisco: United States Attorney General, 1996.

Rescorla, E. *Internet-Draft: HTTP Over TLS*. Internet Engineering Task Force, 1999.

Rotenberg, M. "Prepared Testimony and Statement for the Record." A paper delivered at the Testimony to The Subcommittee on Telecommunications and Finance of the Committee on Energy and Commerce of the U.S. House of Representatives, Washington, DC, June 9 1993.

Rotenberg, M. *Testimony Of Marc Rotenberg, Director Electronic Privacy Information Center, On The Promotion Of Commerce On-Line In The Digital Era Act Of 1996, S. 1726*. Washington, D.C.: The Senate Committee On Commerce, Science & Transportation, Subcommittee On Science, Space & Technology, June 26 1996.

RSA Data Security. *RSA Provides Security Solutions to Worldwide Markets Through New Operation in Australia*. San Mateo, California, 1999. Press Release.

RSA Laboratories. *RSA Factoring Challenge*. RSA.com, 1999. Accessed February 10 1999. WWW. Available from http://www.rsa.com/rsalabs/html/factoring.html.

Rubinstein, I. *Testimony of Ira Rubinstein, Senior Corporate Attorney, Microsoft Corporation on behalf of the Business Software Alliance: IMMEDIATE NEED FOR EXPORT CONTROL RELIEF FOR SOFTWARE WITH ENCRYPTION CAPABILITIES*. Washington DC: House Judiciary Committee, Subcommittee on Courts and Intellectual Property, 1997.

Schneier, B. *Applied Cryptography*. 2nd ed.: Wiley and Sons, 1996.

Schneier, B. *Crypto-Gram Newsletter: Bruce Schneier comments on the "NSA" key in Microsoft CryptoAPI*. Counterpane Internet Security, 1999.

Senderek, R. *KEY-EXPERIMENTS - How PGP Deals With Manipulated Keys*. 2000.

Sessions, W. S. *Encryption: The Threat, Applications, and Potential Solutions, Letter Addressed to Mr. George J. Tenet, Special Assistant to the President and Senior Director for Intelligence Programs of the National Security Council*. Director of the National Security Agency, 1993. Letter with briefing document attached.

Swedeen, B. *Special Report: Notes Encryption: Locks for a Digital World*. Lotus Support, 1998.

TACFIPSFKMI. *Example Potential Solutions for the Draft Export Criteria for Software Key Escrow Encryption*. National Institute for Science and Technology, 1995. Key Escrow Issues Meeting, Discussion Paper Number 4.

Tenet, G. J. "Memo to Leon S. Fuerth and William M. Wise: HELP." National Security Council, made available by EPIC, 1993a.

Tenet, G. J. "Memo to Leon S. Fuerth: Encryption." National Security Council, made available by EPIC, 1993b.

The White House. *Statement by the Press Secretary*. Washington: U.S. Government, April 16 1993.

The White House. *Statement of the Press Secretary*. Washington: U.S. Government, February 4 1994.

The White House. *Administration Statement on Commercial Encryption Policy*. Washington: U.S. Government, July 12 1996a.

The White House. *Executive Order: Administration of Export Controls on Encryption Products*. Washington, D.C., November 15 1996b.

The White House. *Vice President Announces Special Envoy for Cryptography*. Washington: Office of the Vice President, November 15 1996c.

Trusted Information Systems, and Network Associates. *Worldwide Survey of Cryptographic Products*. Software Publisher's Association and TIS, December 1997.

USACM. *Codes, Keys and Conflicts: Issues in U.S. Crypto Policy*, ed. Special Panel of the ACM U.S. Public Policy Committee. New York: Association for Computing Machinery, 1994.

Verisign. *Verisign Granted First Federal Approval to Issue Certificates Enabling Export of Strong Encryption for U.S.-Based Companies and International Banks*. Mountainview, California, July 14 1997.

Verisign. *Lotus Joins With Verisign To Provide Secure Global Communications and Commerce with Strongest Encryption Approved by the U.S. Government*. May 18 1998.

Walker, S. T., Lipner, S. B., Ellison, C. M., Branstad, D. K., and Balenson, D. M. *Commercial Key Escrow: Something for Everyone -- Now and for the Future*. Trusted Information Systems, 1995, TIS Report #541.

Wayner, P. "Encryption Expert Says U.S. Laws Led to Renouncing of Citizenship." *The New York Times*, September 6 1998.

Wiener, M. J. *Efficient DES Key Search*. Ottawa: Bell-Northern Research, 1993.

Wilcox, J. "Expert says Windows has a security breach." *CNet News.com*, September 3 1999.

Wired News. *NAI Back in Key Recovery Group*. November 12 1998.

Zaba, S. *The _NSAKEY in Microsoft's Crypto API: facts, fiction, and speculation*. Was published in Elsevier Information Security Review, but received advanced copy, 1999.

Zimmerman, P. "PGP/NAI merger and key recovery." ed. eston@synernet.com: Cryptome.org, March 18 1998.

Zimmerman, P. "Updated remarks from Zimmerman on ADK bug." ed. Ralf Senderek: Senderek.de, 20 October 2000.

Chapter 6: E-Commerce and Surveillance Policies in the United Kingdom

> The regulation is aimed at ensuring first of all the agents operating in the market, the agency companies, are fit and proper for the purpose and they in turn have the right systems of management control, information flows and so on.
>
> -- Sir Alan Hardcastle

Abstract

This chapter presents the transformation of policy instruments, the responses to government initiatives, and parliamentary debates in the United Kingdom from 1996 to 2000. The UK proposals first tried to regulate the domestic use of encryption services, coupling key escrow with electronic commerce. When this strategy failed other strategies were pursued, finally settling upon government access to an individual's keys by creating a new power within the *Regulation of Investigatory Powers Act* 2000. Capturing the discourse at moments of interest, this chapter shows how translations were attempted, failed and succeeded, and shows the challenges of representing interests of both social and technological actors. These issues will be further discussed in Section III.

6.0 Introduction

While open discussion of cryptography policy in the United States began in the late 1980s and early 1990s, the United Kingdom stated publicly its regulatory intents in 1996. While the United States framed cryptography regulation with respect to national security concerns and was forced eventually to consider industry concerns on global competitiveness, the UK addressed cryptography policy after the advent of electronic commerce (e-commerce). As a result, throughout the discourse successive British governments had to address cryptography and its various implications in tandem with e-commerce.

This chapter will present a view of this discourse, mostly chronologically to show shifts in regulations, regulatory bodies, governments, actors and strategies. Beginning with a statement of regulatory intent in 1996 and a consultation session in 1997, covered in §6.1, this chapter will then follow the policy changes as further e-commerce and market factors were considered, in §6.2.

In November 1999 the Queen's speech announced an assumed de-coupling of e-commerce and law enforcement interests in the policies, with the Labour government shortly thereafter introducing the Regulation of Investigatory Powers Bill (RIP) to Parliament. The

bill's consideration of encryption policy will be discussed in detail in §6.3, while its passage through Parliament will be investigated in some detail in §6.4 in order to show how articulations arose, how the technology was spoken of in detail, and how the structure of the technology shaped interests and actions.

As discussed in §6.5, the bill highlighted the conflicting requirements of secure communication and access requirements of law enforcement agencies; the problems of legislating in a rapidly changing technological environment; the need to minimise the costs and risks of any proposed legislation; the goal of maintaining human rights; and doing all this in a global context.

6.1 Regulatory Intent and Conservative Consultation

E-commerce and cryptography policies are almost inseparable in the UK. From its first public discussions on the issue, the UK Governments have continually framed the issue of secure e-commerce within the UK involving three phenomena: decryption keys, industry, and the interception of communications.

In 1996, the UK Department of Trade and Industry (DTI) published a statement on regulatory intents on encryption (DTI 1996); although there had been previous speeches and some discussion, this was the first modern policy statement. The government's articulated aim was to

> facilitate the development of electronic commerce by the introduction of measures which recognise the growing demand for encryption services to safeguard the integrity and confidentiality of electronic information transmitted on public telecommunications networks. (DTI 1996, par.1)

The articulated goal was originally to provide a legal basis for digital signatures. The government proposed the creation of Trusted Third Parties (TTPs). According to the statement, however, these TTPs were created in the interests of law enforcement.

> The licensing policy will aim to preserve the ability of the intelligence and law enforcement agencies to fight serious crime and terrorism by establishing procedures for disclosure to them of encryption keys, under safeguards similar to those which already exist for warranted interception under the Interception of Communications Act (IOCA). (DTI 1996, par.2)

These TTPs were thus translated entities. These third parties have long been proposed for the purposes of trust and authentication services, as Certificate Authorities (CAs) who would assure integrity of electronic documents, and/or insure against risks in e-commerce.

In introducing another service for these TTPs, the government policy was translating the role of TTPs to meet the interests of the policy: ensuring the capability to decrypt intercepted data through the provision of government access to escrowed keys.

The statement of intent was followed by a consultation paper from the DTI in April 1997, under a Conservative Party Government, and only months before a national election. In brief, the consultation paper outlined the implementation of Trusted Third Parties, and mandatory licensing of such TTPs, where the license would only be granted if these TTPs escrowed decryption keys, i.e. stored a copy of the decryption keys of its clients. The Government at the time felt that the UK was taking the lead.

> Many countries are currently trying to develop a cryptographic policy. Many countries agree with the UK that widespread use of cryptography must not be to the detriment of law enforcement requirements. The Government believes that this scheme is the best way to achieve this balance and that other countries may also see the benefits and follow the UK lead. (DTI 1997, sec 42)

Under this policy it was claimed frequently that individuals were always to be free to use the type of product or service they wished. The Conservative Government merely wanted Government Access to Keys (GAK) from TTPs.

A furore that followed in the consultation process. The consultation process resulted in over 260 responses, 102 from organisations and 158 from individuals (DTI 1998b). The responses were kept confidential for parliamentary review until a year later when a summary report was released. During this period of time a colleague and I solicited openly on the *ukcrypto* listserv for submitted responses and received twenty from individuals and organisations, while some others we searched for on the Internet. My summary report (Hosein 1998) was a representation of the content of twenty-five submissions.

Below I will review the arising issues of concern, and complement my results with the DTI's summary document of the full consultation. The two reports, written independently of each other, have some level of convergence from the data that arose.

DTI Report/Data

Licensing (Mandatory vs. Voluntary), Liability (risks of keys), International (availability of products and varying policies), and Lawful access

Hosein Report/Data

Nature of TTPs (need, encryption services, and trust), Market issues (need for TTPs, international issues, costs and risks), and Lawful access

Table 6.1 Issues arising from the 1997 consultation process

As Table 6.1 shows, both reports found contentions in the mandatory licensing schemes, risks of key escrow/recovery, international availability and policies, costs and liabilities, and issues related to lawful access. Some of these will be reviewed below.

6.1.1 E-commerce Issues

There was a general consensus in the consultation process that the legal recognition of digital signatures for the purpose of supporting e-commerce was a positive development. The DTI report states that "the only aspect of the document to receive almost universal approval was the proposal to legislate for recognition of digital signatures by the courts" (DTI 1998b, par4).

Similar results were found in my substantive review, but this did not mean that there was a true consensus however.[1] A number of respondents pointed out that the consultation paper alluded to a highly centralised infrastructure (Anderson 1997; BT 1997; Hansen 1997; Hyperion 1997; Leech 1997; Lindsey 1997), which is not necessarily conducive to e-commerce, nor entirely necessary. This centralisation is unavoidable if key recovery is the overriding constraint on system design, but has many unpleasant effects on the design of systems to suit real commercial and professional requirements (Anderson 1997). Respondents did not feel that regulation was ideal for the time being, and trust mechanisms would emerge rather than be mandated by legislation (Hyperion 1997).

6.1.2 De-coupling Surveillance from Trust

A general consensus was also reached on the issue of coupling e-commerce and surveillance policies. The DTI reports

> (t)he most common general criticism was that the paper should have more clearly separated the issue of the licensing of TTPs (in particular in their role as Certification Authorities, e.g. for digital signatures), from that of lawful access. These issues were seen as quite distinct in principle, and best addressed separately. (DTI 1998b, par3)

This resulted in confusion between the role of a Trusted Third Party and that of a Certification Authority (CA). Respondents noted that a CA may not need to provide *encryption services*, but it is still a *trusted third party*; trusted to perform its task of binding signature keys to identities by issuing digital certificates (BT 1997). The CA does not need or want to handle the user's private key, and in this sense does not provide an encryption service, according to the proposed policy (HP 1997). Failing to differentiate between authentication and confidentiality services leads to a lack of differentiation between CA and TTP, which in turn reflects a policy that couples e-commerce and surveillance.

Another coupling is the business interest in key recovery and the government interest in key escrow (as occurred in the U.S. as well, c.f. chapter 5). The Business Software Alliance (BSA), an industry coalition of software developers, in their response presented an analysis of the customer feedback to the member companies, and indicated that most of the demand for a key recovery does not involve third-party escrow. While individuals and organisations may wish to recover lost keys, the BSA felt that it is best to leave the development of solutions to this predicament to the market; the cost of governments mandating the use of third parties and escrow is that no one will use the services, and the market will suffer (BSA 1997).

6.1.3 Mandatory Licensing

The *requirement* that TTPs be licensed raised some concern as well, although the responses were more fragmented. Some supported licensing, but only a voluntary scheme; others supported mandatory licensing but not necessarily with the current requirements; others felt that licensing was costly and unnecessary regulation in an unknown market. The DTI report states that

> (a)mong those who approved of the licensing of TTPs, a significant and weighty minority argued for voluntary licensing, even though this was not explicitly discussed or put forward in the paper. There was felt to be a place for unlicensed TTPs if the market wants them. There were many calls for clarification of the suggested exclusions from the licensing regime, and several respondents asked for their own exclusion. One of the reasons for advocating voluntary licensing was this difficulty of defining exclusions. (DTI 1998b, par6)

In the substantive review, some of these concerns of exclusions were fleshed out. The mandatory requirement was of concern to businesses who did not feel it was necessary for them to be licensed; businesses should be excluded from regulation in order to issue certificates to their employees and customers (BSA 1997; Lindsey 1997; UCISA 1997). Further exceptions were felt necessary for virtual private networking, and business communities (BT 1997; Intel 1997); and extranet trading communities and teleworking environments (TMA 1997). The legal community felt that exemptions should apply under evidentiary privileges under common law, i.e. attorneys, physicians, and the clergy (ABA 1997).

With regard to regulatory burdens and costs,

> There were fears that the proposed licensing conditions would be too burdensome and costly. (...) There were many pleas from business organisations for the maximum amount of freedom to be left to the market, and many expressed confidence that in this fast-changing

> area market mechanisms would produce the most effective solutions. (DTI 1998b, par7)

It was felt by some that a new infrastructure for e-commerce was being modelled rather for law enforcement purposes; despite the harm to UK industry (BT 1997; EURIM 1997) caused by placing law enforcement interests above those of trust and commerce (BSA 1997; BT 1997; CBI 1997; CR&CL 1997; HP 1997; Leech 1997).

Some argued that the market, not regulation, should decide the services offered by the third parties (BSA 1997; BT 1997; CR&CL 1997). The regulatory burden, it was argued by some, will not create the right environment in which to encourage exploitation of e-commerce (BT 1997; Leech 1997); and that a true test of the validity of third parties will not occur unless the market is as lightly regulated as possible (Brazier 1997; EURIM 1997).

There was the additional concern that regulation would mandate a structure to the market and its players. Through a number of articulations of 'how the market works', organisations and individuals argued that regulation can provide enough barriers from entry into the market. In particular, the Law Society of England and Wales noted that the regulation would prohibit organisations other than banks and telecommunication providers from entering the market (LSEW 1997). Only major commercial service providers could afford to act before legislation is adopted (Leech 1997); as such a risk may only be taken by large players, rather than smaller companies with too much to lose over such an investment. As a result, only a few expensive third parties would exist, further limiting consumer choice (Hyperion 1997).

6.1.4 International

Often linked with the issue of regulatory and market success was the issue of international regimes, or consistency with the policies of other countries. The DTI summary report notes:

> The danger of international isolation from too strict a UK regime, or a unilateral one, was stressed. The UK should proceed in collaboration with the international community otherwise there could be a danger that it would become a backwater in the world of electronic commerce. (DTI 1998b, par10)

The need for coherence within international markets was argued for by a number of respondents, particularly industry (BT 1997). There was some concern regarding trade barriers for the free movement of technologies, products, and services (BSA 1997; BT 1997; Intel 1997). The licensing of cryptography imported into the UK would force software producers to tailor their products to the licensing criteria, rather than customer

and industry demand, further frustrating international market needs (ABA 1997; Intel 1997).

The consultation paper proposed that all UK citizens only use UK licensed TTPs, and even prohibited the marketing of non-UK third parties within the UK. Some responses questioned its enforceability (BT 1997; Lindsey 1997). It was felt that the proposed regulations provided barriers for the development of third parties to compete internationally, while also limiting non-UK companies from basing their operations in the UK (EURIM 1997). The proposed regulation, it was argued, does not acknowledge the complex ways in which international business operates: companies create joint ventures and subsidiaries necessary to meet specific market opportunities. Rather the proposal forces licensing upon these international businesses where common trust systems were involved previously (EURIM 1997; TMA 1997).

Some argued that the escrow proposals specifically provided further disincentives. As corporations would also be required to escrow keys for themselves, even such a corporate self-escrow scheme creates liabilities and imposes costs that some organisations may not wish to bear, so they will be forced either to abandon operations in the UK, or not use encrypted communications, thus undercutting some of the primary goals of the DTI (BSA 1997).

6.1.5 Risks

One of the risks noted in the DTI summary report,

> Most respondents thought that new criminal offences would be needed to cover the deliberate or reckless disclosure of a user's private confidentiality key, and most insisted the offence should also cover authentication keys. (DTI 1998b, par8)

Interestingly, the term *risk* was not included within the DTI report.

The substantive review found a number of concerns raised regarding risks. Many of these consultation responses, including (ABA 1997; Anderson 1997; BSA 1997; IT 1997) referred to an earlier version of the Risks of Key Recovery report (Abelson and others 1998) as supporting evidence of the risks.

Many declared that requiring decryption keys to reside outside the grasp and responsibility of the owners is questionable (BSA 1997; Leech 1997; LSEW 1997; UK Notarial Forum 1997). The resulting security risk was regarded as too high, as it offered decryption capabilities to others beyond the control of the sender and intended receiver (LSEW 1997).

User trust would not develop: users were said to worry about the third party's ability to keep the keys secure (Bohm 1997; HP 1997; LSEW 1997). The third parties themselves are exposed to the risk of accidental or corrupt disclosure or misuse of private keys. Any disclosure of a key used also for authentication purposes would allow for undetectable forgeries (Bohm 1997; LSEW 1997; UCISA 1997).

Others felt that the proposed regime of lawful access to keys was costly, infeasible, and discouraging to economic growth. With the requirement of access to keys, third parties will need to keep these keys readily accessible; it was argued that this has 'important diseconomies' with regard to both cost and the effectiveness of key security (BSA 1997; HP 1997). The possibility for criminal theft of keys increases with key escrow; the effect will be the increase of the cost of doing business, and may discourage high-technology investment in the UK (ABA 1997). Some declared that the proposals were neither technologically or economically feasible; that the key management infrastructure envisioned did not exist (BSA 1997; IT 1997), and at the very earliest would take several years to develop (BSA 1997).

6.1.6 Specific on Services, Technology, and Keys

When discussing the effectiveness and feasibility of the proposed regime, many respondents discussed the technology in some detail, speaking specifically on keys, key properties, and services. According to the DTI review,

> Comments included:
>
> - escrowing of private keys is contrary to absolutely basic information security precepts;
> - it was wrong to make the assumption that users would normally have separate key pairs for authentication and confidentiality;
> - it was unclear whether a warrant would result in a session key being handed over, or a master key of some kind;
> - the design, implementation and operation of the systems necessary to make TTPs with key escrow workable would involve an unacceptable degree of pioneering and complexity;
> - in conventional public key systems, warranted access to a user's private confidentiality key would only enable decryption of their incoming traffic - to enable decryption of their outgoing traffic would require a warrant to each of their correspondents' TTPs.
>
> Redacted list from (DTI 1998b, par12)

Many of the concerns grew out of perceived ambiguities within the consultation paper. Where technological specificity was provided, the respondents felt that there was a level of

misunderstanding on the behalf of the policy makers despite repeated claims from the DTI that the policy is technology-neutral.

The first perceived ambiguity was the definition of *encryption services*. The consultation document discusses the provision of encrypted services as a subset or the whole of the following:

> key management, key recovery, key certification, key storage, message integrity (through digital signatures), key generation, time stamping, key revocation services; which offered in a manner that allows a client to determine a choice of cryptographic key or allows the client a choice of recipient(s). (DTI 1997, par.74)

This definition was viewed as defective for a variety of reasons, as argued by many (Bell 1997; BSA 1997; BT 1997; CBI 1997; EURIM 1997; Lindsey 1997; UK Notarial Forum 1997). It was felt that most encryption products could be subject to the mandatory licensing requirement; even a simple e-mail product that contains any encryption capability or functionality could be subject to the definition because they may permit 'a client to determine' a 'choice of recipients' (BSA 1997). Companies that sell products that have such encryption functionality may be deemed criminal if they are not licensed; to protect themselves, these companies will either leave the UK market or be forced into the licensing scheme (BSA 1997). Even the secure transport of Internet packets would be in contravention of the licensing requirement (HP 1997). This was despite the DTI claim that the proposed regime would not mandate or outlaw the use of a specific technology.

There was a considerable debate on the technological-neutrality of the proposed regime. Some respondents felt that the interests of law enforcement would prevail in the choice of encryption systems. Most public key encryption systems only permit decryption of *received* text. The consultation paper described how TTPs would allow access to **both** incoming and outgoing encrypted traffic. Access to bidirectional traffic is not possible with traditional cryptosystems; the only system to date that acted in this way was the Royal Holloway *CASM* protocol (Anderson 1997). While the *CASM* protocol was strongly favoured by the UK Government, it did not have the support of the industry (Leech 1997). Its applicability to commercial and individual needs was viewed as dubious; consumers, merchants, and businesses will not accept a scheme that is fundamentally different from those to which they are accustomed (Leech 1997). Some respondents felt that legislation promoting a specific approach would enshrine current technology and restrict innovative schemes (Anderson 1997; CBI 1997; Intel 1997).

A final identified ambiguity is the poor understanding of what constituted the *key*. Respondents felt that the use of encryption for confidentiality services or authentication

services is often confused as being one and the same, and, according to Leech (1997) this in part explains the furore surrounding the DTI proposal. In practice, authentication and confidentiality services may be divided, to the point where a trusted third party that provides authentication services may be licensed, but does not necessarily require the same regulatory conditions as with a confidentiality service (Bell 1997; Data Protection Registrar 1997; Leech 1997). The Confederation of British Industry (1997) argued that there are many different uses of cryptography and many types of services that can be offered. Any policy, they argued, would need to regulate each differently. EURIM (1997), another industry organisation, argued that as companies are particularly concerned with authentication, non-repudiation and proof of origin, arguably such services do not require such law-enforcement oriented regulation.

The DTI consultation paper presumes that authentication keys and confidentiality keys are separable. Under the proposed policy, authentication/signature keys would not have to be escrowed so long as they are used for 'integrity purposes only' (DTI 1997, par.46). The signature and confidentiality private key distinction does not exist in *RSA*. A private key could be stored and accessed that would permit for the forging of legal transactions, giving rise to uncertainty (Anderson 1997). The solution to this policy predicament is to mandate a scheme that uses separate signature and confidentiality keys; it is assumed that this requirement again corresponds to the use of the *CASM* protocol (CBI 1997), again contradicting the technological neutrality claim.

Finally, because of the 'ways keys work', a number of respondents felt that the regime was unlikely to succeed. Confidentiality keys could be generated whenever required and signed by 'legal' authentication keys, without having to escrow either. This occurs frequently in hybrid cryptosystems, through the creation of session keys. There will be millions of Internet and intranet users creating billions of session keys, and these numbers will grow by orders of magnitude (BSA 1997), increasing complexity and costs.

6.1.7 Circumvention

The circumvention argument was repeated a number of times by respondents. According to the DTI summary report,

> By far the most common single point made against the lawful access proposals however, was that the key escrow mechanism might be by-passed by criminals etc. who are the authorities' potential targets. Examples of several such by-pass techniques were given. (...) The conclusion drawn was that the proposals would bring cost and complexity to law-abiding users while not necessarily achieving the results the law enforcement authorities want. (DTI 1998b, par13)

The substantive review found a convergence of opinion on this as well, e.g. (Bell 1997; Bohm 1997; Brazier 1997; BSA 1997; EURIM 1997; Hansen 1997; HP 1997; Hyperion 1997; Lindsey 1997; LSEW 1997). As is common with the 'genie out of the bottle' arguments (that because the technology is already available, trying to make it unavailable would be impractical) respondents felt that many solutions already exist for criminals to benefit from communications between themselves that will render legislation useless.

6.1.8 Evolution of the Consultation

After a number of heated conferences and public debates, the policy was placed on hold. In this period, there was a national election. Even during this election campaign, which resulted in a change of government from Conservative to New Labour, cryptography and e-commerce policy was an issue. In its 1997 election manifesto the Labour Party stated:

> ? The only power we would wish to give to the authorities, in order to pursue a defined legitimate anti–criminal purpose, would be to enable decryption to be demanded under judicial warrant (...).
> ? Attempts to control the use of encryption technology are wrong in principle, unworkable in practice, and damaging to the long–term economic value of the information networks. (Labour Party 1997)

Despite these pre-election claims, many of the next government's early policies were in fact continuations of policy processes initiated by the previous Conservative government.

6.2 De-Coupling E-Commerce and Law Enforcement Interests

In April 1998 the New Labour government released its *Secure Electronic Commerce Statement*.

> The Government has responded to business concerns and criticisms of the previous "mandatory" approach to licensing. (DTI 1998a, sec14)

The new policy promoted a *voluntary* licensing scheme, where licensing remained contingent on the TTP storing a copy of the decryption key (DTI 1998a, sec14). This strategy supposed that if TTPs wanted to be trusted by the public, then they would want to be licensed by the government, as a mark of trust-worthiness.

This policy generated similar concerns from industry and civil society at a number of conferences. A formal consultation document was not released until 1999, when the government released the *Building Confidence in Electronic Commerce* report (DTI 1999a).

The 1999 report included a number of changes from the 1997 consultation paper, but still maintained an emphasis on law enforcement interests.

> The need for new powers for law enforcement agencies to gain legal access, under proper authority and on a case by case basis, to encryption keys or other information protecting the secrecy of stored or transmitted information so as to maintain the effectiveness of the existing legislation designed to protect the public from crime and terrorism in response to new technological developments. (DTI 1999a, sec3)

Some of the changes were a reflection of the concerns previously raised. One such change included the differentiation among the keys-services-institutions relationships: there was an acknowledgement that digital signature keys and integrity/authentication services (assumed to be under a Certification regime) were separate from decryption keys and associated confidentiality services (assumed to be under a TTP-regime).

> The Government is committed to a clear policy differentiation between electronic signatures and encryption. This reflects the valid concerns expressed by industry during the consultation process launched by the previous administration, and recognises the different commercial applications of these services and the different challenges they pose to Government policy. (DTI 1999a, sec35)

As a result of this division in services, CAs would be recommended to be licensed, but are not **allowed** to escrow keys. TTPs, however, which are providers of confidentiality services, had another regime of regulation.

> Providers of confidentiality services are, therefore, encouraged to make the recovery of keys (or other information protecting the secrecy of the information) possible through suitable storage arrangements, or by means of key encapsulation products. (DTI 1999a, sec36)

The DTI was attempting to separate e-commerce (involving signature keypairs) and surveillance (involving encryption keypairs) from one another.

This new policy hinged on technology, however. The policy acknowledged that because signature keys could not be escrowed but these could be used to generate authenticated encryption keypairs, the escrow of confidentiality keys could be circumvented. Therefore the DTI tried to ensure that all legal signature keys are prevented, through the use of x.509 flags, from signing encryption keys, preventing self-certification of encryption keypairs. As the policy tried to plug the holes that were leaking, the policy grew more detailed and specific regarding the technology.

The response to this second consultation document was even larger, with 246 responses: 42 from individuals and 204 from organisations (including 33 from law enforcement agencies, 42 from trade associations, and 12 from law firms) (DTI 1999b, par.1). As the DTI reported in another consultation summary report,

> (m)any people repeated the view that the whole issue of lawful access should be decoupled from the measures to build confidence in electronic commerce, and would be better dealt with in a separate Bill, possibly after the forthcoming Home Office review of the Interception of Communications Act 1985. Confidence–building measures were thought to be more urgent, whilst lawful access measures were seen as: (a) likely to cause delay, and (b) having the potential to reduce confidence in the UK as a good place to base an electronic commerce service or business. (DTI 1999b, par.5)

Additionally, there was a warm reception to the idea of dropping GAK altogether; or at least separating it from the felt need of pushing e-commerce forward. According to the DTI, "so strongly was this felt that many went into considerable detail rehearsing why the Government was right to remove it" (1999b, par.6). At this time the country's leadership began speaking more on the important role of e-commerce, and the need for making the UK 'the best place for e-commerce', e.g. (Brown 1999; Brown 2000).

6.2.1 Abandoning the TTP Regime

In this period, the Prime Minister, through the Cabinet Office, commissioned a report from the Performance and Innovation Unit, entitled *Encryption and Law Enforcement* (PIU 1999). In a forward written by Prime Minister Tony Blair, he outlined the conflicted interests of government.

> I am determined to ensure that the UK provides the best environment in the world for electronic business. (...) But I am equally determined to ensure that the UK remains a safe and free country in which to live and work. The rise of encryption technologies threatens to bring the achievement of these two objectives into conflict. (PIU 1999)

Continuing this strain of interests, the report outlines the importance of encryption technologies to e-commerce (in its chapter 3), but also the importance of access to keys to law enforcement (in chapter 4). The report acknowledged that previous policies were likely to be circumvented by criminals (p.12), and doubted the commercial success of key escrow (p.13). Rather than relying on the unlikely TTPs, a new strategy was proposed: lawful access to decryption keys.

> (T)he task force welcomes the intention to include in the Electronic Commerce Bill provisions to allow lawful access to decryption keys and/or plain text under proper authority. The task force also

> recommended that further attention should be given in the Bill to placing the onus on the recipient of a disclosure notice to prove to the authorities that the requested keys or plain text are not in his possession, and to state to the best of his knowledge and belief where they are. (PIU 1999, p.15)

The government thus abandoned the TTP-model, and began pursuing legislation providing direct government access to keys.

6.2.2 Draft Bill on E-Commerce

What followed from the PIU report and the consultation paper was a period of flux. During this time, the Home Office began consultation on alterations to the *Interception of Communications Act* 1985 (Home Office 1999). The draft Electronic Commerce bill was released by the Department of Trade and Industry (ECB 1999). The E-Commerce bill dealt mostly with the legal recognition of digital signatures and regulating CAs.

The most notable section, Part III, dealt with the granting of government powers to gain access to keys under a notice. The draft bill gave rise to controversy due to problems surrounding its legality with regards to human rights law, particularly the European Convention on Human Rights (ECHR). A legal audit (Beatson and Eicke 1999) was commissioned by Justice, a human rights organisation, and the newly founded Foundation for Information Policy Research (FIPR), a think tank composed of a number of experts from academia, civil society, and industry who organised opposition to previous cryptography policies. The audit stated that the bill may be in contravention to the ECHR on a number of grounds including self-incrimination and the reversal of the burden of proof.

FIPR also engaged in a public analysis of the draft bill, raising concerns on *ukcrypto* and elsewhere (FIPR 1999). These included:

- Uncertainty as to *which key* was required to be handed to law enforcement. Would session keys suffice, or would private keys be required? The draft bill did not recognise differences amongst keys. Moreover, the draft bill did not recognise differences between signature keys and decryption keys.
- The draft bill introduced the offence of *Tipping-Off*, where if an individual's key was accessed by government, he would not be allowed to notify anyone of this situation, under penalty of a prison term. This is both a commercial concern (business officers would not be informed if their communications were, potentially, compromised) and a human rights concern (constitutes a gag-order, and may force an individual to continue using a compromised key).
- If an individual can not produce the key under question (due to loss or destruction or non-availability), the individual must show that he no longer has the key. The result, which the Home Office refuted (Home Office 2000a), is that there is a *reverse burden of proof*; failing to make such a proof, the individual can be sentenced to prison.

FIPR also argued that technological circumvention continued to plague the policy; implementing perfect forward secrecy would destroyed as a matter of protocol.

Another consultation occurred with 92 responses, including: 12 from individuals, 33 from commercial companies, 18 from trade associations, 11 from professional bodies, eight from lawyers, and two from the public sector. These responses were summarised in (DTI 1999c).

> By far the most common single criticism of the draft Bill, often strongly stated, was that Part III should be removed entirely, and its subject-matter addressed in a new or amended Interception of Communications Act (IOCA). The view was that Part III is not concerned with promoting electronic commerce, and could indeed have the effect of reducing confidence in the UK as a place from which to engage in it or provide services for it. The provisions of this part of the Bill attracted more comments, both general and detailed, than any other part, and many responses were about nothing else. There were concerns, sometimes argued in considerable detail, that it could contravene the (ECHR). (DTI 1999c, par.6)

Technological and operational concerns also arose.

> Very substantial costs were foreseen, as well as situations in which some technical or operational infeasibility could cause serious misunderstandings (...). The attempt to restrict disclosure of keys to those used for encryption was questioned on the grounds that dual-use keys are common: the possibility of their compromise would affect confidence in the reliability of electronic signatures etc. (DTI 1999c, par.22)

The summary report also included concerns regarding the 'failure to comply', the reversed burden of proof, and the 'tipping-off' offence.

> ? (...) Part III raises problems under article 8 because by comparison with ECHR case law it may not be precise enough, and may not provide adequate safeguards, to justify any *prima facie* breach of the right to privacy
> ? when the recipient of a (decryption notice) is a suspect, there may be a breach of article 6 (on self-incrimination)
> ? the effective requirement on the defence to prove non-possession (...) may also be in breach of article 6 (presumption of innocence).
>
> (DTI 1999c, par.27)

The government decided to take the first bit of advice where there was the greatest consensus: transplant Part III from the E-Commerce bill to a law enforcement-oriented bill.

6.2.3 The Queen's Speech: De-Coupling

With the controversy surrounding the draft bill, the Queen's Speech in November 1999 introduced the DTI's Electronic Communications bill that was free of issues relating to

access to keys, coupled with a promise that the Home Office would update the *Interception of Communications Act* 1985. These issues surrounding investigatory powers and access to keys were moved to the Home Office's Regulation of Investigatory Powers bill (RIP).

Although de-coupling occurred in legislation, the process of passing the RIP bill still involved articulations of risks and costs, specificity, circumvention, and threats to e-commerce.

6.3 Lawful Access and RIP

Although having legislatively separated e-commerce and lawful access, the government was unable to avoid debate on how investigatory powers may harm the country's e-commerce goals. Although the RIP bill was presented more as an update to *IOCA 1985*, Part III of the bill was essentially lifted from Part III of the draft Electronic Commerce bill. As introduced, clauses 46 through to 51 (referred to as B46–B51 as the numbers shifted throughout the debates due to amendments) addressed particular issues relating to how keys could be accessed, associated offences, and safeguards. Consequently, the critiques of Part III of the draft Electronic Commerce bill were similarly applied the RIP bill.

6.3.1 Key Disclosure

Clause B46 created the power to require disclosure of a key from an individual. Where encrypted data has come under the possession of the authorities, and where these authorities believe a particular person on reasonable grounds has the decryption key, and the disclosure of the key is likely to be of value for purposes connected with the exercise or performance by any public authority of any statutory power or statutory duty, and such a disclosure is proportionate to what is being achieved, then the authorities may require its disclosure. Such a disclosure can take place in the 'interests of national security'; 'for the purpose of preventing or detecting crime'; or 'in the interests of the economic well–being of the United Kingdom'. *National security* and *economic well–being* are borrowed terms from other statutory instruments.

6.3.2 Plaintext Instead of Key

Clause B47 allows the recipient of a notice to use the key to render the information into an intelligible form and provide the authorities with plaintext; rather than submitting the key. This can only occur in situations where the authorities did not specify that compliance is measured through the disclosure of the key itself. Such a specification can only be made where the direction for key–only disclosure is "proportionate".

6.3.3 Offence: Failure to comply

If an individual fails to comply with the notice, then he is guilty of an offence under clause B49. An individual fails to comply if he has or had possession of the key and claims to no longer have it.

The burden of proof is placed upon the individual, however, to prove that the key was not in his possession after the notice was received, or it was not reasonably practicable for him to disclose the key. If the individual fails to prove the above, then he is guilty and may be imprisoned for up to two years.

6.3.4 Offence: Tipping Off

The tipping-off offence is declared in clause B50. Under notice, the disclosure of the key may be kept secret. Recipients of such disclosure orders are not permitted to notify others of the disclosure. Failing to comply may result in a five year prison term.

These powers and offences were shaped and influenced in the bill's passage through the Parliament.

6.4 Evolution of RIP

The Regulation of Investigatory Powers bill was introduced to the House of Commons on February 9th 2000 (Hansard 2000a, Column 250) and brought back for its second reading by Mr. Jack Straw, then Secretary of State for the Home Office, on March 6th 2000 (Hansard 2000b, Column 767).

6.4.1 Process in Parliament

The bill continued on to the House of Commons Committee stage, where it was debated from March 14 to April 6 2000. It then proceeded to Report Stage and Third Reading on May 8 2000 where it was amended further and sent to the House of Lords for consideration.

The bill was introduced to the House of Lords by Lord Bassam, the Home Office Minister, first on May 9th, with a second reading on May 25 2000. Part III was discussed specifically in Committee Stage on June 28 2000, where a significant debate occurred, and the Home Office Minister introduced amendments at the last hour. Part III was then discussed in Report Stage on July 13 2000, when further amendments were introduced. The Third Reading occurred in the House of Lords on July 19th, after which the Bill was returned to

the House of Commons for consideration of the Lords Amendments on July 26 2000. The amendments were commended by the Home Office Minister in the House of Commons and the bill received Royal Assent on July 28 2000.

6.4.2 The RIP Debates

The debates regarding the RIP Bill and those regarding the TTP-regulatory regime were similar in the amount of *furore* generated; in fact the term furore was used by Mr. Ian Taylor in referring the 1997 TTP Consultation document that he previously introduced (Hansard 2000b, Column 795).

When the bill was introduced into Parliament by Mr. Jack Straw, he stated that it was an important bill that represented "a significant step forward for the protection of human rights in this country". It sought to update existing law enforcement activities to secure "a better balance between law enforcement and individual rights".

> Mr. Straw: The Bill is intended to allow the law enforcement agencies to maintain their success record against a diverse series of threats including drug trafficking, money laundering, human trafficking, paedophilia, tobacco smuggling and other serious offences. (Hansard 2000b, Column 768)

With regards to Part III of the bill, Mr. Straw acknowledged "encryption itself is vital to the success of the e–commerce revolution, and helps to prevent certain types of crime, such as fraud on the Internet". However, he pointed out, it can also be used "by criminals to frustrate law enforcement", which "is happening already, and the problems will increase as the technology becomes more available" (Hansard 2000b, Column 775).

Similar statements were made in the House of Lords when Lord Bassam, in an attempt to align industry interests with law enforcement interests, asserted:

> Lord Bassam: Our goal is to make this country the best and safest place in the world in which to carry out e–commerce. I know that industry, too, wants a secure environment in which to operate. (Hansard 2000d, col. 883)

From the reading of Hansard at least three issues are implicated in the legislation. The first is business costs associated with any legislation. The second is the implications for human rights. Finally, there is the problem of legislating technology in a rapidly changing environment.

Business Implications of the Act

Concerns arose that RIP would encourage companies to move out of the UK due to the risks and costs introduced. As articulated by a British Chambers of Commerce commissioned report ('BCC report'), these include the danger of public disclosure of critical company information, increased opportunities for industrial espionage, and reduced trust and confidence in company security (BCC 2000, p.14). The BCC report suggests that the potential danger is that many companies would consider relocating their service provision outside the UK, to countries like Denmark that have decided against policies which require disclosure of keys; though this was disputed by the government (Home Office 2000a; NCIS 2000; Straw 2000b). Some companies did announce their intentions to move their services off-shore, as covered in Whitley and Hosein (2001); however the current status of their intentions is not known to the author.

These concerns were reflected in the various debates. Even Mr. Taylor noted the dangers of creating 'draconian' powers.

> Mr. Ian Taylor: Industry needs to understand fully what the Government intend. (...) It is vital that the cost elements and the burdens on individuals are properly understood. (...M)y purpose (is) to obtain reassurance from the Minister that the attempt to make the penalties as draconian as possible would not mean that almost every company would want to ensure that it placed its private keys with some trusted third party, so that are forced back to a key escrow system. (Hansard 2000b, col.798)

At the committee stage, this was also raised by other members of the Conservative Party, including Mr. Heald who had consulted with industry and reflected what he learned:

> Mr. Oliver Heald: They say: "Any perception by customers and financial institutions that London was less secure because the confidentiality of encrypted messages was not protected as thoroughly as elsewhere could have a significant adverse impact on London's attractiveness as a financial centre. The Government should therefore ensure that the powers of the UK authorities are not out of line with those in other major financial centres." Of course, the powers are out of line with other major financial centres. I am sure that the Minister would be prepared to confirm that he is leading the way bravely. (Hansard 2000c)

Again in the Lords, the concerns of industry were raised.

> Lord Bassam of Brighton: I can state, unequivocally, that we have no intention of placing unreasonable burdens on industry. We recognise that some parts of industry have concerns about parts of the Bill. (...) But it is in no-one's interests to force businesses overseas. (Hansard 2000d, col.883)

Particular concern was raised regarding the tipping-off offence. According to a Conservative peer,

> Lord Cope: A further problem (...) arises from the fact that the person on whom the warrant is served cannot tell anybody else. That may give rise to claims from overseas for breach of contract. It is also likely to lead to overseas companies avoiding using UK services. (Hansard 2000d, col.889)

However, the interests of industry were sometimes represented in other ways. Baroness Thornton, a Labour peer, argued

> Baroness Thornton: I understand also the Government's desire not to frighten off potential investors in our e-economy and to make Britain the best nation in the world in which to do e-business. But surely what businesses and consumers want is a transparent and trusted regime. They do not want the Internet to become synonymous with criminals and shady characters who are a danger to children. (Hansard 2000d, col895)

Representing industry played a large role in Parliament. Often, parliamentarians from all parties would make statements regarding their consultation with industry. In a letter to the Daily Telegraph, the Home Office Minister responsible for the bill, Mr. Charles Clarke, stated

> I believe all the serious commentators with whom we have engaged recognise the importance of and necessity for such a Bill. We have made some significant changes during its Parliamentary passage precisely because we know we have to work in partnership with industry to ensure the Bill has the right kind of impact. (Clarke 2000)

While Lord Bassam made similar claims in the Lords,

> Lord Bassam: The Home Office has spoken formally and informally about this Bill to a large number of organisations. All 40 PTOs (public telecommunications operators) have been invited to a briefing and discussion on the Bill. The ISPA and ISPs generally have been invited. The list also includes: AOL, BT, Demon, Linx, Research Machines, VCB net, BT internet, Energis/Planet Online/Freeserve, Fastnet, Uunet; AICES, OFTEL, FIPR, ICX, AEB, EURIM, ACPO, Royal Holloway College, ISPCon, Scrambling for Safety--I have been scrambling for words after such a list!--and so on. We have consulted very extensively. Other organisations feature on the list, not least the child protection groups. (Hansard 2000d, col.991)

Other political parties also consulted with industry. As Lord McNally, the Liberal Democrat peer, noted in the Committee stage,

> Lord McNally: (W)e have arrived at the crux of the Bill in terms of clearing the hurdle of business disquiet. (...) I was interested in the initial reaction of one of the companies concerned, Vodafone. Its concern was that in seeking a proportionate response, to use a

> favourite expression of the noble Lord, Lord Bassam of Brighton, the provision leant too far towards the requirements of the relevant authorities and failed to take account of the needs of the businesses in question. A good deal of the debate on the clause will revolve around the question whether the powers that the Government seek are proportionate in terms of the real or imagined evils that they seek to counteract and the burdens that they place on business. (...) Industry, which has quite legitimately lobbied and stirred up media and political and parliamentary interests and obtained a response from the Government, should take a proper look at what this means for business. (Hansard 2000f, col.955)

The response from the Home Office was equally referential to industry.

> Lord Bassam: However, there is one consistent and recurring theme: that in bringing forward this legislation we have done some fundamental damage to this industry. I find it hard to accept that. I believe the legislation has been brought forward for entirely the right reason; that is, to find a sensible system of regulation. In doing that, the Government must listen to intelligent and well-founded criticism. The Government have tried to do that. The noble Lord, Lord McNally, referred to Vodafone's off-the-cuff criticism of the Government's moves thus far in bringing forward the amendments today. If Vodafone has further specific points it wishes to put, the Government will continue to listen. (...) Nevertheless, the Government want to ensure the best legislation; legislation that works to the better interests of industry and government, but more particularly industry because that is wealth-generating and is for the good of the country's economy. (Hansard 2000f, col.956)

Lord Bassam continued by mentioning representations of the BCC, the Institute of Directors, and the British Bankers Association. In the light of this, a number of changes were introduced.

> Lord Bassam: I recognise that this is a crucial issue, especially for industry. (...) In the light of those representations, we have decided to recast these provisions. (...) In recognition of the views of industry, we made wide changes to Clause 47 in another place to add an extra test if keys are to be required. (...) We have suggested our own amendments, which take account of the views of industry and cover the majority of points raised by the Committee. (...) We were certainly told by industry that such amendments would offer reassurance. (Hansard 2000f, col.958)

The purpose of the amendments, to be discussed later, was therefore to alleviate industry concerns.

Civil Liberties Implications

Lord Cope regularly consulted and represented civil society organisations' concerns alongside industry concerns.

> Lord Cope: At the start of our debates I was impressed, and I remain impressed, by the sustained opposition made against the clauses

> permitting the police and others to demand keys. That opposition has come from many different groups, ranging from civil liberties organisations through to organisations in the City, the CBI, trade unions and so forth. All those groups have expressed their extreme worries about the provisions as a whole. (Hansard 2000h, col.1065-1066)

Cope, McNally, Phillips and other peers worked with FIPR and other organisations to create amendments to the bill to reflect the concerns of civil society and industry organisations.

This was not a simple process; particularly as the bill was seen by many as a step forward for civil liberties in the UK.

> Mr Jack Straw: This is an important Bill, and represents a significant step forward for the protection of human rights in this country. Human rights considerations have dominated its drafting. None of the law enforcement activities specified in the Bill is new. What is new is that, for the first time, the use of these techniques will be properly regulated by law and externally supervised. That will serve to ensure that law enforcement and other operations are consistent with the duties imposed on public authorities by the European Convention on Human Rights and by the Human Rights Act 1998. (Hansard 2000b, column 767)

The Government was obliged to come up with a statutory basis for invasive investigatory powers; due mostly to the incorporation of the European Convention of Human Rights (ECHR) into the Human Rights Act 1998 (which became effective from October 2000), and related jurisprudence.

There was considerable debate in Parliament and in the media regarding the civil liberties issues, as outlined in legal audits (Beatson and Eicke 1999; Eicke 2000). The grounds for the amendments, however, were articulated mostly as responses to industry concerns.

Technological Environment

A further issue that arose was the challenge of legislating within a technological environment. Despite attempts to make the legislation technology-neutral, technological language emerged from the discourse, most often in dealing with key granularity. Even in introducing the bill, Mr. Straw spoke specifically on the issue of public key cryptography.

> Mr. Straw: A person who does not have possession of the key cannot be guilty of the offence. By definition, the keys are a secret confined to the people who have control of them. One half of the key--the part used by the person communicating data to a recipient--is public; by definition, the other half is private, and that is the part that interests law enforcement agencies. (Hansard 2000b, col.775)

This was later interrogated further by the opposition parties. The definition, sensitivity, and treatment of keys arose as issues.

> Mr. Ian Taylor: (W)hen it comes to confidence in the world of global commerce, it is important to know whether encryption has been entered into and looked at, and whether the private key has been sourced. The inability to tamper with a system is vital, as is confidence that, once encrypted, it is safe and not likely to lead to any commercial loss of security. The integrity of private keys must not be unreasonably jeopardised. If they are, companies will have to consider factors such as the need for global key revocation and change, which will be costly. (...) In clause 52, a definition of "key" is provided that may be a little too vague for comfort. (Hansard 2000b, col.797)

The attempt to be technology-neutral received some scrutiny as well. As the Home Office Minister argued

> Mr. Clarke: The second concern that has been expressed about the Bill relates to key escrow through intimidation. (...) I make it clear to hon. Members and to people outside the House that we shall not force anyone to use a particular technology. Individuals and businesses remain free to utilise any type of encryption, provided they choose the one that best suits their needs. (Hansard 2000b, col.828)

In later discussions in the Lords, it was requested that this be formalised in the bill.

> Lord McNally: The European Encryption Working Group made the following point to me: "We are concerned ... that the Bill as written could lead to the imposition of mandatory technical and design requirements on communications services ... we urge that the Bill be amended to state explicitly that the Home Secretary does not have the authority to impose design and technical requirements upon communications systems and to place the burden of proving possession of the encryption key on the prosecution". (Hansard 2000d, col.892)

This was not followed up upon, however. Among the final words on technological neutrality, the Earl of Northesk stated in opposition to the bill,

> The Earl of Northesk: One of the many difficulties I have with the Bill is that, in its strident efforts to be technology neutral, it often conveys the impression that either it is ignorant of the way in which current technology operates, or pretends that there is no technology at all. (Hansard 2000f, col.1012)

As another instantiation of the level of technological detail in the discourse, the following extract from the Lords Committee Stage discusses the feasibility of the bill; and its circumvention using ephemeral keys, perfect forward secrecy, and even steganography.

> Lord Lucas: Encryption is in theory perfect. (...) Internet communications will use ephemeral keys, and there will be no way of

> breaking that system. Cryptography has evolved in ways which have built-in deniability. The whole way in which the clause has been written assumes that there is only one key, which will reveal one set of information out of an encrypted file. But it is very easy to create a system whereby out of an encrypted file I can produce a Shakespeare sonnet or an order for hard drugs, depending on which key I use to unlock it. There is no way in which the Government can prove that there is a second key if I produce to them a first key. One can hide whole file structures. One can hide the existence of files through the use of keys that go down in layers, so that the first key will reveal one file structure, but if one applied another key it would reveal hidden files below. (Hansard 2000f, col.953)

This view was supported by others,

> Lord Blackwell: The word "key" is widely used in the Bill, and the amendments, as though we were talking about a key that could unlock something simply, like a door to a room. However, developing technology means that, in many cases, keys will not exist in that form. As I understand it, the dynamic generation of new keys may be ephemeral and it may not be possible after the event for somebody to say what the key was, because it was simply generated, used and destroyed.
>
> There are some practical issues that I do not yet understand. Do the Government believe that it is technically feasible after the event to ask people to give them information that will enable them to go back and decode messages that have been encoded and transmitted using such ephemeral keys? I am not sure that it is possible. If the Government think that it is, we need to understand why, and how it can be achieved. If it is not technically feasible, the whole apparatus will fall flat on its face, because everyone will move to those forms of encryption that cannot be caught under the powers in the Bill. Only the honest and the simple will be constrained. (Hansard 2000f, col.967)

The Home Office Minister responded,

> Lord Bassam: The concept of "key" is defined in Clause 52 and it bears some close reading. If there is no key to encrypted data, clearly the powers cannot be exercised. The whole point about encrypted data is that someone somewhere will have the key to that data. That is plain. (Hansard 2000f, col.972)

In the third reading in the House of Lords, feasibility was again raised, but this time in dealing with jurisdiction and globalisation.

> Lord Howell of Guildford: We know (...) that the purpose here is to impose national legislation on what is a global communications system. That is bound to create some limitations on what can be achieved. We also know (...) that technology is moving very fast in this area and may well render some of the provisions of the Bill ineffective almost before it becomes a statute. What worries me about Clause 51 is best put as a question to the Minister. What will happen if a handler of data traffic--a person or persons on whom a disclosure requirement is served--or an Internet service provider, when asked for the key, says, "I do not know where it is. I have no

> idea of its location"? It may be that messages are passing between a giver and receiver within United Kingdom jurisdiction, but it is perfectly possible for the Internet service provider to be in Dubai, the application service provider to be in Bangalore and the key to be anywhere. It could be in Bahrain or it could be moving around. It might not be located in any national jurisdiction and therefore would not be available. (Hansard 2000h, col.1062)

Industry and NGOs were for the most parts responsible for informing Parliamentarians regarding technological details and regulatory feasibility. These educational efforts were not always well received, however. In the final stages of the bill, FIPR released a report claiming that the bill was technologically 'inept' (Brown and Gladman 2000); Mr. Clarke dismissed a comment regarding this report.

> Charles Clarke: However, I do not accept the comments of the Foundation for Information Policy Research quoted by the hon. Member for South Dorset. I would not have responded to this debate except to say that, but I cannot let his remarks stand on the record unchallenged. I accept the genuine feeling with which he said that we had tried to address the point, but not the views of the Foundation for Information Policy Research. We also do not accept that we can do nothing in the face of criminal organisations which work in this way--we must try and deal with the problem. (Hansard 2000i, col. 1186)

Mr. Clarke, in essence, ignored FIPR's articulation as represented by the Opposition; not only because of a different interpretation of the technological, but also because of his dislike of FIPR.

6.4.3 Changes to the Bill

After a significant number of amendments were marshalled in the House of Commons, very few actually passed. In the House of Lords an even larger number of amendments were raised for discussion at the Committee Stage; however the tactics of the Home Office here were different. Rather than debate and be outvoted, the Home Office introduced its own new amendments to the Lords:

> Lord Bassam: Throughout the Bill I have sought to be constructive and to offer constructive opportunities to all to make intelligible and intelligent criticisms. We have invited in all sectors of business. To my knowledge, we have not said, "No, go away" to anyone. That approach has now been widely acknowledged. Therefore, when the Government are criticised for extensively rewriting the Bill, or for putting forward provisions at the very last moment, it is because we have been listening—as we always said we would—and there is no other time when we can make these changes. (Hansard 2000f, col. 957–958)

The most significant change to the bill was the shifting of the default disclosure power. Keys were no longer to be disclosed by default. Rather, the default was changed to

plaintext: an individual can hand over the plaintext to only the specific communications that were intercepted, instead of risking the disclosure of the key that could be used to decrypt all future and other past communications that may be beyond the scope of the notice's authority.

The next significant amendment affected key disclosure to meet the interests of industry. The amendment changed the wording of the tipping-off offence to allow for the notification of the senior officer of a corporate body if the key or information protected by an employee within that body was being requested for disclosure.

A further set of amendments permit the individual to only disclose the keys, at his choosing, that would that satisfy the disclosure notice-period. For example, if Bob creates a key with subkeys for every month, and law enforcement officers arrive asking for the keys to decrypt messages received from Alice during September 26–30, Bob can hand over either the subkey for September, or may even choose to hand over the session keys for each message instead. The key granularity issue first raised in 1997 by critics of the government policy, addressed partly with the separation of signature and encryption keys in 1999, was finally addressed adequately to allow for a settlement.

The reverse burden of proof is also addressed somewhat within the Government amendments at this stage. Removing the "it shall be a defence for that person to show", the amendments place the burden on the prosecution to show that a person was in fact in possession of a key at a specific time, and thus willingly failed to comply with the law. With boldface to show additions, strikethroughs to show deletions:

> (2) In proceedings against any person for an offence under this section, ~~it shall be a defence (subject to subsection (4)) for that person to show~~ **if it is shown that that person was in possession of a key to any protected information at any time before the time of the giving of the section 46 notice, that person shall be taken for the purposes of those proceedings to have continued to be in possession of that key at all subsequent times, unless it is shown—**
>
> > (a) that the key was not in his possession after the giving of the notice and before the time by which he was required to disclose it; ~~but~~
> >
> > ~~(b) that he did, before that time, make a disclosure, to the person to whom he was required to disclose the key, of all such information in his possession as was required by that person to enable possession of the key to be obtained.~~
>
> The individual shall be taken to have shown that he did not have the key only if the prosecution can raise a reasonable doubt.

This change, to a significant extent, placed the burden of proof on the prosecution rather than the individual having to prove innocence/loss, thus limiting the likelihood of this component of the bill being found in contravention to the ECHR and associated jurisprudence.

Some of these amendments are discussed in greater detail below.

Plaintext versus Key

From the earliest days of debates, Mr. Clarke, the Home Office Minister responsible for the bill, stated that the key versus plaintext issue is a non–issue:

> I wish to emphasise one important point. We envisage that the disclosure of the plain text of protected material, rather than a key, will be sufficient in almost all cases responding to a decryption notice and I expect there to be very few cases where disclosure of the keys themselves will be required. (Hansard 2000b, col. 834)

The reason for not changing the original wording, as he elaborates later, is that "our bottom line continues to be that we must retain the flexibility in the Bill to request the disclosure of the key itself in exceptional circumstances" (Hansard 2000c). He accepts that "many in industry have no difficulty with the principle of handing over intelligible data when they were required to do so under some lawful authority. However, they have some worries about handing over the keys". (Hansard 2000c)

However, this explanation did not appease all of the opposition.

> Mr. Heald: The Minister's recent concession when he said that he was considering putting a requirement in the Bill that the key should be obtained only in exceptional circumstances will have knock–on effects for section 46 notices. I imagine that he is suggesting that one category of section 46 notices would require the plaintext and a different section 46 notice would require the giving up of the key, but only in exceptional circumstances. (...) There would need to be a protocol or set of guidelines on how institutions should be approached for either category of section 46 notices. (Hansard 2000c)

At that point, however, the issue was not being entertained.

> Mr. Clarke: We might consider amending the Bill to allow insistence on producing the key only exceptionally and to state what might be exceptional in the code of practice. We might go further and specify that decisions on what is excepted may be escalated to the highest level, so that the Secretary of State or a chief constable, possibly with the approval of a surveillance commissioner or circuit judge if appropriate, would decide whether a circumstance was exceptional according to the code of practice. Obviously, that would set a higher test in the authority regimes than is currently envisaged under the

> Bill. I cannot table such an amendment now, but the Committee will want to know that I am considering those matters and that we intend to return to them on Report. (Hansard 2000c)

The issue was not returned to in the Commons, however, and a recommended amendment from Heald was dropped as a result of the promise of later consideration.

The issue was returned to in the Lords Committee Stage, after further pressure. When Lord Bassam introduced the list of amendments, he stated,

> In the light of those representations, we have decided to recast these provisions. (...) In recognition of the views of industry, we made wide changes to Clause 47 in another place to add an extra test if keys are to be required. (...) We have suggested our own amendments, which take account of the views of industry and cover the majority of points raised by the Committee. (Hansard 2000f, col.962)

The 'extra test' was allowing for the release of any key, thus addressing the granularity issue; while the 'further changes' refers to the re-ordering of plaintext over keys.

In addition to the amendments allowing notification to the corporate directors, shortly thereafter some within industry eased their opposition to Part III of the bill (Clarke 2000).

Burden of Proof

The allegedly reversed burden of proof was first raised within Parliament by the Conservative Shadow Home Secretary in the House of Commons Second Reading:

> Miss Widdecombe: Clause 49 creates the offence of failing to comply with such a notice. Yet the nature of the offence is such that the burden of proving an innocent explanation for failure to provide the key is laid at the door of the accused; in other words, people are presumed guilty unless they can prove that they are innocent (Hansard 2000b, col.781).

The Home Office Minister responded to this accusation at the time with another interpretation:

> Mr. Clarke: (T)he burden falls on the prosecution to prove beyond reasonable doubt that the accused is, or has been, in possession of a key and that he or she failed to comply with the notice. The Bill outlines several statutory defences. ... Innocent people will not suffer under the provisions. As I pointed out, we believe that the Bill is ECHR compatible. (Hansard 2000b, col.834)

Later Clarke had to again respond to criticism.

> Mr. Clarke: It is true that he or she must prove the defence, but they need to do that only on the balance of probabilities. In other words, he or she must explain what has happened. It will be for the court to

> decide whether, on balance, the person is telling the truth. That seems to be an entirely reasonable burden to impose on an accused person. (Hansard 2000b, col. 883)

These arguments were repeated at the Second Reading within the House of Lords when Lord Bassam responded to similar criticism:

> (W)e took issue with the suggestion that the offence reverses the burden of proof. It has also been suggested that individuals can be locked up for two years for forgetting a password. We do not believe that that is likely. We have set out in detail in another place the reasons why we do not believe that it will happen. None the less, we welcome continued debate on how the construction of the offence might be improved. (Hansard 2000d, col. 884)

Further debate ensued, and concern arose in the media. The Home Office changed tact as they introduced amendments to the Committee Stage in the House of Lords.

> Lord Bassam: We have tabled amendments that make it clear that proof of previous possession can lead to a conviction. However, it will not do so if the defendant raises an issue about whether he still has possession of the key. Once that happens, the burden falls back on the prosecution in the normal way. (Hansard 2000f, col.1009)

This was met with approval from the Committee, as Lord Cope acquiesced, "I am glad that the Government have moved on the question of burden of proof. It was important that they should do so" (Hansard 2000f, col.1012).

More amendments followed, including a late amendment in Report stage, introduced by The Lord Cope and The Viscount Astor. This amendment inserted the requirement that the accused must *knowingly* fail to make the disclosure of plaintext or key.

Security of Keys

Two amendments were added at the Report Stage involving the security of the keys. The first required that the keys, once lawfully collected, are stored in a secure manner. The second amendment deals with liability incurred when the key is misused.

> Lord Bassam: My Lords, this amendment addresses a concern that has been put to us on a number of occasions by industry. The concern is that once keys are seized under this legislation and notwithstanding the strict safeguards set out in Clause 55, there remains a possibility that keys could be compromised once they have been seized. Industry is rightly concerned to ensure that that possibility is minimised and that proper sanctions exist in case it occurs. We agree that it would be wrong for the consequences of insecure safeguarding to fall on the owners or users of keys. We also agree, as I indicated on Report, that the duty imposed on public authorities to look after keys should be actionable. In other words, if keys are insecurely stored the responsible public authority can be sued. (Hansard 2000g, col.1073)

This change was purposed to alleviate the concerns of industry (Whitley and Hosein 2001).

6.4.4 Unchanged Issues

The RIP bill received a significant amount of criticism in the media, in Parliament, from industry, and civil liberties organisations (e.g. Davies 2000; Davies, Hosein, and Brown 2000). The pressure peaked at the Lords Committee and Lords Report stages. At the Committee stage, many of the amendments from the opposition peers were made redundant as a result of Home Office amendments. By the Lords Report stage, the opposition peers managed to introduce a selection of amendments, however many were rejected.

The most controversial amendment that was rejected only lost by one vote: the amendment would have required Secretary of State authorisation on each occasion a key (rather than plaintext) was demanded, thus effectively checking the volume of access requests and creating some oversight. The state of affairs remains that all such requests need only be authorised by senior members of the police.

A most interesting amendment attempted to address international policy coherence: if other countries failed to enact similar legislation, the proposed amendment would have rescinded Part III of the bill and thus would have alleviated the off–shore threat, and concerns about human rights. The amendment was rejected, however.

According to Caspar Bowden, then-director of FIPR, as the Bill left the Lords, "It's Zombie legislation. Although clinically dead with macabre wounds, it still lumbers on menacing both individual privacy and commercial confidence" (FIPR 2000). The concluding words were left to Charles Clarke, on the last day as the Bill passed parliament,

> After the Bill receives Royal Assent, we shall work with the industry--and the Opposition, if they are willing--to promote it both in this country and internationally. Given the comments made in the overseas media, we must explain clearly what the Bill is and is not, and why we do not believe it poses a threat to e-commerce in Britain; on the contrary, it will help to achieve the Government's aim of a strong and secure e-commerce economy, to which we are all committed. Propaganda is needed, and I hope that the whole House will help to promote the interests of this country's businesses when the time comes. (Hansard 2000i, col.1209)

6.5 Conclusions

The UK cryptography policy discourse involved a heated debate similar to what occurred in the U.S. As in the U.S., the final settlement differed remarkably in the level of regulation

from what was first announced. An initial attempt at mandatory licensing of one element of e-commerce, trusted third parties, introduced a large debate and a considerable set of consultation responses. This was replaced by a voluntary regime that was argued to be ineffective in practice. The Department of Trade and Industry then intervened directly in the form of the draft Electronic Commerce bill; sections of which were later distributed among the Electronic Communications bill and the Regulation of Investigatory Powers bill.

After the draft Electronic Commerce bill was split in two, the Home Office took over the more contentious aspects that related to law enforcement issues. This was a result of a great deal of controversy over concerns that surveillance considerations were overriding legitimate regulatory needs within e-commerce. However, unlike the DTI and the Cabinet Office, the Home Office's expertise is not in liaising with the business community and many of the problems the legislation faced could be seen to arise from this, as the industry opposition was intense (c.f. (BCC 2000; ISPA 2000)).

Throughout the discourse, a number of issues arose.

First, there was a conflict between secure transactions and the need for certain bodies to be able to access them. E-commerce and law enforcement interests continuously collided, even after attempts to split them apart into two separate statutory instruments.

Second, articulations of costs and risks emerged throughout. The first set of proposals involved an onerous regulatory regime of trusted third parties, and the costs and risks associated with operating such an institution were considered too high for the market to adopt, amongst other reasons. The earlier proposals also failed to differentiate between the types of keys, such as signature and encryption keys, and as a result introduced risks to e-commerce. Under access provisions in the RIP bill, the risk of key disclosure and misuse were of concern to industry. The settlement involved establishing a liability minimisation regime, and disclosure notices sent to corporate directors in the case of keys belonging to employees.

Third, the practical implications of seizing encryption keys for ongoing surveillance leads to interesting technological and human rights implications. The technological issues were addressed mostly through key granularity: after amendments, individuals can now select which keys are disclosed (subkeys, session keys, etc.). The human rights issues involve particularly due process considerations. An authorisation process for accessing keys involving judicial warrants (as promised in the Labour Manifesto), or the Home Office Secretary signs the warrant (as in a failed amendment); was settled in the RIP Act 2000 by requiring authorisation from a senior police officer. Similarly, the treatment of reverse

burden–of–proof of lost/destroyed keys was addressed to some extent in an accepted amendment. The issue of self–incrimination, i.e. an accused handing over information that can be used to generate evidence to incriminate, remains unresolved.

Fourth, governments must attempt to legislate within the context of a rapidly changing technological environment. Often times in the Hansard the parliamentarians noted that all these issues would have to be revisited as the technology continued to change. Moreover, bypassing the statutory powers of RIP is not technologically challenging, and as a result the Act may have to be revisited to increase its applicability.

Finally, the global infrastructure and the nature of commerce involving information and communication technologies implies that regulation that imposes too much on industry may result in a situation of regulatory arbitrage as companies or services move off–shore. This was raised throughout, ranging from the barriers to the marketing and use of non-UK licensed TTPs, the concerns regarding companies moving off shore, and finally under RIP, companies and individuals moving their keys off-shore or beyond government access (Brown and Gladman 2000).

Recalcitrant Technology?

In this study, the technological recalcitrance was not addressed in the same way as in U.S. discourse where systems actually failed. Here we saw articulations of risks and costs; and how policy could harm technology and markets, e.g. escrowing of signature keys.

Even the parliamentarians noted that technology could be developed to enable circumvention. This is a criticism that dates back to the earliest proposals, where it was stated that the only the innocent individuals would comply because the criminals could circumvent the proposals with little effort.

The RIP Act may represent a narrow understanding of technology. Despite detailed discussion of session keys, perfect forward secrecy, signature keys and decryption keys, the Act could not possibly cover all situations. As reports from FIPR (Brown and Gladman 2000; FIPR 2000) outline, technologies are freely available; while the *means* to do so are in some cases inscribed in practice.

For example, another FIPR report (Gladman 2000) outlines how the tipping-off offence is rendered useless by the very simple practice of key-revocation: if an individual feels that his key has been compromised, he may revoke it, and create a new one; this is a common practice with certificates. Under RIPA the individual may not disclose to anyone that his

key has been disclosed to government authorities, but he may revoke it and thus prevent anyone from sending future documents or messages to him under that key, constraining government's surveillance power. Norms and practices within the community of e-commerce have already weakened the powers in RIPA. Even if government wished to legislate against these, it is unlikely considering the impacts that this would have on e-commerce, where key revocation is considered necessary and essential to trust. Therefore a norm, dictated by socio-technological practice circumvents policy.

Articulations and Speaking Authoritatively

Whether the UK's economy has been hurt by the regulatory shifts on e-commerce remains to be known, if it can ever be ascertained. As Lord Cope argued

> So far this Bill has of itself been extremely damaging to Britain's interests because of the perceived threats that it poses. Even if in the course of debates we make amendments which produce a Bill that is 100 per cent acceptable some of that damage will remain. I do not want to expand too much on that point at this stage, but I firmly believe that that is the case. (Hansard 2000h, col. 956)

He claims that the very perception of harm can indeed be harmful; which Charles Clarke seems to note as he made the case for propaganda. The United Kingdom was the first western democracy to pursue government access to keys; while other countries have mentioned similar proposals, few have pursued the issue to date.

Many parliamentarians, civil libertarians, and industry representatives purported to speak for industry, or to speak authoritatively on cryptography, keys, and algorithms. The same occurred for other actors: opponents' motives were "impugned" as they were claimed to be "playing into the hands of some of the most evil criminals on this planet" (Hansard 2000e, col.652) (comments from Mr. Clarke and Mr. Andrew Miller respectively), or argued to be from "vested interests" (Straw 2000a) bent on scaremongering (NCIS 2000). This was also seen in the rebuttal from Charles Clarke regarding the circumvention of RIP on the last day of testimonies, dismissing ideas by dismissing the source (FIPR); while industry representatives were hailed and celebrated as badges of support.

Government access to keys does create some human rights and industry challenges, just as encryption is a challenge to law enforcement and national security interests; viewing these challenges as socially-imposed burdens or technologically-determined obstacles does not reflect the debate that arose. As the policy debate grew, it appeared to take on more technological properties (e.g. key granularity, x.509 flags, and ephemeral keys); but

technological discussions were simultaneously social (e.g. assessing implications of disclosure on trust, self-incrimination, and reverse-burdens).

The debate was socio-technological: articulations of the ways that the technology worked (parliamentary briefings by FIPR and speeches by parliamentarians), articulations of risks and costs (BCC and Risks of Key Recovery report, and discussion of the costs of crime (NCIS 2000; Straw 2000b)), and norms and practices (e.g. revocation and trust mechanisms).

From 1996 through to 2000, the policy environment for e-commerce and cryptography transformed as a number of regimes of regulation were proposed and used, shaped and discarded, and some implemented. At some point in the future, *e-commerce* in the UK may be articulated without any regard to the *government access to keys* policies just as one day the U.S. *export controls* will be separated from *cryptography products*; as *Joliot* was from his *nucleus*, through translations. Due to the landscape over the years covered in this study, however, the two issues were inseparable. Without monitoring socio-technological discourse, a number of issues would be poorly understood, including: the origin of UK's concern for creating the 'best and safest' economy in the world; why certificate revocation may occur quietly with no explanation; the resistance towards using the term 'trusted third party' within e-commerce discussions.

In Section III of this dissertation I will summarise and analyse these developments, along with the discourse presented in chapter 5. These stories will be analysed to try to understand the reversals of the policies, and how these can be explained from the literature presented in Section I.

Endnotes

1. In my review I identified a recalcitrant submission from Nicholas Bohm (1997), a legal expert, who carefully made the point that digital signatures do not require legal standing. This is a methodological point at best, to show the value of substantive review.

References

ABA. *Response to the Department of Trade and Industry's Licensing of Trusted Third Parties for the Provision of Encryption Services*. American Bar Association Science & Technology Information Security Committee, 1997.

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L., Schiller, J. I., and Schneier, B. *The risks of key recovery, key escrow, and trusted third party encryption*. 1998.

Anderson, R. *Response to the DTI*. Cambridge, 1997.

BCC. *The economic impact of the Regulation of Investigatory Powers Bill: An independent report prepared for the British Chambers of Commerce*. London: British Chambers of Commerce, 2000.

Beatson, J., and Eicke, T. *In The Matter Of The Draft Electronic Communications Bill And In The Matter Of A Human Rights Audit For Justice And FIPR*. October 1999.

Bell, N. *Letter in response to the DTI proposal*, 1997.

Bohm, N. *Licensing Of Trusted Third Parties For The Provision Of Encryption Services, Comments On The DTI Public Consultation*. 1997.

Brazier, J. *Response To The DTI Public Consultation Paper Licensing Of Trusted Third Parties For The Provision Of Encryption Services, Version 1.0*. Professional Projects Company Ltd, 1997.

Brown, G. *Speech by The Chancellor Of The Exchequer: 'Meeting The Challenge Of The Internet Revolution'*. London: UK Internet Summit, QE II Conference Centre, 1999.

Brown, G. *Speech by Gordon Brown on Britain and the knowledge economy, London, 16 February*. Labour Party, 2000.

Brown, I., and Gladman, B. *Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses*. Foundation for Information Policy Research, 2000.

BSA. *Comments to the UK Department of Trade & Industry on The Licensing of Trusted Third Parties for the Provision of Encryption Services*. Business Software Alliance, 1997.

BT. *BT Comments on the Public Consultation Paper "Licensing of Trusted Third Parties for the Provision of Encryption Services"*. 1997.

CBI. *CBI Response to the DTI Public Consultation Paper on Detailed Proposals for Legislation for Licensing of Trusted Third Parties for the Provision of Encryption Services*: Confederation of British Industry, 1997.

Clarke, C. "Letter to the editor: Crime and the net." *The Daily Telegraph*, 13 July 2000.

CR&CL. *First Report on UK Encryption Policy, 'A Reply to the DTI Public Consultation Paper on Licensing of Trusted Third Parties For the Provision of Encrypt ion Services'*. Cyber-Rights & Cyber-Liberties (UK), 1997.

Data Protection Registrar. *Response Of The Data Protection Registrar to the Licensing Of Trusted Third Parties For The Provision Of Encryption Services, A Public Consultation Paper on Detailed Proposals for Legislation*. 1997.

Davies, S. "How your privacy could soon RIP: Simon Davies fears government plans for online surveillance will devastate e-commerce." *The Daily Telegraph*, July 12 2000.

Davies, S., Hosein, G., and Brown, I. "Letter to the Editor: Bullying minister." *The Daily Telegraph*, June 20 2000.

DTI. *Paper On Regulatory Intent Concerning Use Of Encryption On Public Networks*. London: Department of Trade and Industry, 1996.

DTI. *Licensing Of Trusted Third Parties For The Provision Of Encryption Services Public Consultation Paper on Detailed Proposals for Legislation*. London: Department of Trade and Industry, 1997.

DTI. *Secure electronic commerce statement*. London: Department of Trade and Industry, 1998a.

DTI. *Summary of Responses*. London: Department of Trade and Industry, February 3 1998b.

DTI. *Building Confidence In Electronic Commerce*. London: Department of Trade and Industry, 1999a.

DTI. *A report for the DTI summarising responses to "Building Confidence In Electronic Commerce"*. London: Department of Trade and Industry, 1999b, URN 99/89.

DTI. *Summary of Responses to PROMOTING ELECTRONIC COMMERCE Consultation on Draft Legislation and the Government's Response to the Trade and Industry Committee's Report (Cm 4417)*. London: Department of Trade and Industry, 1999c.

ECB. *Electronic Commerce Bill*. London: Department of Trade and Industry. 1999.

Eicke, T. *In The Matter Of The Regulation of Investigatory Powers Bill And In The Matter Of A Human Rights Audit For Justice And FIPR*. 2000.

EURIM. *Response to DTI Consultation Paper on Licensing of TTPs: A EURIM Position Paper*. European Information Society Group, 1997.

FIPR. *Analysis of the (draft) Electronic Communications Act 1999*. Foundation for Information Policy Research, 1999.

FIPR. *News release: Second and final day of the House of Lords Report Stage debate on the Regulation of Investigatory Powers Bill*. Foundation for Information Policy Research, 2000.

Gladman, B. "Key Recovery -- meeting the needs of users or key escrow in disguise?" In *EPIC Cryptography and Privacy Sourcebook 1998*, ed. David Banisar. Washington, DC: Electronic Privacy Information Center, 1998.

Gladman, B. *The Regulation of Investigatory Powers Bill: Key Revocation, Government Access to Keys and Tipping-Off*. Foundation for Information Policy Research, 2000.

Hansard. "House of Commons 9th February 2000 (First Reading)." 2000a.

Hansard. "House of Commons 6th March, 2000 (Second Reading)." 2000b.

Hansard. "House of Commons Committee 4th April, 2000 (Committee Stage)." 2000c.

Hansard. "House of Lords 25th May, 2000 (Second Reading)." 2000d.

Hansard. "House of Commons Hansard Debates", 26 June 2000 (pt4). 2000e.

Hansard. "House of Lords 28th June, 2000 (Committee Stage)." 2000f.

Hansard. "House of Lords 13th July, 2000 (Report Stage)." 2000g.

Hansard. "House of Lords Third Reading 19th July, 2000." 2000h.

Hansard. "House of Commons Hansard Debates", 26 July 2000 (pt25). 2000i.

Hansen, D. *Letter to Ian Taylor*. July 14 1997.

Home Office. *Interception of Communications in the United Kingdom: A consultation paper*. Home Office, 1999.

Home Office. *Myths and misunderstandings*. Home Office, 2000a.

Home Office. *Progress of Legislation for Regulation of Investigatory Powers Act 2000*. Homeoffice.gov.uk, August 4, 2000b.

Hosein, G. "Consultation and Contemplation -- What has Gone Before: a summary of the first UK Cryptography Policy consultation process." In *The 1998 Electronic Privacy Information Center Sourcebook*, ed. David Banisar. Washington, D.C., 1998.

HP. *Hewlett-Packard Ltd. response to the DTI's consultation paper on "licensing of Trusted Third Parties for the provision of encryption services"*. John Taylor, Director, HP Labs Bristol, Stefek Zaba, 1997.

Hyperion. *Response to the publication by the DTI of a proposal on the licensing of trusted third-parties, Neil McEvoy (1997)*. Hyperion Systems Limited, Neil McEvoy, 1997.

Intel. *Response to the UK Government consultation paper on the licensing of trusted third parties for the provision of encryption services*. Intel Corporation (UK) Ltd., 1997.

ISPA. *Response to the Smith Group Report for the Home Office on Technical and Cost Issues Associated with Interception of the Internet*. 23 May 2000.

IT. *Response to DTI*. I.T. Consultancy Limited, 31 May 1997.

Labour Party. *Manifesto*. 1997.

Leech, J. *Letter to Nigel Hickson, Subject: Licensing of TTPs for the Provision of Encryption Services*. May 27 1997.

Lindsey, C. *Comments on the DTI proposals for the Licensing Of Trusted Third Parties*. May 22 1997.

LSEW. *Licensing of Trusted Third Parties for the Provision of Encryption Services, Consultation Paper published in March 1997 by the Department of Trade & Industry - an Information Society Initiative*. Law Society of England and Wales, 1997.

NCIS. *NCIS hits back at opponents of Regulation of Investigatory Powers Bill*. London: National Criminal Intelligence Service, 2000.

PIU. *Encryption and Law Enforcement, a Cabinet Office report*, Performance and Innovation Unit, 1999.

Straw, J. *Letter to the Editor of the Daily Telegraph*, June 16, 2000a.

Straw, J. "Letter to the editor: Bill will not cause e-commerce to decamp", *Financial Times*, 15th June 2000b.

TMA. *The TMA Response to the DTI Consultation on the Licensing of Trusted Third Parties for the Provision of Encryption Services*. Telecommunications Managers Association, May 30 1997.

UCISA. *Universities and Colleges Information Systems Association (UCISA) response to DTI consultation paper on the Licensing of Trusted Third Parties for the Provision of Encryption Services*. Universities and Colleges Information Systems Association, 1997.

UK Notarial Forum. "Response to the DTI Consultation Paper, Comment,." *The Journal of Information, Law and Technology (JILT)*, Number 3, June 1997.

Whitley, E. A., and Hosein, I. "Doing politics around electronic commerce: Opposing the Regulation of Investigatory Powers Bill." A paper delivered at the Realigning Research and Practice in IS Development: The Social and Organisational Perspective, Boise, Idaho, 2001.

Chapter 7: Understanding Socio-Technological Regulatory Discourse

1902: A Ban on Coded Cables. **Washington**: Colombia has officially announced that she will not permit cipher dispatches to pass from her territory to foreign countries. This surprising attitude is described in a despatch received by the Navy Department. No notice will be taken of the Colombian announcement unless there should be an actual interference with the despatches of American officers. It is pointed out that under the treaty with New Granada the United States is empowered to preserve communication across the isthmus.

-- International Herald Tribune, In Our Pages 100, 75, & 50 years ago

Building real-world cryptographic systems is vastly different from the abstract world of most books on cryptography, which discuss a pure mathematical ideal that magically solves your security problems. Designers and implementers live in a very different world, where nothing is perfect and where experience shows that most cryptographic systems are broken due to problems that have nothing to do with mathematics.

-- Bruce Schneier, on the release of Practical Cryptography, March 2003

Abstract

In Section II of this dissertation two discourses were presented involving the cryptography policies in the United States and the United Kingdom. This data was collected and presented by theories and methodologies based on capturing socio-technological discourse, as presented in Section I. The purpose of this chapter is to analyse the issues that arose from each discourse: the actors, the alliances, the principles, and the regulatory devices proposed and used. I will present the socio-technological discourses as regulatory discourses consisting of shifts in regulatory regimes. This will lead to chapter 8 where these ideas are discussed in the context of other technology policy discourses.

7.0 Introduction to the Analysis of Regulatory Shifts

Although the two discourses presented in Section II were different in form and procedure, each involved a set of regulatory regimes that were negotiated and transformed. Focusing on moments of interest, and looking specifically at technological issues forced a socio-technological representation of the discourses. While it is possible to view each case as the collection of human actors with interests, as the regulation literature often practices, I propose in this chapter that the socio-technological discourse is richer.

The shifts in regulatory regimes that occurred in each discourse may be described in a number of ways; in this chapter I will present a synthesis of how the actors, interests, principles and translations appeared in socio-technological discourses. Expressing the socio-

technological discourse as a regulatory discourse will allow me to develop and express my argument for why we may wish to reconsider traditional explanations.

Each discourse involved a number of actors, a multitude of interests, articulations of risks, costs; not uncommon to other regulatory discourses. Additionally, each discourse involved technology, through representations, translations, and objections. The purpose of this chapter is to analyse the flow of the discourse, the actors, the interests, alliances, the strategies and the regulatory devices proposed and used; in essence the programmes of action (Latour 1991, p.125), achieved through translation (Callon 1991, p.143). This analysis will follow the framework proposed by Braithwaite and Drahos (2000) who study global regulatory discourse as a web of actors, including Haas' (1992) notion of the epistemic community, and as a contest of principles. I will argue that understanding the cryptography policy regimes (Braithwaite and Drahos 2000, p.26) and their changes (Hood 1994) requires an appreciation of the technological actor amidst the many other actors in the discourse.

In §7.1 I will argue that the socio-technological discourses may be interpreted as regulatory discourses. Sections 7.2 and 7.3 will review each discourse and emphasise the regulatory regimes and their transformations. Using the Braithwaite and Drahos framework of analysis, §7.4 will review the mechanisms, actors, and the conflict of principles and the translations, while §7.5 will discuss of some implications to the regulation literature.

7.1 Socio-Technological Discourse as a Regulatory Discourse

The cryptography policy discourses that I presented were socio-technological representations of a discourse involving a heterogeneous set of interactions (Latour 1991). In chapters 5 and 6 I argued that each representation of the discourse was enriched by not using deterministic accounts of either the social or the technological.

In the U.S. discourse, although arguments of technological determinism could explain that governments could never control the technology, such accounts would not explain why cryptography policy was such a controversial political issue. Nor would a technological determinist account explain why solutions like PGPADK, Microsoft CAPI, Lotus WFR were developed; these were less 'efficient' and more 'complex' solutions that were not immediately derived from the laws and practices of cryptography and computer science, nor from the 'needs of the market'. It is also unlikely to account for the lack of adoption of Clipper: a market was created by the policy, the technology was available and affordable and provided a solution to a consumer interest in privacy.

At the same time, however, a purely social account would not be able to account for the rise of concerns regarding the risks of key recovery, recommendations on minimal lengths of keys, and the role that faster computing technologies played in changing export policies. Nor would such accounts describe the failure of Clipper on technological grounds, the articulations of complexity, costs, and infeasibility from a number of actors including government officials, industry representatives, scientists and experts, and advocates. Even if social accounts included these actors, it would be impossible to resolve their differing interpretations on key sizes, costs, and risks.

Similarly in the UK discourse, the very presence of a discourse of social actors discounts a technological account; while the risks and costs articulations, and resistance to proposals despite social incentives (e.g. licensing) discourages the viability of social accounts. A socio-technological description was able to account for the inclusion of actors and principles that solely technological or social accounts would not. Technological accounts are dismissed in the debates in Parliament on grounds of political friction amongst actors; while the technology is said to have structured many of the debates regarding such fundamental rights as the presumption of innocence and rights to privacy.

Collecting and representing data at the moments in a discourse where capacities are interrogated, articulations are stated, objections arise and recalcitrance emerges, as indigenous and exogenous forces appear, permits a more socio-technological explanation. My presentation of the data resulted in this situation where we can identify actors, try to ascertain the multitude of interests involved, interrogate the capacities, and make sense of the translations, forces, and objections. In turn, we may try to understand the contest of principles that occurred.

A framework for understanding regulatory discourse is offered by Braithwaite and Drahos in their compendium on the development of various global business regulations. In this work, they use Latour's ideas to understand how actors, principles, and mechanisms make up regulatory discourse. Their studies are centred on the idea that regulation is

> a process in which different types of actors use various mechanisms to push for or against principles. (...) Principles are abstract prescriptions that guide conduct. (Braithwaite and Drahos 2000, p.9)

Regulatory mechanisms are the tools that actors use to achieve their goals. Understanding the contest of principles surrounding the mechanisms is key, they argue (p.15); but we should not expect that a single mechanism or a single principle necessarily rules and wins.

> Dense webs of influence are needed to pull off an accomplishment as difficult as establishing a (...) regulatory regime that secures

> compliance of relevant actors in business and the state. Such webs are dense in the sense of involving many types of actors mobilizing many types of mechanisms. (p.13)

Their compendium lists the most likely actor-categories who participate in policy discourse, who are constituents to the webs of influence. These are summarised in Table 7.1.

Mechanisms	Actors	Principles
? military coercion	? Organisations of states	? lowest-cost location
? economic coercion	? states	? world's best practice
? systems of reward	? business organisations	? deregulation-decentralisation
? modelling	? corporations	? strategic trade
? reciprocal adjustment	? Non-Governmental Organisations	? rule compliance
? non-reciprocal coordination	? Mass publics	? continuous improvement
? capacity building	? Epistemic communities of actors	? national sovereignty
		? harmonisation
		? mutual recognition
		? transparency
		? national treatment
		? most favoured nation
		? reciprocity

Table 7.1 Adapted from Braithwaite and Drahos (2000, p.24-26)

This framework will be related to the cryptography policy types presented in Section I.

> *Type 0*
> Restricting the development, implementation, and use of cryptography.
> *Type I*
> Policies affecting the development, implementation and use of algorithms
> *Type II*
> Policies of allowing for lawful access to keys
> *Type III*
> Policies maintaining capacities to brute-force keys

Table 7.2 Cryptography policy types. See chapter 1

Type 0 policies were not pursued seriously in either the U.S. or the UK; while all the other types of policies were introduced in some form or another. The remainder of this chapter will identify the policy types used in each regime shift in both discourses, while also identifying the primary actors, mechanisms, and translations.

7.2 A Regulatory Discourse: Policy Shifts in the U.S.

A number of regulatory regimes were proposed in the United States to limit the development, proliferation and use of cryptography. There are three identifiable phases to the policy discourse: pre-1990s regime, the domestic policy regime involving escrow/recovery, and foreign-domestic regime using export controls.

7.2.1 Pre-1990s: Primarily Type I Policies

Up until the 1990s, the U.S. government worked mostly on trying to control the development, adoption, and proliferation of algorithms. These type I policies were usually regulated actively by the National Security Agency (NSA) and formally by the Department of State (DoS), under export controls and classified as munitions.

The NSA had two missions, however: to ensure its capacity to intercept and analyse international communications, and to ensure that domestic communications were secure. These missions came into conflict in the 1970s in the design of *DES*, when the NSA suggested changes. These changes generated some concern that the NSA was introducing weaknesses. In fact the NSA proposed two changes, one that removed a potential fault and another that moved towards a type III policy by restricting the key-size. The restriction of key lengths to 56-bits was articulated as being for engineering purposes; cryptographers now discount that, although most accepted that 56-bits was sufficient security at the time, considering the existing computing environment.

This acceptance of 56-bits faded in the 1990s as computing technology grew more powerful, and as computer scientists and mathematicians developed abstract and real techniques (such as DESCracker) to *brute force* shorter keys, as experts declared that shorter keys were no longer required for engineering purposes, and longer keys were required for effective protection against faster computers and cracking methods (Blaze and others 1996). A number of conflicting articulations emerged at this point of controversy. The Federal Bureau of Investigation (FBI) claimed that 56-bits was too strong, a claim supported by the NSA, even as DESCracker's development manual was published on the Internet showing that this was not the case.

The NSA acted similarly in the development of the standard for public key cryptography. Here the NSA pushed for its own algorithm, over the market standard, *RSA*. The NSA proposal, now the *Digital Signature Standard* (*DSS*), only allows for signature-creation and verification, while *RSA* permits encryption as well. This can be seen as the NSA acting in a consistent manner with some of its regulatory interests: if *RSA* was established as a standard for signature-creation and verification, all those using *RSA* would also be able to use its encryption-decryption functionality. The NSA managed to de-couple, at least within the standard, the e-commerce regard for authentication from the e-commerce and privacy concerns with confidentiality.

It may be said that *DES* and *DSS* are both socially constructed/shaped algorithms to meet the interests of the U.S. Government to promote security but also to maintain their

capacities to make sense of intercepted data. These interests conflicted in *DES*, but converged with *DSS*.

Cryptography increasingly became an issue with the growth of computing and networking resources, while there was increased knowledge regarding cryptography outside of government agencies, and industry began to develop applications for use in the market.

7.2.2 Domestic Regime: Type II Policy

The Clipper Chip policy regime was the U.S. government's first formal attempt at ensuring lawful access to keys through key escrow. This was a socially constructed technology to find a 'balanced solution', developed by the NSA, enrolling high-level actors within the Clinton Administration.

This policy was a case of direct intervention into the market, but through indirect regulation (Lessig 2000): use of Clipper was not legally required, but its use in the market was being supported to meet a similar outcome. The Administration had succeeded in translating AT&T's interests in selling a secure phone into selling a Clipper-embedded phone. The U.S. Government would provide AT&T with its first customer, ordering several thousand phones immediately, thus providing AT&T with an incentive, and hopefully through network externalities (Arthur 1988), even more clients.

The closed algorithm, *Skipjack*, raised a number of concerns, despite articulations from the NSA directorate claiming that the 80-bit keys and the secret development process made it secure. As a large key meant that it could not be brute forced, the government argued that proper warrant procedures would have to be adhered to by agencies. However, the secrecy of the algorithm raised the suspicion of security specialists and cryptographers. They worried that backdoor access was designed into the algorithm to let government circumvent the warrant process, for example by limiting key ranges. That is, there were concerns that the Clipper regime was truly a type I-III hybrid, only disguised as a type II policy.

As Latour argues, however, society is not stable enough to project itself into an object (Latour 1999, p.179). Even while it was designed in the interests of national security and law enforcement, Clipper exhibited other characteristics. Flaws in the black box were found by Blaze (1994) and means for circumvention were identified. The flaw was a part of the design of the *Escrowed Encryption Standard*, and could not easily be fixed. These findings resulted in a front-page article in the New York Times, which coincided with a time of great opposition, including the Sink Clipper campaign and the petition with over 50,000 signatures opposing the policy.

Testimonies to Congress and special reports from academics, specialists, cryptographers, scientists, NGOs, industry associations began appearing, referring to key escrow as a 'step backwards' in security, a threat to industry, and to civil liberties. Civil libertarians spoke of the privacy and human rights concerns as well as technological details; experts and specialists spoke of civil liberties and threats to the information infrastructure; and industry representatives spoke of harm to business, civil liberties, and security of the information infrastructure. Coalitions formed as a number of NGOs concerned with electronic privacy issues found their roots in this movement. Translations were bountiful, contingent coalitions were formed. Clipper as a domestic socio-technological regime of intervention was eventually abandoned as a policy.

7.2.3 Foreign-Domestic Regime: Type II-Type III policy

With the domestic regime threatened by an alignment of NGOs, industry, and an increasingly organised epistemic community, the Clinton Administration created a new strategy, again using export controls. First, the term *key escrow* was replaced with *key recovery*. This was an attempt to translate the interests of industry who may feel that their business clients may wish to retain access to employees' keys in case of accidental loss. Second, the infrastructure that would *verify the authenticity* of public keys (the Public Key Infrastructure (PKI)) was translated into an infrastructure to *recover the private encryption keys*, the Key Management Infrastructure (KMI). Third, export controls *restricting export of strong cryptography* were translated into an export regime *liberalising strong but recoverable cryptography*.

Industry, for the most part, did not immediately oppose this new regime. The regime could be interpreted as export control relief, so long as industry could find means of implementing key recovery. Industry would have to convince their foreign clients that key recovery, as defined by the U.S. policy, would meet the market's interests. The Key Recovery Alliance (KRA) was founded, as industry expended research and development costs trying to find solutions to the problems posed.

The community of experts on security and cryptography generally opposed this new scheme, as did civil libertarians. The latter saw this new proposal as a means of meeting the domestic interests of the FBI and other law enforcement agencies because the 'voluntary' KMI would become the national standard, and software firms would develop one version of their products for both international and domestic use; thus maintaining the goals of the Clipper regime. The former community, in two separate reports (Abelson and others 1998; Lloyd and Oorschot 1998) found that the costs and risks of the proposed regime were unbearable and rendered the system infeasible, and with a limited likelihood of success. The Risks of Key Recovery report, stated

> Key recovery systems are inherently less secure, more costly, and more difficult to use than similar systems without a recovery feature. The massive deployment of key-recovery-based infrastructures to meet law enforcement's specifications will require significant sacrifices in security and convenience and substantially increased costs to all users of encryption. Furthermore, building the secure infrastructure of the breathtaking scale and complexity that would be required for such a scheme is beyond the experience and current competency of the field, and may well introduce ultimately unacceptable risks and costs. (Abelson and others 1998)

In a sense these articulations may be interpreted as Cost-Benefit Analyses (CBAs), and as a result may suffer from the criticisms from the regulation literature of bias, an over-emphasis on efficiency, and "spurious elaboration and levels of technicality that impede policy discussions" (Baldwin and Cave 1999, p.95). While it is possible to discount such CBAs as mere interpretations, using a form of Latourian-triangulation, however, we can see cross-actor-category support for these results. These risks can be interpreted as being confirmed by a report from the NSA (National Security Agency Undated, but prior to 1994), and by the KMI task-force, TACDFIPSFKMI, when it was unable to come up with a viable standard (Pressman 1998).

Industry also began to notice problems, and understood the complaints of the civil libertarians and the epistemic community of specialists, and voiced these concerns e.g. (Holleyman 1995). As Microsoft's lawyer noted in testimony, "(t)he Administration's policy is an attempt to use export policy to control the domestic use of encryption" (Rubinstein 1997).

While the government and other proponents of the policy argued that key recovery could be built in to the technology and identified a number of vendors, further interrogation showed that the vendors of *key recovery* were developing *business key recovery* rather than *key escrow*, as was presented in the case of Entrust Technologies. Session keys were not being recovered, wiretaps would not be effective, and surreptitious access to keys remained non-trivial.

Even Pretty Good Privacy's solution did not, by design at least, allow for surreptitious access to data as the user would be aware of the additional decryption key. This solution encountered problems as it was later found that there was a flaw in the code that allowed (apparently unintended by design) surreptitious replacement of the alternative decryption key and thus decreasing security for all users and affecting trust in the application. Specialists commented that this justified the claims of the authors of the Risks of Key Recovery report.

The international market for the development of strong unescrowed keys developed and in turn, led to an increase in foreign availability of products. This was despite promises from the U.S. Government and attempts by the Clinton Administration through its 'Crypto-Tsar', Ambassador Aaron, to ensure the adoption of key recovery policies in other countries. Using the language of Braithwaite and Drahos (2000), the U.S. Government was hoping for the mechanism of reciprocal adjustment that other countries would adopt key recovery policies.

To placate concerns, the Administration shifted the regulators and instruments. Cryptography was removed from the U.S. Munitions List and rested solely as a dual-use good under the Export Administration Act, thus being shifted from the responsibility of the Departments of State and Defense to the Department of Commerce (DoC) under the Bureau of Export Administration (BXA). Regardless of these shifts, articulations arose of loss of sales and loss of contracts by U.S. industry to foreign competitors.

No longer seen as munitions, partial and sectoral liberalisation then occurred. The partial-liberalisation resulted in the development of *step-up crypto* for Secure Sockets Layer (SSL). This scheme allowed for the export of cryptography that could be enabled as strong encryption (128-bit) so long as it was used only in specific industries, e.g. financial and medical. This claimed cartelisation of strong cryptography quickly became a badge of trust for foreign e-commerce firms. However, the development of the alternative *SSLeay* outside of the jurisdiction of the U.S. controls, as well as the development of 'patches' such as Fortify that implemented 128-bit SSL world-wide provided a circumvention to the U.S. regulations, and thus to the industry protections. The code for each application was mirrored worldwide, while SSLeay was implemented in popular webserver software, and quickly the privilege of the claimed 'cartel' eroded. Baltimore Technologies, an Irish-based company did not need to concern itself with mirroring, however; as Ireland's export regulations were looser, Baltimore's patch to SSL could be downloaded directly from their web site.

Industry in the U.S., while lobbying against the controls, was developing *appropriate* technology for export; holding many interests at a given moment. Microsoft held grave concerns about export controls as they generated higher testing and production costs, and made distribution more difficult. As a result Microsoft, and with the Business Software Alliance, testified often in protest against the regulations. Meanwhile, Microsoft developed the Cryptographic Application Program Interface (CAPI). CAPI had to be designed in a specific way so that it could not be *patched*, i.e. it could not be crypto-with-a-hole. This resulted in the development of a system where Microsoft acted as an obligatory passage

point to the use of cryptography within its operating system, having to sign all cryptographic modules (CSPs) only once they were authorised by the U.S. Department of Commerce BXA. This propelled the U.S. policy through providing extra-jurisdictional reach: CSPs developed outside of the U.S. would have to meet U.S. export control requirements, presumably with weak encryption or key recovery. This solution further damaged the public trust in Microsoft, particularly with the discovery of NSAKEY. This key was later found to be innocuous, but only after significant interrogation about its placement, its functionality, and its ability to be replaced.

Lotus also lobbied; and developed a 'negotiated' solution, Workfactor Reduction (WFR). Lotus was permitted to sell stronger encryption (64-bits) to foreign clients than its competitors, while ensuring that once the keys are captured, the NSA would only have to brute force 40-bits in order to decrypt the information. Although Lotus developed this system openly, it became particularly controversial when the Swedish government discovered that the NSA's interests were embedded within the code of the Lotus Notes used by civil servants. This was again raised in a study of the NSA and its global surveillance programmes, even though the claims (Campbell 1999a; Campbell 1999b) contained inaccuracies. This points again to the importance of appropriate interrogation of the capacities claimed by actors; politics may be discovered by opening the black box, but we must be careful in identifying exactly what the politics may be.

As reports of losses to U.S. industry, increases in foreign availability, partly due to off-shore development, and claims of technological risks, failures, and circumvention, the U.S. government began to increase the frequency of export controls liberalisation. While other strategies were proposed in the Congress such as tax breaks for companies developing key recovery products, or the requirement that any interaction with government agencies required the use of key-recovery enabled encryption, these strategies were not adopted by the Clinton Administration.

Liberalisation reduced the policy to a one-time review by the NSA, then to mere notification of the existence of the products. That regime even acknowledged the ability to post source code and applications on the Internet; they would be permitted so long as an email was sent to the BXA notifying them of the location of the resource, and so long as access was prevented to recognised terrorist nations. The feasibility of this was again called into question, particularly considering the openness of the Internet.

After the terrorist attacks on the U.S. in September 2001, a member of the U.S. Senate proposed re-introducing a requirement for key recovery, but legislation was not introduced.

A relevant change that occurred, however, was the regulator of export controls, the BXA, was translated into the *Bureau of Industry and Security*.

> (T)he Bureau of Industry and Security serves the public in many ways where industry and national security intersect, including not just export licensing and enforcement, but also defense trade advocacy and critical infrastructure protection. (...) The new name better reflects the breadth of the Bureau's activities in the spheres of national, homeland, economic, and cyber security. (Department of Commerce 2002)

The effects of the transformation of this regulator remain to be seen; however the likelihood of re-establishing regulations on the export and use of strong cryptography seems minimal. Alternative means of gaining access to encryption keys have arisen in the U.S., and will be discussed in chapter 8.

7.3 Another Regulatory Discourse: Shifts in the UK

The United Kingdom pursued a number of type II cryptography policies to gain access to decryption keys, that went through many iterations.

7.3.1 Mandatory Regulation of Encryption Services

The first formal regulation proposal was a mandatory licensing scheme of Trusted Third Parties (TTPs), publicly released by the Department of Trade and Industry (DTI). This was a translation of an electronic commerce entity (assumed to be required for trust in e-commerce) into a surveillance-enabler: TTPs were to escrow keys.

The mandatory licensing regime hinged on some regulatory and technological designs. First, it presumed that private signature keys and private encryption keys were separate; and as such the private signature keys (only used for signature-creation) would not have to be escrowed. Second, the policy required that UK customers could only use UK TTPs; and to prevent international competition the proposed policy recommended a ban on marketing of non-UK TTPs, thus drawing a ring-fence (Hood 1994, p.34). Finally, the proposed regulatory regime, despite statements of technological neutrality, included the requirement of lawful access to both incoming and outgoing traffic, arguably requiring the use of a specific algorithm and protocol (*CASM*), despite market preferences for *RSA*.

The response of actors outside of government, including industry, NGOs, and individuals was generally one of concern. Respondents advised that regulatory competition would hurt the nascent market for certification authorities in the UK; the barriers to entry into this market would provide sufficient disincentives for any company to begin offering services,

short of large companies such as banks, effectively creating a cartel. The risks and costs of maintaining the prescribed facilities were articulated as being too high providing further disincentives, possibly rendering it infeasible. As the proposed regime did not ban the use of encryption products directly, circumvention was argued as being trivial. In effect, it was argued that the ring-fence had many holes, and those within the fence would find the regulation too burdensome.

7.3.2 Voluntary Regulation of Encryption Services

After the 1997 elections, the Labour Government, through the DTI, released a new proposed regulation with some marked changes. In an attempt to de-couple surveillance from e-commerce policy, the new regulatory regime treated Certification Authorities separately from Trusted Third Parties. Either could apply for a voluntary license; and would presumably be interested in doing so, as a license would act as a government-issued mark of trust. A TTP seeking a license, however, was required to escrow encryption keys. CAs, who deal only with signature keys, would be prevented from escrowing these keys.

This proposed regime also hinged on some regulatory and technological designs. First, a company could not be both a CA and a TTP unless both arms were licensed or not licensed simultaneously (thus preventing a situation where Acme-CA could be licensed and enjoy the benefits of the accorded public trust, and then set up non-licensed Acme-TTP that would carry a trusted brand but not be required to perform escrow). Similarly, certificates issued from CAs would have to be designed, using X.509 flags, to prevent the private signature key from signing encryption keys, thus preventing 'trusted' certificates from endowing 'trust' to unescrowed encryption keys.

Concern from respondents was not abated by this shift in policy. There were continued calls for a de-coupling of e-commerce and surveillance components; at least in the form of separate regulations and legislation. The regime was considered impractical, and unlikely to be used; a study from the Cabinet Office concurred and supported a shift away from TTP regulation.

7.3.3 Lawful Access to Keys in E-Commerce Bill

The next regime was introduced by the DTI in the form of the draft Electronic Commerce bill. Replacing the TTPs regulation scheme, Part III of the draft bill established powers of lawful access to keys. To support these powers, the bill also introduced offences of failing to provide the keys when requested, and for tipping-off others regarding a key that has been accessed by law enforcement authorities.

While the move away from regulating e-commerce institutions was welcomed generally, respondents found a number of problems in the regime. The lack of key granularity within the bill was of concern. The bill failed to acknowledge that in many cases session keys would suffice, or that private encryption keys could be used as keys for digital signatures (that according to the draft bill could not be accessed by government). The most controversial set of concerns was introduced by the Foundation for Information Policy Research (FIPR) and Justice when they commissioned a legal audit (Beatson and Eicke 1999). The audit argued that the bill reversed the burden of proof with the 'failure to comply' offence and this could be challenged using the Human Rights Act.

7.3.4 Lawful Access to Keys in Investigations Bill

In the November 1999 Queen's speech, encryption as an e-commerce application and encryption as a communications confidentiality application were decoupled into separate legislative initiatives. The first, embodied in the Electronic Communications bill dealt with the legal standing for digital signatures, and was managed by the DTI. The second, introduced by the Home Office implemented lawful access to keys, embodied within Part III of the Regulation of Investigatory Powers bill (RIP). RIP included the same regime proposed originally in the draft Electronic Commerce bill.

Its passage through the Parliament was controversial. Concerns were raised about keys placed off-shore to avoid the reach of UK law; as some companies vowed to do. Industry was alarmed that employees' keys could be accessed by government without the knowledge of the corporate executives. Parliamentarians and industry were concerned that regulations should be in-line with other countries for fear of British companies operating under a tougher regime than international competitors. Articulations of circumvention, technology-neutrality, and concern for the granularity of the keys also arose. The legal contentions regarding the reverse burden of proof did not disappear either, as another legal audit was commissioned, resulting in similar findings (Eicke 2000).

Media attention also grew. This attention peaked in the House of Lords stage of debate and with the release of a report commissioned by the British Chambers of Commerce on the risks to the UK economy (BCC 2000), with open letters to broadsheet newspapers (one such letter (Privacy International et al. 2000) included 49 signatory organisations and individuals ranging from Index on Censorship to the Countryside Alliance), editorials written by ministers and experts on both sides of the debate, ranging from the Home Office Secretary (e.g. (Straw 2000)), to NGOs and computer scientists.

Amendments were introduced by the Opposition parties, usually advised by industry representatives, the Foundation for Information Policy Research, and experts. The Government, pre-empting many of these amendments, introduced their own set in the House of Lords. Their amendments allowed for the notification of the corporate director of an employee's key being lawfully accessed (addressing industry concerns in part); allowed the individual to choose which key they wished to disclose (addressing key granularity in part); changed the placing of burden of proof of failing to comply, moving much of the burden to the prosecutors (addressing the legal audit in part); and reordered the object of lawful access, where plaintext will be requested by default and in some circumstances the individual will be ordered to hand over the key (addressing the legal audit and proportionality concerns in part).

Among the most active actors was the Foundation for Information Policy Research (FIPR), that advised the media, parliamentarians, and other actors in industry and NGOs. With its advisory council, FIPR released a number of reports criticising the bill on legal and technological grounds. Four reports were particularly noteworthy. First, the legal audit pushed for changes in the reverse-burden of proof. Second, a report was released that highlighted the importance of maintaining the security of the keys (Gladman 2000a). An amendment was later introduced requiring Government agencies to keep the keys under a level of assured security. Two further FIPR-related reports argued that because of socio-technological practices (Gladman 2000b) and systems design (Brown and Gladman 2000), the RIP bill was ineffective even while imposing burdens on the users of encryption.

The BCC and FIPR reports can also be perceived as Cost-Benefit Analyses, exploring risks and costs to the proposed regulations. However, we investigated the role of these reports in (Whitley and Hosein 2001) and found that they can be seen also as tools of political discourse, adding additional entities to the debate. These reports were unwelcome by Government officials. This was particularly the case for discussion of technological circumvention (Brown and Gladman 2000), that was discounted primarily because of its authors and distributor (FIPR), rather than its substance.

7.4 Patterns in Cryptography Policy Regulatory Discourse

Although the stories of the discourses in the U.S. and the UK surrounding cryptography policies were substantively different, a number of common threads appeared. In each there were some interesting developments that may assist in understanding policy development and transformations. Some of these will be summarised briefly below.

7.4.1 On Actors: Granular, Grouped, and Technological

A large number of actors were mobilised by each discourse. Considering how Latour (1991) and Callon (1991) consider a network (or collective), and in turn Braithwaite and Drahos (2000) regard networks and webs of action, understanding a policy requires consideration of the actors. These actors may be human or non-human, social or technological actors, all who are part of or are referred to within a discourse.

> If we speak of a drug, add the drug company, the clinical trials, the disputes among scientists about its mode of action, the many ways in which patients are talking about its effects on their bodies, and so on. If we talk of a new planet discovered around other stars than the solar system, don't forget to add the Hubble telescopes, the mathematical treatments necessary to code the information received, the disputes among cosmologists about planetary formation, the effect this new planet has on the public conception of life on earth etc. (...) If we talk about a new software, add what it does to the company, to the hierarchy of people in it, to the skills, to the ergonomics of the screen, etc. For every object adds its society, or more precisely, its associated collective. (Latour 1998)

I will synthesise the actors below by presenting actor-categories in order to identify patterns that may have arisen. These actors entered the discourse sometimes through invitation, but also through lobbying, campaigns, by implication, and other activities. Although there is no simple classification scheme for actors because of their diverse interests, actor-categories will be separated in a manner consistent to the work of Braithwaite and Drahos (2000).

> States act as agents for other actors such as business corporations and other actors act as agents for states; this reflexive agency reconstitutes both agents and principals continually. States are part of actor networks; far from rising above these actor networks, state action has little impact without them. (p.548)

However, they do not categorically recognise this, and their 'actors' lack granularity. In their analyses Braithwaite and Drahos often refer to 'government' and 'state', offering only some granularity to these terms. Instead I propose the following actor-categories, or entities:

- government law enforcement
- government national security agencies
- government executive,
- government commerce and trade agencies
- parliamentarians
- industry organisations and industry representatives
- non-governmental organisations (NGOs) and advocates
- specialists and experts
- media
- mass publics

Table 7.3 Granular Actor-Categories, or entities

Even within this level of granularity regarding the actor-category names there are still a multitude of ambiguities. The characteristics and roles of some of these entities will be discussed below.

The very presence of cryptography as a threat to the abilities to intercept communications mobilised government agencies, particularly those involved in *law enforcement* and *national security*. Early in the U.S. discourse, debate centred on *national security* entities. The Departments of Defense and State were charged with the regulation of export controls, and the NSA was charged with protecting national interests, developing and using cryptography while disallowing foreign interests from gaining access to cryptography. The NSA and related institutions eventually developed the *Escrowed Encryption Standard*, its algorithms (*Skipjack*), a translated version of a public-key standard (*DSS*), and advocated and testified for their adoption. They also prevented strong cryptography (restricting *DES* to 56-bits), reviewed and advised exported cryptography (as in Microsoft CAPI), but also ensured that code met its interests (Lotus WFR), permitting incremental strong cryptography only with policy support (step-up crypto). The NSA did support the use of domestic encryption without algorithmic weaknesses (*DES*), however. Similar institutions in the UK (GCHQ and CESG) played relatively quiet roles in the public discourse; the reasons for which are beyond the scope of this study.

Law enforcement related entities often led the charge against liberalisation. In the U.S. this was mostly performed by the FBI and other actors within the Department of Justice (DoJ). The Home Office spoke primarily on law enforcement concerns in the United Kingdom. On occasion, the National Criminal Intelligence Service (NCIS) would speak on the importance of access to communications and the costs of crime, as would the Association of Chief Police Officers (ACPO).

Although the perspectives of *law enforcement* and *national security* entities was often supported by the *government executive*, at times the executives in both countries would act as arbiters, representing national security and economic actors' interests simultaneously. In the UK, apart from the ministers for the Home Office, the executive (Cabinet members) had to represent economics, civil liberties, and law enforcement arguments. Similarly, the Clinton Administration was in the difficult position of balancing policies on Critical Infrastructure Protection, economic trade and security, and law enforcement and national security. Often the *executive* pursues policies dictated by their agencies; as we saw the Clinton Administration adopt Clipper, that was developed under the Bush Administration's NSA; and the Labour Government adopted only slight changes from the Conservative Government's position on TTP-licensing, despite its Manifesto.

The *government commerce and trade* entities also played a confused role, trying to support commerce and strategic trade while also acting as gatekeepers regulating the technology and the services that national industry was willing to offer. The Department of Commerce (DoC) was charged with supporting trade, while its subsidiary BXA was charged with controlling trade. The BXA was designed for this confusion: it was created in 1985 to separate the Commerce Department's export control function from its trade promotion function, acknowledging that the mandates and actions are divergent (Heinz 1991, p.21). The Department of Trade and Industry (DTI) was responsible for supporting e-commerce, while arguably the proposals for TTPs did much to inhibit the development of a trust infrastructure.

At the legislative level *parliamentarians* did take an active role in the discourse. Congress in the U.S. was active in pursuing testimonies in committees in both the Senate and the House of Representatives, and a number of bills were introduced to Congress by members of both houses. Likewise, apart from ministers in the UK, Conservative and Liberal Democrat MPs and peers in the House of Lords played active roles in soliciting and representing comments from other actors, and suggesting amendments.

Industry organisations and representatives were active in the debates, but not necessarily pushing for deregulation in a coherent and cohesive manner. Many of the companies who were politically active were also developing technologies and services in accordance with the contested policies, and trying to meet market demand. Industry often spoke in groups; whether through the Key Recovery Alliance, or the Business Software Alliance, amongst others. In the UK, a number similar industry lobby groups participated in the discourse, such as the Confederation for British Industry, Alliance for Electronic Business, the British Chamber of Commerce, to name a few. Individual companies also spoke out often, particularly in the consultation processes.

One of the most active categories of actors was the *Non-Governmental Organizations and advocates*. NGOs in the U.S. were activated by this issue; some ran campaigns, others supported or aligned themselves with campaigns and participated actively with less frequency. NGOs played an essential role in lobbying governments, informing the media, researching national policies, and using the Freedom of Information Act to penetrate the strategies of government. In the United Kingdom, NGOs organised pivotal conferences, informed the media; but did not play the role as actively as their American counterparts, with a few exceptions, notably the Foundation for Information Policy Research.

The role played by the *specialists and experts*, as individuals and academics, or committees, or editorial boards of reports can not be overstated. Consensus should not be assumed; some spoke fervently in support of controls, but from my experience, the vast majority spoke in favour of allowing strong cryptography to be used without introducing weaknesses. The *Minimal Key Lengths* and *Risks of Key Recovery* reports articulated their ideas on the costs and challenges to the government policies; and individual cryptographers and security specialists testified in the U.S., and spoke often at conferences and to the media. In the UK, these same reports were used in the consultation responses of companies and individuals. Many UK experts also participated in the discourse, sometimes wearing the badges of their companies, educational institutions, affiliated NGOs. Some of these later founded FIPR in 1998. Professional organisations were active, such as the Association for Computing Machinery (ACM) with its special panel report (USACM 1994), and legal associations such as the American Bar Association, or the Law Society for England and Wales. The legal auditors of the lawful access powers in the UK may also fall within this actor-category.

A final category of actor is the *technological*. Every actor identified to this point has spoken of the technological, representing the technological in some form or another. Sometimes the technological actors were the object of regulation, sometimes even when neutrality promised. In some cases the technology was spoken for by a multitude of actors, and its specifications interpreted differently. In other cases, the technology acted through recalcitrance, in objection, by failing to work in expected ways, e.g. Clipper, or prompting renegotiations, e.g. key granularity amendments in RIP. The 'technology' was not just cryptography; it could have been keys, algorithms, implementations, standards, and even communications infrastructure.

7.4.2 On Interests and Alliances: non-monolithic and non-transitory

Collecting actors together under 'categories' is a hazardous exercise; the categories established above do not necessarily infer a commonality of interests and goals. Nor are interests monolithic, and more importantly, they are rarely shared in full when actors align with others.

The review of the actor-categories above indicates some of these strains already. To merely claim that *government*'s interests is in *surveillance at all costs using any regulatory intervention however implemented* would be a gross over-simplification. The NSA showed a set of seemingly confused interests in its input on the development of *DES*, both strengthening the algorithm and shortening the keys. Law enforcement agencies have come out in defence

and derision of encryption; defending it because it can increase security and minimise risks while deriding it for their loss of ability to gain access to secured data.

Executive arms of government (the White House, the Prime Minister's office and Cabinet) have an interest in supporting e-commerce but also in maintaining the power of law enforcement and national security entities. There is also some interest in upholding individual rights, in accordance with the Constitution and the Human Rights Act respectively.

The government commerce and trade entities had a confused set of interests. The U.S. Department of Commerce and its BXA were responsible for enforcing export controls, but this was not their only interest. They also pursued and advocated strict regimes: the Commerce Secretary and Under-Secretary vigorously advocated the value and importance of export controls for national security. In converse, the UK DTI was initially responsible for proposing and advocating the regulation of encryption services; and introduced the investigative powers in the draft Electronic Commerce bill. The DTI had an interest in supporting e-commerce, in seeing the development of trust infrastructure; but it wasn't until the de-coupling of the legislation after the Queen's Speech that the DTI could pursue e-commerce legislation without being burdened with representing surveillance interests.

Members of the legislatures were not a coherent interest group either. It would be a mistake to assume that all Opposition-party politicians were opposed to proposed regulations; supporters and detractors took many positions and existed in many parties. In the U.S. Congress some Republicans proposed harsher regimes than those proposed by the Clinton Administration. In the UK, some Conservative MPs supported harsher penalties for non-compliance within RIP. Finding a settlement that satisfies the interests of politicians to support industry, act against criminal elements, and maintain the trust of the voting public is non-trivial, as the political science literature no doubt appreciates.

The interests of experts and security specialists were similarly fragmented. Some from within this community argued that key recovery was required, useful, and not necessarily a threat (e.g. Entrust Technologies' cryptographers and researchers). Others, though fewer, argued publicly in support of key escrow (e.g. Denning). It is important to note that one of the largest collections of cryptographers and security specialists work at the NSA; their interests in the policy as employees may differ from their interests as members of a scientific community. Interestingly, however, their interests were articulated and represented in both countries' discourses.

An epistemic community, according to Haas (1992, p.3) are shapers and influencers of decision-making processes, while apart from the political factors and actors (1992, p.5). Cryptographers and computer scientists, as they tried to speak primarily *objectively* on risks, costs, feasibility, socio-technological practice and design, often tried to separate the social from the technological, but invariably involved articulating either the interests of access or confidentiality. This community is most noteworthy when its articulations are across actor-categories, and a cross-actor body of interests can be derived. The NSA found ways of making *DES* less susceptible to attack; and designs its own algorithms in similar ways to academics and practitioners. Similarly, when the NSA agreed with the weaknesses in key recovery systems, despite political and ideological differences, this showed a common set of knowledge-practices, and perhaps beliefs, or aversions. Accordingly, Haas' notes that solidarity of the

> epistemic community members derives not only from their shared interests, which are based on cosmopolitan beliefs of promoting collective betterment, but also from their shared aversions, which are based on their reluctance to deal with policy agendas outside their common policy enterprise or invoke policies based on explanations that they do not accept. (1992, p.20)

Similarly, Adler and Haas note that "epistemic communities are not in the business of controlling societies; what they control is international problems" (1992, p.371). The common views within this community from their articulations include the importance of cryptography to secure data, of the threat to unsecured communications and data, and a common assessment of inadequate means of protection; these views were influential within the discourse, often repeated by others.

Industry also exhibited a number of interests. At various times in each discourse, industry actors can be found seeking protection, deregulation, or maintenance of the status quo. As a result, ascertaining a cross-industry interest is non-trivial. Identifying even the interests of one given company is also quite challenging, particularly as a company has a set of interests that are not necessarily coherent. For example, marketing departments may want to sell to as many countries but also wishes to sell strong cryptography to concerned customers, while legal departments want to abide by laws but minimise liability as well, while designers may share values with the epistemic communities or with NGOs. Some sought protection or perceived 'liberalisation' differently. For example some firms felt that export of strong but escrowed encryption was a satisfactory liberalisation. Apart from the Key Recovery Alliance, however, most U.S. firms publicly supported some form of liberalisation of export controls, often vocalising these interests under umbrella organisations. In the UK some were quiet in the face of government proposals, or chose to be spoken for at the alliance-level.

NGOs were not a united front either. Some NGOs had goals of minimising the harm of the regulations; others sought the abolishment of national controls only. Child-protection groups in the UK pushed for harsher penalties for failing to comply with lawful access to keys requests; and on occasion derided both industry and other NGOs for supporting criminals. In the U.S., some of the organisations represented were arguing in support of industry and free market ideas and regarded controls on cryptography as unfavourably as other forms of regulation; while other NGOs were interested in the civil liberties concepts but remained uninterested regarding regulatory burdens.

As the actors allied with one another into coalitions (Stigler 1988, p.xiii), even contingently, the diversity of the interests were both concealed and brought forward. In the case of concealing conflicting interests, as 'civil liberties' NGOs allied with industry groups such as the BSA, their interests were aligned on export controls liberalisation or against the Clipper Chip. Chasms of differences still existed with regard to government's role in regulating e-commerce (particularly in the case of copyright, privacy regulations, or even ideology of government intervention generally). At times conflicting interests are brought to the forefront even when an alliance is forged: the regulatory regime shift to liberalisation of export controls to 56-bits was initially welcomed by industry, thus creating an alliance between government and industry. It can be said that some within industry felt that this was meeting their interests and they could convince the market of the need for key recovery and strong cryptography (through the Key Recovery Alliance; and through the work of the Crypto-Tsar), even though the industry articulation of key recovery was quite different from government's articulations. Industry is thus placed in a difficult position; not wishing to be seen as supporting terrorism and child pornography it aligns with government interests; but not wishing to appear, in foreign markets at least, as co-opted by the U.S. Government, aims for strong cryptography and openness. The experiences of Lotus, Microsoft, and PGP in the media brought these conflicts forward. Similarly, in RIP bill process, the larger industry organisations were vocal in opposing the bill, alongside NGOs; but when some key amendments were made in the interests of industry, the informal coalitions disbanded.

The interests of a given technology remain elusive, as discussed in Section I. It is possible to consider how the attempts to embed societal interests into a technology have led to failure both socially and technologically (e.g. Clipper); or introduced conflicts of interests for the public to see (e.g. NSAKEY). In these senses, technology can be seen as objecting to interests and translations; or may be seen to support the arguments and interests of others, such as NGOs, industry, and those in the epistemic community. The support is contingent and fleeting however: even NGOs and some within the epistemic community are

concerned with widespread use of public-key technology for the cause of civil liberties, as a **threat** to privacy (c.f. Brands 2000; Brands, Hosein, and Perrin 2001).

As Pouloudi and Whitley (2000) warn, ascertaining the interests of both humans and non-humans is far from trivial. As a result, an analysis of interests may not provide conclusive results. Understanding the interests of a single actor is challenging; if this actor is a large organisation, the problem is compounded. In alliances the problem is exacerbated through concealment and conflicts.

Braithwaite and Drahos (2000) have similar findings on interests. A number of motivations are involved for a given actor within a discourse (p.547), and these actors "may lack any synoptic grasp" of their own interests (p.548). They find fault in rational-choice accounts and value-maximizing motivations in economic and international relations theories, considering these accounts simplistic (p.548). Instead, I proffer that noting the actions, speech, objections, and articulations of actors within the discourse may provide something more concrete for study. Watching the process of alignment and translation may provide additional insight into the socio-technological discourse.

7.4.3 Translations

Considering actors within a discourse, in their interests and alliances, the operation of translation is key. Monteiro and Hanseth (1995, p.336) note that the simpler a network of actors is, the easier it is to align; the more complex, the more complex it is to align. Complexity arises as the number of mechanisms and actors increases. Or as Latour states this point, maintaining reality is paid for by a continual extension in the *syntagms*, the continual extension of the amount of devices or means used to translate the network (Latour 1991). *Translation* permits this analysis without having clearly defined actors and assigned interests, as Latour expands,

> Instead, we can follow the way in which actant B attributes a fixed border to actant A, the way in which B assigns interests or goals to A, the definition of those borders and goals shared by A and B, and finally the distribution of responsibility between A and B for their joint action. In a universe of innovations solely defined by the associations and substitutions of actants, and of actants solely defined by the multiplicity of inventions in which they conspire, the translation operation becomes the essential principle of composition, of linkage, of recruitment, or of enrolment. But since there no longer exists any external point of view to which we could ascribe the degree of reality or of success of an innovation, we can only obtain an evaluation by triangulating the many point of views of the actors. (1991, p.124)

Often these translations involve the use of a *mechanism*, such as coercion, systems of rewards, modelling, and reciprocal adjustment (Braithwaite and Drahos 2000, p.25). Other times they can arise through mere speech at moments of interest.

Each regulatory regime was an essay in translation, using a mechanism. At every regulatory shift with a new proposed mechanism, another strategy and set of actors and interests were interacting. Translations also involved the overt attempt to appropriate or shape the interests of other actors. Finally, translations as articulations, and the reduction and expansion of articulations, also arose.

Regulatory Regime Shift as Translation

Each shift in regulation involved translation in the regulator, the mechanism, and/or the regulated. As policy strategies changed and the perception of the landscape transformed, the U.S. Government shifted responsibilities for export controls from the Departments of State and Defense over to the Department of Commerce. This shift was a translation of the regulators' goals and interests. The same applies for the shift between the DTI and the Home Office. It has been argued that when the DTI presented the original policy on TTPs, this was a translation of the DTI's responsibilities. Moving the policy to the Home Office made the Home Office responsible for e-commerce-related affairs.

Similarly, the shift of mechanism in the U.S. from domestic controls to export controls in the U.S. resulted in export controls being used as a foreign and domestic control; this was a translation of the interests of government, but also a translation of the instrument of regulation. Export controls were transformed into also being a domestic control; while previously they were tools for strategic trade and national resource management. The translation of e-commerce regulation into the regulation of TTPs for access to encryption keys is another example of translating the regulatory instrument. The shift from licensing of TTPs to the lawful access to keys in RIP also translated the goals of RIP, originally positioned as an update to the *Interception of Communications Act* 1985; just as previously, an electronic commerce legislation to support digital signatures was translated into a law enforcement mechanism for access to keys.

Another form of translation as regime-shifting is directed at the object of regulation. The original policy of the UK set the TTPs as the object of regulation, rather than regulating encryption products that were already openly available. In so doing, the regulatory regime was endowing the TTP with a specified form and function that it may not otherwise have taken on. Likewise, when the policy transformed from mandatory licensing to voluntary licensing, this involved translating the regulations into a trust infrastructure. That is, the

license was translated from a permit of operation into a trust-mark (at least according to the DTI). This is a transformation of the license as a mechanism of economic coercion (those with licenses are permitted to trade) transformed into a reward system (those with licenses may be rewarded with government-sanctioned trust).

Shaping Interests as Translation

Government policies have continually tried to translate the interests of other actors. The Clipper Chip is a case in point: AT&T was convinced to embed Clipper, as the U.S. Government promised to be a customer (government contracts are valuable). The interests of AT&T to market a secure phone were translated by the concerns of government agencies. This was a case of creating incentives to shape the market, or a system of rewards. In return for their co-operation, AT&T had the power of government as a contractor as economic support, and the resulting network externalities. The public response and the work of the NGOs and epistemic community, as well as the flaw within Clipper broke the momentum (Hughes 1994) of this technology policy regime.

Other forms of shaping interests include the translation of *export-with-strong-encryption* into *export-with-recovery*, a translation of export controls into a mechanism for controlling foreign and domestic use of encryption. This could be considered economic coercion, in that companies could not export without meeting the government's interests; harming their trade and market competitiveness until product compliance could be assured. It was also a system of reward, however; companies who abided by the intended goal of implementing key recovery-within-two-years could immediately export stronger cryptography.

The coupling of lawful access to keys in TTPs was a translation of e-commerce institutions into surveillance institutions. This translation reached its full potential only when Home Office ministers translated the earlier *government executive* articulations about making the UK 'the best place' into 'the best and safest place' for e-commerce. The amendments introduced by Home Office ministers in the House of Lords stage also were attempts to translate the interests of industry into amendments, which in turn would abate the concerns of industry.

Translation is not just a tool of the powerful, however. Industry spoke of civil liberties and rights to privacy, translating the interests of NGOs in order to further the cause of liberalisation. NGOs and members of the epistemic community spoke on behalf of industry to raise the status of their voice; the BCC Commissioned report was an example of this, where the authors, primarily academics, civil libertarians, and smaller-industry representatives used the BCC's status as the means of getting their ideas heard. NGOs sponsored many other reports: the Center for Democracy and Technology sponsored the

Risks of Key Recovery reports; FIPR used legal audits to translate the European Convention of Human Rights into RIP-parlance.

Articulation as Translation

Another form of translation involves articulations. Representation of technology (an articulation) to meet an actor's interests is a translation of that technology; when others also speak otherwise, we see a Latourian and anti-essentialist contest of articulations, or triangulation.

Debates over the strength of 56-bit encryption involved a battle of articulations: the FBI and NSA concurring that 56-bit encryption is too challenging for law enforcement and thus the need for domestic controls; then DESCracker showed otherwise, in a sense of objecting to what is said about the strength of 56-bit keys. Similarly, Clipper was an articulation of the key escrow policy; the ten criteria and the work of TACDFIPSFKMI were articulations of key recovery. It is interesting to note that in both countries' parliaments, parliamentarians eventually spoke in specific terms regarding the technology, discussing keys, algorithms, and bits; again involving translation.

The key granularity issue is another example. While the TTP regulatory regime was clear that keys used for integrity purposes only would not be escrowed, respondents to the consultation process, and the authors of the Risks of Key Recovery report later repeated that the market standard, *RSA*, used keys for both signature and confidentiality purposes. As a result, the government's articulation would permit for the escrow of signature keys; and thus their translation of signature keys presupposed a specific technological design. When the regime shifted to voluntary licensing, the policy contained an articulation of how signature keys must not be able to sign other keys, using X.509 flags (despite technology-neutrality). This was a translation of alternative forms of key management infrastructures, and was seen as a reduction of the functionality of cryptosystems, and in the integrity of secure communications.

Companies also managed their articulations. The translation of export controls policy into technology involves interpreting the policy and creating design articulations and specifications for implementation into code. Microsoft interpreted the export controls in such a way that allowed the firm to become an obligatory passage point for cryptographic modules provided by other software vendors. PGP interpreted the key escrow requirements into the specifications for the Alternative Decryption Key, though poorly implemented into code. Lotus interpreted the export controls as requiring merely the inclusion of the NSA into the process of key creation, ignoring law enforcement interests. Entrust interpreted key

recovery differently than the articulations of Denning and Branstad (1997), pursuing business key recovery rather than surveillance-enabling key recovery.

Returning to the anti-essentialist critique, a number of interpretations of the functionality and 'capacity' of encryption algorithms and keys were offered and their essential natures. However the anti-essentialist triangulation more often than not led to a Latourian triangulation where the actors' speech converged, particularly over time. This notably led to a situation where articulations of the infeasibilities of key recovery, or the feasibilities of techniques of circumvention became more prevalent, from a variety of actors with varying interests. While it is interesting that the objections of the technological actor often reinforced the voices of the epistemic community, this does not mean that without the epistemic community the objections would not have occurred.

7.5 Summary: Discourse as a Contest of Principles

Each discourse was an interplay of actors pursuing various interests, and translating other actors. The discourse involved regulatory regimes, shifting and being shifted by resistance and changing conditions. Articulations of costs, risks, challenges arose and shaped interests of access to secured data and communications, as NGOs and industry allied and spoke for each other and concealed their differences for the moment. Translations were bountiful, shifting strategies and interests, and the actions of actors. Somewhere in this midst, technology had a role to play; it is spoken of, spoken for, and it even objected.

Above I have presented many of the conditions of the environment new policy courses were selected in each country, and the surrounding discourse, but I have not explained why these changes took place. That is, I have met Stigler's agenda for describing the establishment and transformations of regulations on cryptography in the U.S. and the UK, but I have not been able to explain why cryptography policy transformed.

Explaining why there was a reversal of the U.S. policy that eventually tended towards liberalisation, and explaining why the TTP regime in the UK failed is not as easy as saying that the policies could be circumvented, or foreign availability existed, or that the costs were too high. Making sense of the regulatory discourse is not as simple as saying the interests of industry and NGOs took precedence over national security concerns.

A review of the regulation literature and its explanations for regulatory change and reversals shed some light on these cases. It can be said that the traditional habitat for government regulations to access to communications and stored data were threatened by technological developments; but such a deterministic approach would not accommodate explanations of

why cryptography policies also failed because of e-commerce concerns. Even Lessig's ideas of indirect regulation and the role of architecture as a regulator would not explain why key recovery was developed in some technologies, but also why these technologies did not necessarily meet the interests of governments. In fact, understanding regulation emergence and transformation as a discourse, or as Braithwaite and Drahos' web of influence (p.13) may be more useful.

> Actors seek, through principles, to incorporate into regulatory systems and social practices changes that are consistent with their general values, goals and desires. The abstract nature of principles means that the successful weighting of one principle or set of principles over another means that the direction for action has to be settled on. Once the direction has been set, the process for generating detailed rules of conduct (or changing them) can take place. (Braithwaite and Drahos 2000, p.19)

However they failed to include the technological as one of those actors. We may include technology as an actor within each discourse, its objections to translations and alliances, but also representing some interests. Then we may see more principles that were contested, and those that were not, within the negotiation of the resulting regulations.

The principles can be seen to emerge from the discourse, as we capture statements and shifts. The early policy of the U.S. to regulate algorithms and knowledge regarding cryptography involved a limited set of actors, traditional mechanisms, and a limited number of principles (see Table 7.4).

Regime: Pre 1990s. Object of Regulation: Algorithms and Knowledge

Policy Type: I		
Mechanism	Actors	Principles
Export Controls ? ECA ? EAA ? ITAR	Regulator: Government National Security ? NSA ? Department of Defense ? DoS Other Actors ? Cryptographers outside of the Government ? Some developers in industry	? Academic Freedom ? Trade ? National Security from Foreign Threats

Table 7.4 Regime: NSA control over cryptography research

This policy regime existed within an environment where cryptography was not yet considered an essential component to general communications and commerce. As its importance grew, the need for implementation and standardisation also grew, resulting in the development of *DES* and *DSS* (Table 7.5).

Regime: NSA Intervention on Standards. Object of Regulation: Algorithms and Keys

Policy Type: III		
Mechanism	Actors	Principles
Export Controls ? ECA ? EAA ? ITAR ? Standards shaping (*DES* and *DSS*)	Regulator: Government National Security ? NSA ? DoD ? DoS ? NIST Other Actors ? Cryptographers outside of the Government ? Some developers in industry ? Epistemic Community ? Private developers (Cypherpunks, academics and experts) ? Deep Crack ? *DES*, Key sizes, differential cryptanalysis ? *DSS*, Key sizes, private signature keys ? *RSA*, private encryption keys	? Academic Freedom ? Trade ? National Security ? Foreign Availability ? Domestic Strength ? Knowledge: Academic knowledge; minimal keysizes, DESCracker ? Trust

Table 7.5 Regime: NSA Intervention on Standards

A number of additional actors were introduced as the object of regulation transformed to include standards, functionality, and key sizes. Interests were not monolithic, with the confused role of the NSA, balancing the conflicting interests of national security and domestic strength of cryptography. The number of developers grew, and the ability to implement cryptography into software grew easier as the number of developers and experts in cryptography grew. The foreign availability of cryptography increasingly became an issue, both for national security actors as well as industry. As knowledge increased regarding key sizes and articulations and technologies emanated showing that regulated key sizes were inadequate, combined with the principle of trust in digital networks, new regulatory strategies began emerging.

The U.S. Government tried a domestic policy first, being the Clipper initiative (Table 7.6).

Regime: Clipper and Escrowed Encryption Standard. Object of Regulation: Market for Secure Communications

Policy Type: I, III, disguised as Type II		
Mechanism	Actors	Principles
? Direct Intervention on Market of Supply ? Direct Intervention on Market of Demand ? Shaping Standards (*EES*)	Regulator: Government National Security and Law Enforcement ? NSA ? DoJ ? White House Other Actors ? Congress ? Industry of Software and Hardware Developers ? Epistemic Community ? Private developers (Cypherpunks, academics and experts) ? NGOs and Advocates ? Law Enforcement Access Field (LEAF) ? Checksum ? Skipjack Algorithm ? Mass Publics and Media	? Privacy ? Law Enforcement ? National Security ? Openness of Algorithm ? Trust ? Technological Effectiveness ? Public Interest ? Circumvention (by Government and Criminals)

Table 7.6 Regime: Clipper and *EES*

NGOs and advocates began playing an increasing role in activating mass publics with petitions, the media through education and events, and interacting with Congress through lobbying, raising attention to principles of privacy and trust. In turn the principle of trust affected Clipper as the epistemic community raised concerns about whether the technology could be trusted, let alone achieve its stated claims as articulations of failures emerged.

As the Clipper regime failed, new strategies were attempted, incorporating the interests of software and hardware industries who were increasingly interested in security and trust because of a growing interest in e-commerce (Table 7.7).

Regime: Key Recovery. Object of Regulation: Industry Software and Hardware Developers, Keys, Algorithms, Key Recovery Concept

Policy Type: II, III		
Mechanism	Actors	Principles
? Export Controls ? Standards (EES and KMI) ? Translating 'Key Recovery' ? Reciprocal Adjustment with Foreign Countries (Modelling and Harmonisation) ? Incentives for Export ? Coercion	Regulator: Government, Commerce and Trade ? DoC BXA ? White House ? Crypto-Tsar ? DoJ ? NSA ? TACDFIPSFKMI Other Actors ? Congress ? Industry of Software and Hardware Developers ? Epistemic Community ? NGO/Policy Advocates ? Foreign Developers and Technology ? Global Information Infrastructure, Internet ? Session keys ? Export permits (BXA signed) ? PGP ADK, Lotus WFR, Microsoft NSAKEY	? Privacy ? Law Enforcement ? National Security ? 'Trust' and 'Security' ? Technological ability to work ? Public Interest ? Free Speech ? Costs and Risks reports (Risk of Key Recovery, NRC, Entrust, etc.) ? Market Needs ? Foreign Availability and circumvention ? Technological neutrality ? E-commerce ? Trade

Table 7.7 Regime: Key Recovery

Returning to the mechanisms of export controls, and again trying to use standards such as the *EES* and principles of KMI, coercive regulatory techniques were used to promote the development of key recovery. Other actors pushed back against these developments, while some also tried to develop the technology accordingly. Principles of privacy, law enforcement, national security began to conflict with concerns regarding foreign availability (markets outside of the 'ring-fence' of regulation). The principle of 'letting the market decide' was in conflict with the principles of 'national security' and 'law enforcement' even as attempts were made to redefine key escrow, to incorporate 'what the market wanted'. Attempts to redefine trust and security also emerged; but non key-recovery cryptography appeared to promise trust and security without the same set of risks and costs as key recovery solutions. As these principles were negotiated, liberalisation eventually occurred.

The situation in the UK began already pre-supposing the benefits of cryptography to e-commerce, but negotiation occurred surrounding the term 'trust' (Table 7.8).

Regime: Mandatory Licensing of Trusted Third Parties. Object of Regulation: Trusted Third Parties

Policy Type: II		
Mechanism	Actors	Principles
? Licensing (Mandatory) ? Coercion ? Technological Mandating ? National Use Only (Blocking Foreign Availability)	Regulator: Government, Commerce and Trade ? DTI Other Actors ? Policy Advocates ? Industry (potential TTPs) ? Industry (potential E-commerce) ? Epistemic Community ? Private Signature Keys and Private Encryption Keys ? Non-UK TTPs ? Bi-directional Algorithms for Access (*CASM*) ? PGP and other available products ? Internet	? Privacy ? Law Enforcement ? Trust ? Commerce ? Market choice ? Costs, Risks ? Effectiveness ? Foreign availability and circumvention

Table 7.8 Regime: Mandatory TTP Licensing

This first policy proposal using the coercive mechanism of mandatory licensing included a large set of actors, many of who were not yet well-formed, but the excitement surrounding the new economy began to buzz and market imperatives were often expressed. Privacy and law enforcement principles conflicted as did articulations regarding how commerce and trust 'worked'. This regulation was being considered at a time where the exact form and nature of e-commerce remained unresolved, but certainty regarding its international nature already emerged: the principles of effectiveness of the regulations and foreign availability clashed. All of these principles were affected by technological factors; whether through deciding which algorithms and keys would be used and how they would affect commerce and trust, through to the Internet and advertising of off-shore TTPs.

A softer approach was taken later as the norms and practices surrounding e-commerce began to appear, resulting in many changes, including a separation of TTPs from CAs. Voluntary licensing was offered as an incentive scheme, with some mandating of technological considerations, pre-supposing a specific form of certification (Table 7.9).

Regime: Voluntary Licensing of Trusted Third Parties. Object of Regulation: Trusted Third Parties and Certification Authorities

Policy Type: II		
Mechanism	Actors	Principles
? Licensing (Voluntary) ? Incentives ? Technological Mandating	Regulator: Government, Commerce and Trade ? DTI Other Actors ? Policy Advocates ? Industry (potential TTPs) ? Industry (potential CAs) ? Industry (potential E-commerce institutions) ? Epistemic Community ? U.S. software industry and key encapsulation products ? X.509 flags, private signature keys, private encryption keys	? Privacy ? Law Enforcement ? Trust ? E-commerce ? Market choice ? Costs, Risks ? Effectiveness ? Foreign Availability, Circumvention ? Technological neutrality

Table 7.9 Regime: Voluntary TTP Licensing

Increased industry attention to the proposals gave further weight to principles of market choice, e-commerce, trust, and costs. There were differences in understandings and articulations regarding 'trust', whether it would emerge from practices or through licensing; and thus questioning of the feasibility of the regulations in achieving either conflicting principle of law enforcement or promoting commerce.

With a greater understanding of the institutions involved in e-commerce, and the likelihood of achieving any regulatory success, a new approach was introduced. Rather than using indirect regulation, by regulating third parties, the new policy regime proposed regulating individuals directly by requiring the disclosure of keys (Table 7.10).

Regime: Draft Electronic Commerce Bill Law Enforcement Access to Keys. Object of Regulation: Keys

Policy Type: II		
Mechanism	Actors	Principles
? Coercion (GAK)	Regulator: Government, Commerce and Trade; and Government, executive ? DTI Other Actors ? Policy Advocates ? Industry ? Epistemic Community ? FIPR ? ECHR ? Keys and Passphrases	? E-commerce ? Law Enforcement ? Trust ? Feasibility and Effectiveness ? Costs, Risks ? Human Rights

Table 7.10 Regime: GAK in E-Commerce bill

This coercive mechanism faced a reduced set of opposing actors because industry conduct was not directly regulated. However a legal audit introduced specific concerns regarding the structure of the regulations and the goals of law enforcement in the face of civil liberties and human rights instruments.

Principles of costs and risks were less prevalent at this stage in this new policy; although the principle of trust conflicted with law enforcement's interests as concerns arose surrounding which key was being discussed.

With the passing of the regime of lawful access to keys to the RIP bill, apart from the shifting of the regulator, many of the actors remained the same. The increased role that NGOs and notably FIPR played affected in turn the growth of awareness in the media, and the mass public as well.

As there was a bill, parliamentarians entered the discourse, representing industry, NGOs, and other actors and principles (Table 7.11)

Regime: RIP Bill and Act. Object of Regulation: Individuals and plaintext, keys (with granularity)

Policy Type: II		
Mechanism	Actors	Principles
? Coercion (GAK)	Regulator: Government, Law Enforcement ? Home Office ? NCIS, ACPO Other Actors ? FIPR ? Policy Advocates ? NGOs ? Industry ? Epistemic Community ? Parliamentarians (MPs and Peers) ? ECHR ? Media and Mass Public ? Keys (granularity) ? Perfect Forward Secrecy and Steganography	? Law Enforcement ? E-commerce ? Trust ? Security ? Rights of individuals ? Norms and Effectiveness (Revocation and Circumvention) ? Regulatory Arbitrage (off-shore, competition) ? Costs and risks ? Technological neutrality ? Economy (Best vs. Best and Safest)

Table 7.11 Regime: GAK in RIP

Many of the same principles collided as in the preceding regulatory regime. Within the discourse in parliament, more principles were articulated. Notable amongst these were the regulatory feasibility issues due to technological circumvention and regulatory competition.

A further legal audit gave rise to concerns regarding civil liberties; whilst reports from industry and NGOs alluded to a conflict of principles between trust, security, costs, and law enforcement interests. Amendments were produced to translate these principles, and the bill passed even as companies were promising to move keys and services off-shore.

7.5.1 Explaining Regulatory Change

Arising from this collection of regulatory shifts was a number of principles espoused by a number of actors. Accounting for regulatory change would require accounting for all of these principles (and perhaps more), their conflicts and resolutions. As programs or regimes became more complex, more actors became involved or implicated, pursuing goals and articulating varying principles.

Technology also introduced actors and principles. Cryptography's service to e-commerce introduced more industry actors to the discourse, raised public attention, and constrained government action, or at least required translations of cryptography to meet principles of law enforcement. That cryptography was interpreted in so many ways by so many actors led to more actors being involved, more interests and principles being pursued, and more attention to the issue. But technology was not deterministic; the foreign availability and circumvention principles propped by industry and NGOs were not the only reasons for regulatory change.

In fact, regulatory change did not occur for any one reason, and one would be challenged to explain the shifts in any one way. Explanations may include issues not included within this study because of limitations of data collection (e.g. non-public meetings). Even today each actor would *explain* the shifts differently. To put it simply, software developers may say the changes were due to technological reasons such as risks, costs, or foreign availability due to the Internet; lobbyists may say the changes were due to political reasons of creating alliances and convincing other actors of one's interpretation; government authorities may say they were due to misunderstandings of the other actors and poor appreciation of the concerns of law enforcement and national security; and NGOs may say that they were due to politics, belief in civil liberties, or powerful opposing interests. Almost any combination of the principles can be seen as explaining the final results in each discourse.

Even with the theories presented by Hood (1994), one can account for the shifts in the policies in many ways. The *New Economy* could be the 'idea' behind deregulation and lessening business burden as governments did not want to regulate nascent markets or hurt trust in e-commerce, in this *force of ideas* account. There were numerous articulations of economic harm, costs, and companies moving off-shore as many developed concerns regarding 'economic security' that may have overridden traditional concerns of 'national security'. Both the UK and the U.S. Governments wanted to aid the development of e-commerce and the new economy; appearing to harm this potential was in turn harmful to their images. Some advocates and many in industry were fuelled by libertarian beliefs, and ideas propagated regarding the end of government, the end of the nation state, data havens, anonymous electronic cash; all of which were in some way enabled by cryptography.

Alternatively *power of interests* accounts could accommodate the powerful interests at stake, and their transformation. While companies in the U.S. were in the past willing to acquiesce to export controls, they were no longer willing to do so as their interests to sell products to foreign markets superseded nationalism and foreign policy concerns. Growing concern regarding information networks and increased flows of information created greater awareness of privacy and confidentiality interests, with the growth of NGOs and business actors, willing to pay more attention to the warnings of the epistemic community. Even government interests transformed, as it became increasingly concerned with the Human Rights Act in the UK, and e-commerce.

An explanation that considers the *change of policy habitat* would be equally interesting. Faster computers, combined with the Internet and e-commerce, all of which allowed and created momentum for the widespread use of cryptography. This spread increased its availability and resulted in a circumvention of existing regulations. This in turn rendered policies

useless, leading to the revolt of the business community, whose subjection to the regulations placed them at a competitive disadvantage to international competitors. These shifts led naturally to a liberalisation in the U.S. as regulations were deemed futile in the face of technological and market pressures; and to direct regulation of the individual in the UK as the centralised markets assumed by the DTI policy were no longer applicable in e commerce-oriented decentralised markets.

Finally, viewing the shifts as policy *self-destruction* can offer rich explanations. As we saw the NSA had conflicting goals to secure American traffic and to subvert security in foreign traffic; eventually the conflict in these goals would lead to a situation where the NSA would have to capitulate to one or the other. Similarly, companies may find it in their interests to protect their data and the data of their clients to the highest capabilities; and so they would move development and/or keys off-shore, or use products and services available in the foreign markets to the disadvantage of U.S. companies and proposed UK TTPs. The successive changes to each policy that would have been necessary to manage these 'side effects' would have created a regime so burdensome and complex that liberalisation and regulatory shift was necessary, and each policy naturally self-destructed.

That we can explain the shifts in cryptography policy by any of the above does not devalue this study. Rather, this indicates that any explanation of the policy shifts is affected by ontological, epistemological, and methodological assumptions. If we give sufficient autonomy to social actors, some explanations seem more likely than others; similarly for autonomous technological actors. If we view interests as rational and attribute them to actors, then we can see transformations as a result of powerful bodies; if we see interests as emergent, then we can see transformations resulting from shifts in public perceptions. If we consider functional observations of costs and effectiveness, we will see regulatory burdens rising and creating harm to the point of regulatory transformation and renegotiation.

Instead if we regard the entire process as a discourse of the social and the technological, such a view allows descriptions to emerge resulting from principles pursued, mechanisms attempted, and actors incorporated and excluded, alliances formed and failed. Treating rationalist, functionalist, interpretivist, and public choice accounts as articulations allows for their capture and inclusion as part of the discourse; or derivative from the discourse.

The environment captured in each discourse shows that there were a number of contending principles emerging from discussion surrounding cryptography policy. The complexity in the explanation can be found in the complexity in the discourse, the number of actors, and the amount of conflicting principles pursued by these actors. Stigler's call for research on

explaining why policies are developed remains enigmatic; what I provide is an argument for opening the *black box* of technology policy to see the discourse. This discourse is sometimes broad and large, and I provide some means for capturing socio-technological discourse involving *moments of interest* and mapping regulatory shifts. In so doing, we capture the technological and social actors. Apart from avoiding determinism, socio-technological explanations may capture more of the discourse, and add to an understanding of the principles involved, and their conflicts.

Interrogation of capacities of any of the actors is required; I argued for this particularly for the technological, but any interpretive research would have to accept that actors have many interests, actors view mechanisms and other actors in many different ways, and that the principles being pursued can only emerge from the discourse, rather than be assumed *a priori*. Similar conclusions can be drawn from alliances and coalitions: we can not assume ahead of time that industry or NGOs will act against or in support of regulation. One of the most interesting components of cryptography policy discourse was the diverse set of coalitions and alignments; left and right, extreme and pragmatic co-operating and speaking for one another. This can not be assumed for all policy discourses. Nor can it be assumed that these coalitions still exist. Further discussion of these points will be presented in the next chapter, as implications of the research and its results are considered and applied to other policy domains.

Chapter 8: Implications of The Technological Actor

> When the Fourth and Fifth Amendments were adopted, 'the form that evil had theretofore taken' had been necessarily simple. Force and violence were then the only means known to man by which a government could directly effect self-incrimination. It could compel the individual to testify -- a compulsion effected, if need be, by torture. It could secure possession of his papers and other articles incident to his private life-a seizure effected, if need be, by breaking and entry. Protection against such invasion of 'the sanctities of a man's home and the privacies of life' was provided in the Fourth and Fifth Amendments by specific language. But 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet. Moreover, 'in the application of a Constitution, our contemplation cannot be only of what has been, but of what may be.' The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.
>
> The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.
>
> -- Justice Louis Brandeis, OLMSTEAD v. U.S., 277 U.S. 438 (1928), Dissenting Opinion.
>
> He who breaks a thing to find out what it is, has left the path of wisdom.
>
> -- J.R.R. Tolkien

Abstract

This dissertation has shown the richness in accounting for regulation and transformations within regulatory discourse, particularly if accounts are socio-technological in nature. This chapter will discuss some of the lessons regarding the nature of the technological actor within a socio-technological discourse. These lessons will be applied to other regulatory discourses, as new strategies were developed to apply regulation within a landscape of social and technological actors, some involving cross-jurisdictional strategies. The limitations of these ideas and findings will also be discussed.

8.0 Introduction

This dissertation has presented theory for a socio-technological study of discourse and two technology-policy discourses. Section I of the dissertation introduced cryptography as a mathematical technique and political artefact. This was followed by a review of the regulation literature and the role for technology within regulatory webs, modalities, and habitats. The literature review in chapter 3 introduced the notion of a technological actor

within a discourse, and developed the *moments of interest*, the points in a discourse where the actors, human and non-human, take form, translate and shape the interests of others. The methodology presented in chapter 4 supported this pursuit, based on an ontology of actors, social and technological, interacting, and at times articulating interests and objectives in the world; and an epistemology of gaining knowledge through interaction, deep immersion, and an evolving hermeneutical understanding of both theory and data.

The cryptography policy discourses presented in Section II involved a number of actors, interests articulated, mechanisms proposed, translations attempted, and principles conflicted. The point was to show that the technological actor, within a discourse, had a role to play in assisting our understanding how regulation arises, changes, and fails. In the U.S. study, the *technological* had a large role, as the regulations specified its nature, through key size restrictions or through requirements of escrow or recovery. In the UK, the technological was involved in each proposed regime despite claims of technology-neutrality. Articulations of technological circumvention and jurisdictional arbitrage were common to each discourse.

The technological actor did not dictate what occurred in each discourse. What I found, however, was that looking at the technological actor brought out more depth, from which emerged even more actors and principles. Searching for articulations showed that within the discourses many, if not most, actors had to speak specifically on the technology in order to speak on the policy. The emergence and importance of the epistemic community was outlined by the prevalence of their articulations regarding the technological; but also it was interesting to note their comments on the social. For example, the Risks of Key Recovery report did not focus solely on efficiency issues, but also spoke on trust and risks, that are notably social institutions and by-products. The epistemic community was often organised by the NGO and advocacy community, whose role can not be understated within each discourse. Without these communities, regardless of the technological, the policy outcomes would probably have been different.

Translations were bountiful, originating from and affecting both the social and the technological. The social translated the technological through articulations, attempts to align and embed principles and interests. The technological can be said to have translated the social through objections, recalcitrance, but also through the very fact that social actors spoke on the technological, questioned social transactions based on technological constraints: linked notions of trust to digital signatures, security and privacy to keys. These notions were also interrogated, with the interpretations of a number of actors in order to push for the anti-essentialist sense of triangulation, and ended up with Latourian

triangulation where more often than not, the actors appeared to speak the same language regarding the technology. Risks, trust, costs, efficiency, and keys became the language of many actors, no matter how divergent their interests and the principles they pursued.

The translations and the formation of actors and alliances can only be understood once we abandon determinism of any form, and allow interests and principles to emerge from the discourse. Then we can see how the regulations, and the world, take form; understand the conditions of their development, and understand some of the driving principles to their success and failures. We can see the costs of the alignments; how regulating cryptography effectively required a regulation of access to the Internet, something that could not be achieved easily in democratic societies. Putting cryptography 'back into the bottle' was not a seriously considered option; even after the events of September 2001, such proposals were not seriously considered. In the end we saw the establishment of one of the harshest regimes in the world in the UK where government can compel an individual to hand over a key, despite concerns regarding self-incrimination and issues regarding civil liberties, as protected by the Human Rights Act and the jurisprudence of the European Court of Human Rights.

A number of these issues will be raised in this chapter to understand briefly the implications of this study. In §8.1 I will discuss the implications and weaknesses for this study based on its ontological, epistemological, and methodological assumptions. In §8.2 I will discuss the means of capturing the technological actor, and its implications for the Information Systems and the Regulation disciplines. Implications on the cryptography policy discourse will be discussed in §8.3. In §8.4 I will present some of the technology policy implications of these findings, discussing other policy discourses. I will show in §8.5 how new strategies are being pursued to cater for jurisdictional and technological principles similar to those that arose in this study. A summary and discussion of further research will be presented in §8.6.

8.1 On Assumptions and Weaknesses

The research and analysis of each discourse lead to a few implications. These can be regarded as methodological, epistemological, and ontological in nature.

8.1.1 Implications of the Methodology

Having been close to the data, deeply immersed in the field of actors, it is fair to say that the representations of each discourse are even still quite simplistic. The amount of data that could not be included due to the methodological decision to rely on data that could be

supported by additional evidence, was enormous. Although the shaping of my own understanding and interests due to a hermeneutical understanding was explained in chapter 4, no matter how many measures I could take to include as many actors as possible within the discourse, it is inevitable that I would exclude some principles and interests.

Much of what has been presented here has been reviewed by colleagues who were direct actors in each policy discourse, and this only placed further pressure to be fair to the data; this accounts for the size and complexity of Section II. I believe that if this work was shown to government officials, their response regarding the representation would be that it is simplistic, and may not focus sufficiently on domestic and national security threats. Similarly, privacy advocates would say the same about privacy and human rights. Despite this, however, I predict that both sets of actors would accept the representation, or my 'puppets' (Lee 1991), as being relatively fair. My continued interaction with many of these actors helped to ensure that my understanding of the issue developed within reason.

8.1.2 Epistemological Implications

My deep immersion into the interaction of actors in the discourse confirms my belief that ascertaining the interests of the actors is a difficult and problematic experience. Asking actors for their interests is problematic for a number of reasons: I may not be perceived as a disinterested actor; and as Braithwaite and Drahos argue, the actors may not have a synoptic grasp of their own interests (2000, p.548).

Having worked in a software firm that developed cryptography-based software, I noticed how difficult it is to see the interests of the developers, the company founders, and the executives. What they claimed in public at conferences was often quite different from what they would discuss in mailing lists within the epistemic community, and different from what they would speak of over coffee. To say that human interests are embedded within a technology is, in my opinion, simplistic. This is consistent with Latour's idea that society is not stable enough to project itself into a given technology (1999, p.179). Rather a set of negotiations, a discourse, occurs even at this level where granular social and technological actors determine each other's forms. The technological is more and less than the social intentions involved in its creation; presuming that the social interests are even related.

Collecting the interests of actors, particularly within such a political and secretive discipline of cryptography with principles involving national security and privacy of individuals, is non-trivial, if at all possible. We may rely only upon what is said, the articulations, the reports, and what the actors state publicly. Back room discussions may have shifted the regulatory regimes; there are explanations that I may not have been able to capture. Yet I do

not provide an authoritative explanation for the reversals; rather I merely provide a description of the conditions within which regulatory change occurred. This is the weakness of my epistemology; but at the same time, the same can be said of any study.

8.1.3 Ontological Implications

Viewing the world as actors pursuing interests, creating alliances, is already a controversial ontology. That these actors are both social and technological makes matters more complex. Apolitical ontologies of benign policies, technologies, and governments clearly would not have brought out the full colour of the landscape. However, assuming self-interested actors does little to add colour as well, as raised previously whilst discussing epistemology. The ontology of actors with unclear, emergent interests and principles, sometimes conflicting, adds some understanding to the complexity of this world. Governments did not necessarily wish to regulate; companies did not necessarily want to sell products to just anyone in any market; individuals didn't necessarily want military-grade cryptography to purchase books on-line. It can be said that the discourse made the interests more black and white, as political discourse may require.

Adding the technological as an essential component to the research approach was a hazardous exercise. Granting agency to technology is dangerous theoretically. My point is not that technology determined the policy; nor merely that technology caused a change of policy due to changes in the policy habitat (Hood 1994). My view was that society and technology are part and parcel of the same discourse, and inseparable (Latour 1991; Latour 1999). That is, my ontology was that the world is actually socio-technological, full of negotiations, alignments, alliances, and compromises. Excluding the technological within our explanations requires explicit explanation; after all politics and society consist of technology.

The particular attention to technological issues was an intentional research act to show that technology had a role to play in technology policy. Of course if I would have concentrated so much on other factors, such as time, critical issues such as participation and inclusion, power issues such as the nature of the nation-state, different results would have been presented. Not giving overt priority to the study of power and politics may detract from my study. Latour's response to accusations of this line of research being apolitical in its presentation of findings sets this out clearly.

> Refusing to explain the closure of a controversy by its consequences does not mean that we are indifferent to the possibility of judgement, but only that we refuse to accept judgements that transcend the situation .... Domination is an effect not cause. In order to make a

> diagnosis or a decision about the absurdity, the danger, the amorality, or the unrealism of an innovation, one must first describe the network. (Latour 1991, p.130)

Describing the habitats (Hood 1994), webs of influence (Braithwaite and Drahos 2000), modalities of regulation (Lessig 1998), the network (Callon 1991), or the collective (Latour 1999) of social and technological actors provided useful means of describing the regulations and transformations. I leave discussions on the 'power of government', 'politics of civil society', and other such issues for further research.

Latour's 'situation', networks, and collective, or Braithwaite and Drahos' web of influence bring us to the 'discourse', where action occurs, statements are made, articulations are shared, and the actors take form, and negotiation and compromises take place, and objections stated. Whether public or private, open or closed, my ontology that the world is embroiled in and encompassed by discourse allows for a macro and micro approach to problems. The micro approach allows us to watch how each actor's capacities are discussed and negotiated. The macro approach allows us to treat all actions, all statements, even explanations, as elements of the discourse. Deterministic accounts, tales of social construction, accounts based on economics and trade, and reports on policy analyses are all parts of the discourse. What can be extracted from the discourse are patterns, principles, and lessons, particularly involving the objection of technological actors.

It can be said that the description of the social may have suffered while I emphasised the technological. Walsham (1997) notes that socio-technological case studies may suffer from overemphasising the technological, and may also require book-size presentations of the results. Even Lessig notes this challenge due to the complexity of each modality or regulation, and giving an explanation of each set of interactions can 'easily overwhelm' (1998, p.685). These are fair criticisms, but for the purposes of a PhD dissertation, I felt that I could be liberal with explanation. As for journal publications and conference papers, and even conference presentations, I feel that I have been able to do 'justice' to the data even within constraints of time and space.

8.2 Understanding the Technological Actor

The technological actor is useful to regulation theory and to Information Systems. Both of these disciplines suffer from a lack of appreciation of the technological. Chapter 2 reviewed the literature on regulation and showed how technology is either treated nominally, deterministically, or merely in the background. Chapter 3 showed that the IS literature lacks

an appreciation for the role of technology, supported by Orlikowski and Iacono's claim that often the technology is taken for granted (2001).

Orlikowski and Iacono (2001) argue that we must try to find a way of theorising about the IT artefact. This must be done, however, in a way that accepts that the artefacts are not natural, neutral or universal; capturing articulations and a number of different interpretations must be expected, in accordance with the anti-essentialist viewpoint (Grint and Woolgar 1997). Secondly, they argue that we have to accept that artefacts are embedded in some time, place, discourse, and community, in an attempt to abandon technological determinism. Capturing the technological actor within a discourse, as argued previously, necessarily requires an abandonment of determinism (both social and technological). Third they argue that artefacts are made up of fragile components, and are thus not monolithic, uniform, or unified. This was noticed as the articulations arose in the discourse and changes to the objects of regulation occurred, or limitations and weaknesses in designs were noticed. Granularity in the technology increased as 'cryptography' was decreasingly treated as some holistic black box.

Orlikowski and Iacono's fourth claim is that artefacts are neither fixed nor independent, and rather emerge from ongoing social and economic practices. Their point is that we must look for how technologies change over time, and how they are shaped by social forces. I would argue that while this is true, there are times, based on Latour's ideas, that the object does take form through rejecting what is said about them, or rejecting translations in that they fail in alliances, or force further action and objections in humans. Finally, Orlikowski and Iacono claim that artefacts are not static, but dynamic and contingent, and are prone to fail, redevelopment, and change. Cryptography may be implemented in a number of ways, admittedly, but in the discourses of study, cryptography as an actor was settled upon the more there was discourse. Smaller keys were abandoned for larger keys; weaker algorithms were fixed to resist known means of attack. Adaptations of the algorithms were attempted, just as the process of codifying laws was based on interpretations of both the technology and the laws (varying from Lotus, Microsoft, PGP, and Entrust).

Being able to identify both within the IS and the regulation literatures how technology brings changes in strategies, and how technology is an essential part of a given discourse is valuable for understanding how technology interacts with individuals, organisations, and society. The technological actor captured at moments of interest within a discourse shows how actors regard technology, but also how technology may be recalcitrant, introduce its own actors, and act (or allow others to act) as obligatory passage points (Callon 1986). Adding technology to the frame of understanding helps us to understand how regulation

forms, and is transformed, and the possible role that the technological plays in binding and breaking regimes. This may contribute to understanding other forms of regulation, and other regulatory discourses.

The goal of capturing articulations, translations, and speech regarding technological actors assists in understanding the interests of human actors as well. That the NSA both developed Clipper yet claimed that there were risks in key recovery says something about the NSA. When government spoke specifically about key recovery, compared to when business spoke of key recovery, it was possible to discern a difference in motivation between the two sets of actors. Technological specifications of Trusted Third Parties also divulged information that the DTI was not yet willing to admit, that the policy was not technology-neutral and had envisioned specific algorithms (*CASM*) designed to meet the interests of the Government in interception and decryption capabilities.

We must also interrogate the technological actors as they take form. Triangulation is an important device from both the anti-essentialist and Latourian perspectives. Just because the media regarded NSAKEY to be an NSA translation of CAPI did not mean that the NSAKEY allowed for surreptitious access by the NSA. In triangulating, it is often helpful to seek out the epistemic community to hear their comments. The relationship between technology and the epistemic community within political discourse is interesting and worthy of further study.

This call to interrogate the technological actor is not to say that the technological actor is the primary actor, or necessarily an obligatory actor within a discourse. Rather the point of this research was to show that additional depth into a discourse can be sought if we look for the technological actor. Sometimes it may very well be in the background and perhaps unnecessary to interrogate. The researcher's task is to decide if it is appropriate to bring it forward for interrogation.

Within technology policy at least, I predict that the role of the technological actor will be important to understand. Without analysing the technological actor within the cryptography policy discourse, claims of the benefits of key recovery could not be assessed adequately. Circumvention of policy would also not be understandable and taken merely on the merits of the actor making such claims. The principles that arose could not be as easily explained without understanding the technological actor; after all why was cryptography both an issue for e-commerce and national security, and why was it difficult to de-couple these issues? Why did cryptography policy types appear to be similar across countries? In each case, it was in part because of the technological.

It is my contention that if we are able to understand the role of both the social and the technological sufficiently within a discourse, then we will be able to better understand policy shifts in accordance with Hood's explanations. The *force of ideas* may incorporate some technology, as various ideologies may be associated with new technologies and economies. The *power of interests* accounts may include technology as a set of interests, or show how technology affected the interests of actors. The *change of policy habitat* accounts may incorporate technology into explanations of how new socio-technological structures affect existing policies and the according structures. Finally, policy as its own *self-destruction* may incorporate some form of technological actor contributing to the self-destruction, or that assists in explaining components of the self-destructive policy design. From all of these explanations, principles may emerge, and we can understand the constitution of policies by seeing the actors, mechanisms, and alliances involved.

8.3 Understanding Socio-Technological Regulatory Discourse Settlements

The settlements in the U.S. on liberalisation and the settlement in the UK on lawful access to keys, however, do not mean that the discourses have ended. In each case, new strategies have been developed by a number of actors to maintain or question the new state of affairs.

Some consider the current regime in the UK as institutionalised in the *Regulation of Investigatory Powers Act* 2000 to be hazardous to civil liberties. There is discussion of questioning its legality under the European Convention on Human Rights, particularly on grounds of proportionality and self-incrimination.

The U.S. Government may not implement similar measures of regulating the individual use of encryption, or lawful access to keys. In some senses, the U.S. policies involved indirect regulation because directly regulating the actions of individuals is constrained by many other laws, and the Bill of Rights. We have already seen collisions of the 1st Amendment and the right to publish source code; it is predicted that the 4th Amendment constraint on government may be called to question as some consider lawful access to keys to be an *unreasonable search and seizure*, and similarly the 5th Amendment constraint on self-incrimination would be problematic if an accessed key will be used to collect evidence. A number of proposals were considered, but never actually introduced. Rather, the Department of Justice in the U.S. pursued technological solutions.

The first solution emerged from a criminal court case, *United States v. Scarfo* (Politan 2001). It was discovered that the FBI surreptitiously placed a key-logger system (KLS) on the

computer of a suspect who was using PGP to encrypt files. Once they discovered the passphrase, the files were decrypted, and incriminatory evidence was found. The court asked that the details of the KLS be disclosed to ensure that it did not perform more than the FBI claimed, i.e. did not over-disclose data to the investigators beyond the remit of the warrant. The Department of Justice argued that such a disclosure would harm national security interests and future law enforcement investigations. The Judge decided that the disclosure and review would take place in-camera. The judicial review sided with the prosecution: the over-disclosure of infomation was not considered problematic, and the evidence was not suppressed. The case eventually ended in a plea bargain, but the KLS's existence is now known, and it is now part of the discourse.

Another solution is the placement of a virus on computers that will disclose private encryption keys. The FBI confirmed the existence of *Magic Lantern* in December 2001 (Reuters 2001), claimed by some to have been used to install the KLS in *Scarfo* (Cryptome 2001). Controversy arose surrounding this announcement, as anti-virus companies argued that they could not leave a hole in their protection software to allow for Magic Lantern. Doing so, they argued, would create a conflict of interests. Moreover if each country's law enforcement agency developed a similar form of virus, each virus would have to be excluded from anti-virus products: translating the purpose of the software, and affecting consumer trust.

All of these solutions directly affect traditional laws and constitutional protections. Although the powers enforced by these solutions are not clearly illegal, it is not controversial to argue that the powers are quite different from previous powers of law enforcement. In the RIP debates, it was acknowledged that the power of lawful access to keys had no precedent. Similarly, *Scarfo* questions whether the KLS was an interception system or a search and seizure, with the former requiring greater due process provisions than the latter according to U.S. law. Finally, the idea of legitimating viruses sanctioned by the state requires the enrolment of anti-virus companies and their products.

The discourse of social and technological actors does not always end in settlement. There are two points worth noting however. First, proper interrogation of the technologies appears to be a controversial idea; *Scarfo* questioned whether a technology's capacities can be reviewed openly prior to allowing evidence into the court, just as the capacities of *Skipjack* were questioned for perhaps introducing further faults. Similarly for the anti-virus companies, who usually protect their intellectual property from open review; it will be difficult to verify without appropriate interrogation of the technology, whether there have been attempts to permit Magic Lantern through the anti-virus software defences. Second,

the importance of understanding social and technological actors within a discourse is particularly valuable when we also consider legal issues such as jurisdiction. Applying a KLS in another jurisdiction is technologically as easy as doing it within the U.S., but legal technicalities arise. Similarly with the anti-virus companies: would Israeli or Finnish anti-virus companies allow a U.S. Government virus to slip through their products' defences?

Again principles of trust, commerce, national security, and law enforcement arise and conflict with one another. Another set of issues that also continue to arise are regulatory competition and international arbitrage (Sun and Pelkmans 1998). This occurs as countries seek reciprocity and mutual recognition (Braithwaite and Drahos 2000) of national policies, and other such mechanisms. My point is not that these same issues will always arise; rather I would posit that the conflict of principles and the settlement upon clear mechanisms are not trivial exercises.

8.4 The Technological Actor and Other Policy Discourses

Throughout the 1990s there were a number of national policies introduced to regulate the use of technology. While some of these will be discussed here, the discussion will be brief as each case involves its own discourse with a number of actors and principles sought; and so the explanations may appear simplistic. The point of this section is to show how this research approach may be used to collect and analyse data from other policy discourses to understand their richness. Actors, interests, principles, alliances and objections will be highlighted for each.

8.4.1 Censorship

Without a full review of the issue of censorship, it suffices to say that some governments decide that there are specific types of information that are considered 'indecent or harmful' and thus unacceptable for citizens to access. In the pre-Internet era, it is argued, such controls were more technologically feasible as governments could control the flow of data across borders as this data was usually in the form of tangible goods, or access was enabled by industries that were regulated, and infrastructure that could be governed. With the common use of the Internet and its expansion across borders, problems have arisen. Governments still try to maintain controls through regulation, but they inevitably encounter challenges. It can be said that the traditional habitat of censorship transformed, but this transformation was socio-technological: not only because of the protocols, but also because of the nature of the industries, regulations, and interests surrounding the traditional regulations did not easily apply to the new set of actors.

The situation in Australia provides an example of the challenges that arise. Consider the statement of a proponent of government regulation, Gareth Grainger, Deputy Chairman of the Australian Broadcasting Authority:

> Broadcasting and now the Internet make use of public property, the airwaves and bandwidth. Broadcasting remains, and the Internet is clearly emerging as, a means of mass communication of a particularly intrusive nature. (...)
>
> It is essential for policy makers and legislators, as they review existing and prepare new rules for broadcasting and the Internet, to revisit and restate the public interest objectives they believe should apply to those industries and their governance. (Australian Broadcasting Authority 1999)

He translates the Internet into a 'means of mass communication', thus falling under the remit of the ABA. In turn, the ABA acts within its remit to pursue its goal of meeting the public interest for content controls.

In response to Mr. Grainger's comments and initiative, Clarke (1999) states

> What is appalling about this statement, the government's policy, and the legislation that was passed by the Opposition-controlled Senate as well as the Government-controlled House, is that it is framed in blithe ignorance of the nature of the technology and hence of the behaviour that it pretends to regulate. This results in no advantages to the intended beneficiaries, and is to the serious detriment of all involved.

Professor Clarke (a professor in Information Systems) argues that the ABA's translation of the Internet is faulty, or ignorant. His claim is supported by many others, many of who disagree with censorship. This is an example of the problem that arises when we let humans speak for the technological actors: the interests of the speaker are embedded within their interpretations and representations. Similar articulations arose from the hacker community (Dogcow 1999), who also advised individuals on the means of circumvention of the controls, using encryption, point-to-point connections, proxy connections, and many other technological actors. By introducing these new interpretations to the actor considered 'the Internet', its *black box* is opened and we see a different set of actors within, including servers and protocols.

Proponents of censorship often turn to introducing new technological actors of their own. At first rating systems for content were proposed, where files were to be attributed with a rating; translating the nature of 'files' to including 'files+ratings'. The American Civil Liberties Union responded with a report (1997) countering with their own articulation regarding the Internet: that because of the *culture, economy, and structure of the Internet* such a

rating system would be impractical, particularly due to international arbitrage and concerns for the burdens upon small business.

Another actor introduced by proponents of censorship is client-side filters that would prevent users from accessing 'indecent files'. Again a report was released, this time by the Electronic Privacy Information Center (1997) that interrogated the capacities of the filters and showed that because of the *nature of the Internet*, its distribution, and the challenge behind creating sufficient automated verification of decency, these filters would also block some 'non indecent' content. Additionally, some indecent material still was not filtered. Later reports claimed that these filters were not at all *objective*, but were politically developed to block web sites that opposed the interests of the developers, such as free speech organisations. In this sense, by blocking more than 'indecent' information, but also less than 'indecent' as well, and blocking political opponents, the interests of the developers were not all that is exhibited by the filters. Rather, it can be said that the technology itself exhibits regulatory characteristics.

Interesting issues also arose with the first formal policy process on content regulation in the U.S. When the *Communications Decency Act* was struck down by the courts in *ACLU vs. Reno* (1996), the claim was that deciding what was indecent information was too difficult; and restricting access based on the age of consent was also technologically challenging and costly. The court stated that "any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig", and this was "due to the nature of the Internet" and the Constitution. The articulation of the court regarding infrastructure claimed that the internet was different from all previous information infrastructure, and as a result the habitat was different, and the interests that had to be defended were also different.

8.4.2 Communications Surveillance and Interception

There is no shortage of cases that can be studied regarding government policies and surveillance. As mentioned in chapter 2, the case of the *Communications Assistance for Law Enforcement Act* in the U.S. is an interesting study of indirect regulation. In this case the U.S. Government enrolled the telecommunications industry and an NGO to create CALEA in order to meet the interests of law enforcement within the 'digital age'. That is, technology was changing in the telecommunications infrastructure that made it more difficult for government to maintain their wiretapping capabilities over telephones. So the law enforcement community enrolled the telecommunications industry with subsidies (over 500 million USD), and the civil liberties community through negotiation away from worse alternatives (Bakel 1996) in order to reshape the infrastructure to make it wiretap-enabling.

If CALEA was just another policy issue, it would have been simple, and approaching it from a purely social way would tell the basic story: Governments wanted access when the 'system' changed; they negotiated with industry, and costs were discussed, and the outcome met the issue of costs and civil liberties.

However, looking at it from a socio-technological perspective, the analysis may be different. The U.S. Department of Justice wanted to shape an infrastructure for their interests, i.e. to maintain their powers of interception, so they acted within a discourse with the other actors (telephone companies, NGO). The technology was translated -- the capacities were changed, and the costs and efficiency issues did come up, but this was to be resolved through subsidies. CALEA was passed, the policy process ended, but the technology policy issue continued. Since the original policy settlement in 1994 more powers have been requested to meet government's interests, such as location data. The principles pursued by the government are more than just interception: it became *Interception + Irrespective of technology*. Since then, the government has not been willing to pay for all of the changes; it is now *Interception + Irrespective of technology + Regardless of Subsidy*. In fact CALEA is now an actor within the subsequent discourse: because of CALEA, the U.S. Government can make further requests for further powers even when their interests change. Through the translating of a technology, not only is government determining the type of society, but also technology remains up for interpretation and its 'capacity' becomes less and less of an issue. As a regulated entity, telephone companies could not make arguments of foreign competition or costs and burdens; the discourse was quite different from cryptography policy. There was also a limited epistemic community, but NGOs did participate and some criticised the Act publicly.

In contrast, in 1999 the Department of Justice appealed to the Internet Engineering Task Force (IETF) to develop a protocol for the Internet that allowed for wiretapping, because both actors agreed that wiretapping on the Internet was challenging. The nature of the 'voice' of the IETF was democratic where all members had a vote, and anyone can be a member. After a lengthy debate, the IETF decided against creating such a protocol. Some dissent was present, as some believed that the IETF could (and should) create a determinist protocol for wiretapping that could be used around the world; but determinist in the sense that it disallowed flexibility, and would uphold a high-safeguarded warrant regime technologically.

Shortly thereafter, evidence regarding *Carnivore* began to appear. Carnivore (now named DCS1000) was developed for the FBI, designed to collect, filter, and transfer network traffic to law enforcement officials. The system is under the control of the FBI, and

installed at ISPs when a warrant is issued. Similar to *Scarfo*'s KLS, concern arose regarding the nature of the data that Carnivore collected: was it collecting all IP traffic for all users of the ISP, and then filtering out 'interesting' and 'relevant' data? Or was it able to focus on the individual named on the warrant, and when appropriate, only gather traffic data (email headers)? A review of the system was conducted in a closed environment, and even still trust in the system remains an issue. When the U.S. Congress passed the USA-Patriot Act in October 2001, an amendment was included providing judicial oversight of law enforcement's use of Carnivore, permitting greater interrogation of the capacities of the technological actor.

8.4.3 Other Policies: Traffic Data and Intellectual Property

The policy discourses surrounding traffic data and intellectual property involve a different set of actors from one another. Traffic data access by law enforcement tends to involve similar actors to surveillance policy discourses, with industry generally seeking subsidies or minimal regulations; and with some alliances between policy advocates and industry. Intellectual property is a case where NGOs and policy advocates tend to be opposing the alliance of government and industry. Even more complex is that the *industry* actor-category or entity is quite fragmented, and in turn so are their interests. In the recent policy debates surrounding trusted computing platforms, computer and content industries debated each other often regarding costs and threats to their respective interests and markets. More simply put, there was a contest of principles even within industry.

The unifying strand behind these two discourses, however, is that the technological can be understood to play a role of changing the landscape. In the case of traffic data, the very constitution of 'traffic data' changes for each communications infrastructure, each protocol, and each service. Therefore, the sensitivity accorded by law to 'traffic data' should depend on the technology (Escudero-Pascual and Hosein 2003). The strategy of policy-makers, however, is to insist on creating technology-neutral policy. Similarly for intellectual property, laws have been introduced and passed (such as the U.S. *Digital Millennium Copyright Act*) that were written to maintain the copyright privileges of the non-digital world within the now digital environment. In so doing, however, the powers of copyright holders are increased according to the law, and the fair use rights of individual diminished (Lessig 2001).

As a result, technology-neutral policy can be used politically, as including and excluding the technological from the discourse has political implications. With the RIP debates in Parliament, arguments of technological circumvention were dismissed due to politics between FIPR and the Home Office ministers. In these cases, the technology-social

interaction is disregarded, and in so doing, the powers of the government and content industry are actually increased. Omitting actors within the discourse, therefore, is strategic. The 'updating' of laws, even those that 'maintain the status quo' (Reno 1996) through being 'technology neutral', are thus questionable.

8.5 Global Policy Issues

The policies discussed in §8.4 point to consideration of the technological actor within policy discourse. This section will briefly discuss policy strategies that deal primarily with jurisdictional conflict, and in turn, international regulatory co-operation.

In both the U.S. and UK policy discourses, statements and claims regarding international complications continually arose. In the U.S., foreign availability of encryption products threatened the U.S. control of the market, and exacerbated the burden of export controls. In the UK, early policies required subjects to use UK TTPs, a violation to the single market ideal of the EU. Later policy discourse, particularly in Parliament and in the BCC report, relayed concerns regarding regulatory arbitrage, and how policies could place the UK's economy at a disadvantage. The dosing words in the debates in Parliament included the Home Office minister's call for international propaganda to combat the harmful claims of the policy's opponents.

International co-operation and harmonisation of policies were sought in cryptography policies. The U.S. sought agreements with other countries on export controls through international agreements (i.e. COCOM, and later the Wassenaar Arrangement). The U.S. Government also sought harmonisation of key recovery policies at the OECD. The Crypto-Tsar position was created to pressure other countries to adopt U.S.-friendly policies to ensure harmonisation, but also to ensure a market for U.S. key recovery products.

The cause of harmonization has been used in other surveillance and data flow management policies. Articles 25 and 26 of the *EU Data Protection Directive* require that before personal data is sent to other countries outside of the EU, these countries must have 'adequate' laws to protect this data. This policy result is relatively unique, however, in that it actually raises intentionally the protection of individual rights across borders.

For years the Group of 8 Industrialised countries have been working to harmonise surveillance laws to allow for mutual legal assistance in criminal matters, and also to ensure that all the G8 countries share similar surveillance powers. These 'powers' include lawful access to communications, traffic data, and requiring the retention of traffic data at ISPs

and telephone companies for a period of time specified by the policy, and in direct conflict with data protection laws in some of the member countries (Canadian Delegation 2001).

Another model for harmonisation and cooperation, however, is the Council of Europe convention on cybercrime (Council of Europe 2001). The CoE, a 43-member international treaty-making body, has been working since 1997 on this convention. It is in fact three conventions in one. First it harmonises substantive law on hacking, and other such crimes. Second it harmonises procedural powers, ensuring that all signatory states pass laws giving powers of surveillance and evidence collection to law enforcement agencies. Finally, it acts as an unprecedented mutual legal assistance treaty, ensuring that all signatory states share the surveillance and evidentiary powers with other states upon request.

The CoE convention is not only an effort in harmonisation and cooperation, however; it is an effort in modelling (Braithwaite and Drahos 2000), where countries will accept that the powers described in the convention should be translated into national law. Although there is some interpretation allowed by ratifying states, it is argued that this flexibility exists only to grant even more power to some states that are not limited by legal constraint (Global Internet Liberty Campaign 2000).

In creating international pressure to regulate, and also creating a harmonised set of rules across borders, governments are in effect decreasing the likelihood of regulatory arbitrage principles arising in future discourses. Companies will be less likely to move off-shore with their encryption keys, particularly as Article 19 of the CoE Convention can be interpreted as requiring countries to create lawful access powers to secured data. Costs of adherence to the regulatory requirements will be born equally regardless of jurisdiction. Governments are given incentives to sign the convention; countries who wish to gain access to investigative data from other countries will want to sign, while countries who also want an international imperative to pass new laws criminalising activities and creating powers of investigation can now derogate responsibility to the Convention.

The benefit of this discourse to governments, however, was that it was not conducted publicly and involved limited consultation (Global Internet Liberty Campaign 2002). The Council of Europe, to the best of its abilities, managed to limit the amount of actors invited to participate. In essence the discourse now speaks for itself, and it speaks in the language of principles of lawful access to data. Like the traffic data and copyright discourses, the effects of the technological actor are dissuaded from study; but unlike these discourses, other actors were also intentionally excluded.

8.6 An Agenda for Future Research

The line of inquiry presented in this dissertation pursues the technological within socio-technological discourse. I have argued that we may better understand regulation as a socio-technological discourse in the case of cryptography policy; and have contended that such an approach is of use for studying other policies. The approach used sees the regulatory world filled with actors with interests pursuing principles, and translating action and interests of others within regulatory discourse. The dissertation contends that we must identify the actors, interrogate capacities and interests of humans and non-humans, and by looking at the discourse at moments of interest we may generate a deeper understanding of explanations of regulatory change, and principles articulated.

This form of inquiry is a multidisciplinary contribution, and calls for further multidisciplinary research. Generally, the contribution is to the social sciences, and specifically to our understandings of Regulation and Information Systems. The notion of discourse as where negotiations take place, policies introduced and transformed, and interests and principles emerge through interaction among actors, contributes to our understanding of how regulations, technologies, institutions, and rules take form. The very notion deserves further research, involving critical, political, and anthropological literature to understand who is included, who is excluded, and how to activate discourse.

Understanding the discourse surrounding the creation of policies and the formation of coalitions in line with Stigler's call for research (1988, p.xiii and 1983, p.541 respectively). It also gives us the means to understand the role of technology within these discourses, to see how it objects to, translates, and is translated by articulations of other actors. The regulation literature has been lacking an appreciation of the technological actor. Although Braithwaite and Drahos (2000) acknowledge the importance of discourse (or webs of influence), they fail to include technology as an actor despite their Latourian approach. Hood acknowledges that technology may play a role in explanations of policy transformations, but finds that existing explanations of policy habitat changes are deterministic, while other explanations of interest transformation and policy self-destruction continue to lack adequate appreciation of technology (Hood 1994). Lessig and his call for the New Chicago School brings technology into the regulatory sphere by considering architecture as a modality of regulation (Lessig 1998); but he fails to explain sufficiently how a technology can be used as an indirect form of regulation, and how it can fail to do so as well. More importantly, he fails to explain how we can capture the role of technology within regulation beyond reading the laws or looking at the Code (Lessig 2000).

The means of capturing the technological actor, and in turn understanding other actors through their attempts to translate, and translation by the technological actor also contributes to the discipline of Information Systems. Previously, Information Systems has been weak on discussing either the social (Clarke 1988) or the technological (Orlikowski and Iacono 2001). This dissertation argued that neither must be ignored and neither can be deterministic when seen within a discourse, supported by similar views of actors within networks (Callon 1991), or entities within collectives (Latour 1999). The work of Callon and Latour, however, does not recommend the means for collecting data regarding the interplay of the social and the technological. My proposal of *moments of interest* within a discourse provides means to see how the actors take form. This technique was used within two discourses to show the emergence of interests and principles, articulations and translations, and how strategies were changed.

There are countless limitations, however, to this line of research. The data collection had to be limited considering the breadth of each discourse. Often actors in the field would recommend a report that I had not yet seen, or offer a quotation and reference that I had not yet heard; the scope of collection had to be limited due to exhaustion. The intentional research act of paying close attention to the technology was supported by constant interrogation of statements and claims of capacities; this level of attention was also aimed at some human actors to the best of my capabilities, but surely more could have been done on this.

Much more of the context could have been included and explained if I had studied interests and histories more, and/or performed more interviews. I could have included past glories of the NSA, past controversies and abuses. I could have included more on the legislative environment in the 1990s, explaining general reluctance to regulate technology but also while doing so selectively, and politically. I could have used different approaches, consider issues of power, how norms evolve, how laws structure action, how political systems structure debate, and issues of governance and globalisation; but I leave this to future work, by myself and others.

Despite all these limitations and faults, there remains some value. All explanations are like models; faulty, but they provide insight. It is my hope that the discourses as presented provided some insight into how regulations were formed and are transformed, and some additional insight into how these can be explained, accounted for, and understood.

References

Akrich, M. "The de-scription of technical objects." In Shaping technology / building society: studies in sociotechnical change, ed. Wiebe E. Bijker and John Law, 205-224. Cambridge MA: MIT Press, 1994.

"ACLU v. Reno." United States District Court for the Eastern District of Pennsylvania, 1996.

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Neumann, P. G., Rivest, R. L., Schiller, J. I., and Schneier, B. Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption. Washington: Center for Democracy and Technology, 1998.

ACLU. Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet. American Civil Liberties Union, 1997.

Adler, E., and Haas, P. M. "Conclusion: Epistemic Communities, World Order, and the Creation of a Reflective Research Program." International Organization, Volume 46, Number 1, 1992, pp. 367-390.

Anderson, R. "Why Cryptosystems Fail." A paper delivered at the Proceedings of the 1st ACM conference on Computer and Communications Security, Fairfax, Virginia, 1993.

Arthur, W. B. "Chapter 26 -- Competing Technologies: an overview." In Technical change and economic theory, ed. Giovanni Dosi, Christopher Freeman, Richard Nelson, Gerald Silverberg, and Luc Soete, 591-607. London: Pinter Publishers, 1988.

Atkinson, P., and Hammersley, M. "Ethnography and Participant Observation." In Strategies of Qualitative Inquiry, ed. Norman K. Denzin and Yvonna S. Lincoln, 110-135. London: Sage Publications, 1998.

Australian Broadcasting Authority. Broadcasting, co-regulation and the public good. 1999, NR 101/1999.

Bakel, R. v. "How Good People Helped make A Bad Law." Wired Magazine, February 1996.

Baldwin, R., and Cave, M. Understanding regulation: theory, strategy, and practice. Oxford: Oxford University Press, 1999.

Baldwin, R., Scott, C., and Hood, C. A reader on regulation Oxford readings in socio-legal studies. Oxford: Oxford University Press, 1998.

Bamford, J. The puzzle palace : a report on America's most secret agency. Boston: Houghton Mifflin, 1982.

Banisar, D., and Schneier, B. The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance. New York: John Wiley and Sons, 1997.

Baskerville, R. L. "Investigating Information Systems With Action Research." Communications of the Association for Information Systems (on-line edition), Volume 2, Number 19, 1999.

Baskerville, R. L., and Wood-Harper, T. "Diversity in information systems action research methods." European Journal of Information Systems, Volume 7, Number 2, 1998, pp. 90-107.

Baskerville, R., and Pries-Heje, J. "Grounded action research: a method for understanding IT in practice." Accounting, Management and Information Technologies, Volume 9, Number 1, 1999, pp. 1-23.

BCC. The economic impact of the Regulation of Investigatory Powers Bill: An independent report prepared for the British Chambers of Commerce. London: British Chambers of Commerce, June 2000.

Beatson, J., and Eicke, T. In The Matter Of The Draft Electronic Communications Bill And In The Matter Of A Human Rights Audit For Justice And FIPR. October 1999.

Bijker, W. E. Of bicycles, bakelites, and bulbs : toward a theory of sociotechnical change Inside technology. Cambridge, Mass: MIT Press, 1995.

Bijker, W. E., and Pinch, T. "The Social Construction of Facts and Artifacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other." In The social construction of technological systems: New directions in the sociology and history of technology, ed. Wiebe E Bijker, Thomas Hughes, and Trevor Pinch, 17-50. Cambridge, MA: The MIT Press, 1987.

Bimber, B. "Three Faces of Technological Determinism." In Does technology drive history ? : the dilemma of technological determinism, ed. Merritt Roe Smith and Leo Marx, 79-100. Cambridge, Mass: MIT Press, 1994.

Black, J. "Group discussions sessions 5 and 6." A paper delivered at the Short Course on Regulation, The London School of Economics and Political Science, 11th-15th September 2000.

Blaze, M. "Protocol Failure in the Escrowed Encryption Standard." A paper delivered at the Second ACM Conference on Computer and Communications Security, Fairfax, VA, November 1994.

Blaze, M., Diffie, W., Rivest, R. L., Schneier, B., Shimomura, T., Thompson, E., and Wiener, M. Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security: A report by an ad hoc group of cryptographers and computer scientists. Business Software Alliance, 1996.

Boland, R. J. "Phenomenology: A Preferred Approach to Research on Information Systems." In Research Methods in Information Systems, ed. E. Mumford et. al., 193-201. North-Holland: Elsevier Science Publishers, 1985.

Borisov, N., Goldberg, I., and Wagner, D. Security of the WEP algorithm. Berkeley, CA: Computer Science Division, University of California, Berkeley, 2001.

Bowker, G. C., Timmermans, S., and Star, S. L. "Infrastructure and Organisational Transformation: Classifying Nurses' Work." In Information Technology and Changes in Organizational Work, ed. W Orlikowski, G Walsham, M.R. Jones, and J.I. DeGross, 344-370. Cambridge: Chapman & Hall on behalf of the International Federation for Information Processing (IFIP), 1995.

Braa, K., and Vidgen, R. "Interpretation, intervention, and reduction in the organizational laboratory: a framework for in-context information system research." Accounting, Management and Information Technologies, Volume 9, Number 1, 1999, pp. 25-47.

Braithwaite, J., and Drahos, P. Global business regulation. Cambridge: Cambridge University Press, 2000.

Brands, S. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy: MIT Press, 2000.

Brands, S., Hosein, I., and Perrin, S. Privacy Increases Smartcard Security. Venice, Italy: 22nd Data Protection Commissioners Conference, 2001.

Briceno, M. RE: GSM security questions. posted to UKCrypto mailing list, October 21, 1999.

Brown, I., and Gladman, B. Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses. Foundation for Information Policy Research, July 2000.

Callon, M. "Some elements of a sociology of translation: Domestication of the scallops and fishermen of St. Brieuc Bay." In Power, action and belief: a new sociology of knowledge?, ed. John Law, 196-233. London: Routledge, 1986.

Callon, M. "Techno-economic networks and irreversibility." In Sociology of Monsters: Essays on Power, Technology, and Domination, ed. John Law, 133-161. London, England: Routledge, 1991.

Campbell, D. "Only NSA can listen, so that's OK." Telepolis, June 1 1999b.

Campbell, D. DEVELOPMENT OF SURVEILLANCE TECHNOLOGY AND RISK OF ABUSE OF ECONOMIC INFORMATION (An appraisal of technologies for political control): The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition. European Parliament Directorate for General Research, Directorate A, The STOA Programme, 1999a, Part 4/4.

Canadian Delegation. Discussion Paper for Data Retention Workshop. Tokyo: Group of 8 Conference on High-Tech Crime, 2001.

Checkland, P. "Soft Systems Methodology: A Thirty Year Retrospective." Systems Research and Behavioral Science, Volume 17, 2000, pp. S11-58.

Checkland, P. Systems Thinking, Systems Practice. Chichester: John Wiley, 1981.

Clarke, R. "Economic, Legal, and Social Implications of Information Technology." MIS Quarterly, Volume 12, Number 4, 1988, pp. 517-519.

Clarke, R. "Subject: ABA Demonstrates Its Ignorance to the World." Forwarded to the Politech Mailing List, message titled FC: More on Australian official demanding Net-regulation -- demonstrating ignorance to the world, November 3 10:42:30 -0800 1999.

Council of Europe. Convention on Cybercrime, ETS no.185. Strasbourg, 2001.

Cowan, R. "Nuclear Power Reactors: A Study in Technological Lock-in." Journal of Economic History, Volume 50, Number 3, 1990, pp. 541-567.

Crowell, W. P. Testimony of William P. Crowell, Deputy Director, National Security Agency. Washington DC: House Judiciary Committee, Subcommittee on Courts and Intellectual Property, 1997.

Cryptome. Dirty Lantern. JYA, December 18 2001. Accessed December 28 2001. Available from http://cryptome.org/dirty-lantern.htm.

Denning, D. The Future of Cryptography. Georgetown University, Revised January 6 1996. Accessed August 30 2002. Available from http://www.cosc.georgetown.edu/~denning/crypto/Future.html

Denning, D., and Branstad, D. K. A Taxonomy of Key Recovery Encryption Systems. Georgetown University and Trusted Information Systems, 1997.

Denzin, N. K., and Lincoln, Y. S. "Introduction: Entering the Field of Qualitative Research." In Strategies of Qualitative Inquiry, ed. Norman K. Denzin and Yvonna S. Lincoln, 1-34. London: Sage Publications, 1998.

Department of Commerce. Commerce Department Renames Agency "Bureau of Industry and Security". Washington D.C, April 18 2002.

Diffie, W., and Hellman, M. "New Directions in Cryptography." IEEE Transactions on Information Theory, Volume 22, Number 6, 1976, pp. 644-654.

Diffie, W., and Landau, S. Privacy on the line : the politics of wiretapping and encryption. Cambridge, Mass.: MIT Press, 1998.

Dogcow. Evading the Broadcasting Services Amendment (Online Services) Act 1999. 2600 Australia, 1999.

Dosi, G. "Chapter 10 -- The nature of the innovative process." In Technical change and economic theory, ed. Giovanni Dosi, Christopher Freeman, Richard Nelson, Gerald Silverberg, and Luc Soete, 220-237. London: Pinter Publishers, 1988.

Dosi, G., and Orsenigo, L. "Chapter 2 -- Coordination and transformation: an overview of structures, behaviours and change in evolutionary environments." In Technical change and economic theory, ed. Giovanni Dosi, Christopher Freeman, Richard Nelson, Gerald Silverberg, and Luc Soete, 13-37. London: Pinter Publishers, 1988.

Dunn, A. "Of Keys, Decoders and Personal Privacy." The New York Times, October 1 1997.

Eicke, T. In The Matter Of The Regulation of Investigatory Powers Bill And In The Matter Of A Human Rights Audit For Justice And FIPR. March 22 2000.

Electronic Privacy Information Center. Cryptography and Liberty: An International Survey of Encryption Policy. Washington, D.C., 1999.

Electronic Privacy Information Center. Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet. February 1997.

Ellison, C. Cryptography Timeline. Carl Ellison, June 2 1996. Accessed October 13 1998. WWW. Available from http://www.clark.net/pub/cme/html/timeline.html.

EPIC. EPIC Cryptography and Privacy Sourcebook: Primary Documents on U.S. Encryption Policy, the Clipper Chip, the Digital Telephony Proposal and Export Controls. Washington, D.C.: David Banisar (editor), 1994.

Escudero-Pascual, A., and Hosein, I. "The hazards of technology-neutral policy: questioning lawful access to traffic data." Communications of the ACM2003, Accepted for publication October 24 2002.

Fallows, J. "The American Army and the M-16 rifle." In The social shaping of technology, ed. Donald A. MacKenzie and Judy Wajcman, 382-394. Buckingham [England]: Open University Press, 1999.

FIPR. RIP Information Center. Foundation for Information Policy Research, April 16 2001. Accessed September 17 2001. Available from www.fipr.org/rip.

Galliers, B., and Jarvenpaa, S. "Editorial." The Journal of Strategic Information Systems, Volume 11, Number 1, 2002, pp. 1-3.

Galliers, R. D. "Choosing Appropriate Information Systems Research Approaches: A Revised Taxonomy." In Information Systems Research: Contemporary Approaches and Emergent Traditions, ed. H.-E. Nissen, H.K. Klein, and R. Hirshheim, 327-345: Elsevier Science Publishers, 1991.

Garfield, M. J., and Watson, R. T. "Differences in national information infrastructures: the reflection of national cultures." Journal of Strategic Information Systems, Volume 6, Number 4, 1998, pp. 313-337.

Gladman, B. The Regulation of Investigatory Powers Bill -- The Provisions for Government Access to Keys. London: Foundation for Information Policy Research, 2000a.

Gladman, B. The Regulation of Investigatory Powers Bill: Key Revocation, Government Access to Keys and Tipping-Off. Foundation for Information Policy Research, 2000b.

Global Internet Liberty Campaign. Member Letter on Council of Europe Convention on Cyber-Crime Second Protocol. 2002.

Global Internet Liberty Campaign. Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2. December 2000.

Goldberg, I., and Wagner, D. "Randomness and the Netscape Browser: How secu re is the World Wide Web?" Dr. Dobbs Journal, January 1996.

Grint, K., and Woolgar, S. The machine at work : technology, work, and organization. Cambridge, Mass: Polity Press, 1997.

Haas, P. M. "Introduction: Epistemic Communities and International Policy Coordination." International Organization, Volume 46, Number 1, 1992, pp. 1-35.

Hanseth, O., Monteiro, E., and Hatling, M. "Developing information infrastructure: the tension between standardisation and flexibility." Science, Technology and Human Values, Volume 11, Number 4, 1995, pp. 407-426.

Harvey, L. "A Discourse on Ethnography." In Information Systems and Qualitative Research, ed. Allen S. Lee, Jonathan Liebenau, and Janice I. DeGross, 207-224. London: Chapman and Hall, 1997.

Harvey, L. J., and Myers, M. D. "Scholarship and practice: the contribution of ethnographic research methods to bridging the gap." Information Technology & People, Volume 8, Number 3, 1995, pp. 13-27.

Heilbroner, R. L. "Do machines make history?" In Reprinted in Does Technology Drive History? The Dilemma of Technological Determinism (1994), ed. Merrit Roe Smith and Leo Marx, 53-65. London: MIT Press, 1967.

Heilbroner, R. L. "Technology Determinism Revisited." In Does Technology Drive History? The Dilemma of Technological Determinism., ed. Merrit Roe Smith and Leo Marx, 67-77. London: MIT Press, 1994.

Heinz, J. US Strategic Trade: an export control system for the 1990s. Boulder, Colorado: Westview Press, 1991.

Holleyman, R. W. Testimony of Robert W. Holleyman, President, Business Software Alliance On The Export of Software with Encryption Capabilities. Gaithersburg, MD: National Institute of Standards and Technology, 1995.

Hood, C. Explaining Economic Policy Reversals. Buckingham, England: Open University Press, 1994.

Hosein, I. "The Collision of Regulatory Convergence and Divergence: Updating policies of surveillance and Information Technology." The Southern African Journal of Information and Communication, Volume 2, Number 1, 2001, pp. 18-33.

Hosein, I., and Whitley, E. "Developing national strategies for electronic commerce: Learning from the UK's RIP Act." Journal of Strategic Information Systems, Volume 11, Number 1, 2002, pp. 31-58.

Hughes, T. P. "Technological Momentum." In Does Technology Drive History? The Dilemma of Technological Determinism, ed. Merrit Roe Smith and Leo Marx, 101-114. London: MIT Press, 1994.

Janesick, V. J. "The Dance of Qualitative Research Design: Metaphor, Methodolatry, and Meaning." In Strategies of Qualitative Inquiry, ed. Norman K. Denzin and Yvonna S. Lincoln, 35-55. London: Sage Publications, 1998.

Janson, M., Guimaraes, T., Brown, A., and Taillieu, T. "Acquiring expert knowledge on IS function design." In Information Systems and Qualitative Research, ed. Allen S. Lee, Jonathan Liebenau, and Janice I. DeGross, 303-323. Boston: Kluwer Academic Publishers, 1997.

Jones, M. "Structuration Theory." In Rethinking management information systems: an interdisciplinary perspective, ed. Wendy Currie and Robert Galliers, 103-135. Oxford: Oxford University Press, 1999.

Kahn, D. The Codebreakers: The Story of Secret Writing. Revised ed. New York: Scribner, 1996.

Kerckhoffs, A. "La Cryptographie Militaire." Journal des Sciences Militaires, 1883.

Klein, H., and Myers, M. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies In Information Systems." MIS Quarterly, Volume 23, Number 1, 1999, pp. 67-94.

Kling, R. "Social Analyses of Computing: Theoretical Perspectives in Recent Empirical Research." ACM Computing Surveys, Volume 12, Number March, 1980, pp. 61-110.

Latour, B. "Social Theory and the Study of Computerized Work Sites." A paper delivered at the Information technology and changes in organizational work : proceedings of the IFIP WG8.2 Working Conference on Information Technology and Changes in Organizational Work, Cambridge, UK, December 1995.

Latour, B. "Technology is society made durable." In Sociology of Monsters: Essays on Power, Technology, and Domination, ed. John Law, 103-131. London, England: Routledge, 1991.

Latour, B. "When things strike back: A possible contribution of science studies to the social sciences." British Journal of Sociology, Volume 51, Number 1, 2000, pp. 107-124.

Latour, B. Pandora's hope: Essays on the reality of science studies. Cambridge, MA: Harvard University Press, 1999.

Latour, B. Progress or Entanglement? Two models for the long term evolution of human civilisation. Taiwan: Institute for National Policy Research Conference, 1998.

Lau, F. "A Review on the Use of Action Research in Information Systems." In Information Systems and Qualitative Research, ed. Allen S. Lee, Jonathan Liebenau, and Janice I. DeGross, 31-68. Boston: Kluwer Academic Publishers, 1997.

Lee, A. S. "Integrating Positivist and Interpretive Approaches to Organizational Research." Organization Science, Volume 2, Number 4, 1991, pp. 342-365.

Lee, N., and Stenner, P. "Who pays? Can we pay them back?" In Actor Network Theory and After, ed. John Law and John Hassard, 91-112. Keele, UK: Blackwell Publishers/Sociological Review, 1999.

Lessig, L. "The New Chicago School." Journal of Legal Studies, Volume 27, Number June, 1998, pp. 661-691.

Lessig, L. Code : and other laws of cyberspace. New York, N.Y.: Basic Books, 2000.

Lessig, L. The future of ideas : the fate of the commons in a connected world. 1st ed ed. New York: Random House, 2001.

Levin, H. J. "New Technology and the Old Regulation in Radio Spectrum Management." The American Economic Review, Volume 56, Number 1/2, 1966, pp. 339-349.

Levy, S. Crypto: How the Code Rebels Beat the Government Saving Privacy in the Digital Age. New York: Viking Press, 2000.

Lloyd, S., and Oorschot, P. v. Key Recovery Feasibility Study. Entrust Technologies, 1998.

Lundvall, B.-Å. "Chapter 17 -- Innovation as an interactive process: from user-producer interaction to the national system of innovation." In Technical change and economic theory, ed. Giovanni Dosi, Christopher Freeman, Richard Nelson, Gerald Silverberg, and Luc Soete, 349-369. London: Pinter Publishers, 1988.

MacKenzie, D. A., and Wajcman, J. "Introductory Essay." In The social shaping of technology, ed. Donald A. MacKenzie and Judy Wajcman, 3-26. Buckingham [England]: Open University Press, 1999.

Markus, M. L. "The Qualitative Difference in Information Systems Research and Practice." In Information Systems and Qualitative Research, ed. Allen S. Lee, J. Liebenau, and J. I. DeGross, 11-27. London: Chapman & Hall, 1997.

Matenlaers, P. "Acquiring expert knowledge on IS function design." In Information Systems and Qualitative Research, ed. Allen S. Lee, Jonathan Liebenau, and Janice I. DeGross, 324-341. Boston: Kluwer Academic Publishers, 1997.

May, T. The Cyphernomicon: Cypherpunks FAQ and More. 1994, Version 0.666.

Merkle, R. C. "Secure Communication Over Insecure Channels." Communications of the ACM, Volume 21, Number 4, 1978, pp. 294-299.

Mingers, J. "Combining IS Research Methods: Towards a Pluralist Methodology." Information Systems Research, Volume 12, Number 3, 2001a, pp. 240-259.

Mingers, J. The Paucity of Multimethod Research: a Review of the IS Literature. Warwick: Warwick Business School, University of Warwick, 2001b.

Monteiro, E., and Hanseth, O. "Social Shaping of Information Infrastructure: On Being Specific about the Technology." In Information Technology and Changes in Organizational Work, ed. W Orlikowski, G Walsham, M.R. Jones, and J.I. DeGross, 325-343. Cambridge: Chapman & Hall on behalf of the International Federation for Information Processing (IFIP), 1995.

Morse, J. M. "Designing Funded Qualitative Research." In Strategies of Qualitative Inquiry, ed. Norman K. Denzin and Yvonna S. Lincoln, 56-84. London: Sage Publications, 1998.

Myers, M. "Critical Ethnography in Information Systems." In Information Systems and Qualitative Research, ed. Allen S. Lee, Jonathan Liebenau, and Janice I. DeGross, 276-300. London: Chapman and Hall, 1997.

National Research Council, Dam, K. W., W.Y.Smith, Bollinger, L., Caracristi, A., Civiletti, B., Crook, C., Fuller, S., Gelb, L., Graham, R., Hellman, M., Katz, J., Neumann, P., Ozzie, R., Schmults, E., Stone, E., and Ware, W. Cryptography's Role in Securing the Information Society. Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, National Research Council, 1996.

National Security Agency. Potential Opposition Issues. Fort Meade, Maryland: National Security Agency, Undated but prior to 1994.

Nelson, R. R., and Soete, L. L. G. "Chapter 28 -- Policy Conclusions." In Technical change and economic theory, ed. Giovanni Dosi, Christopher Freeman, Richard Nelson, Gerald Silverberg, and Luc Soete, 631-635. London: Pinter Publishers, 1988.

Noll, R. "The Economic Theory of Regulation after a Decade of Deregulation: Discussion piece." In A Reader On Regulation, ed. Robert Baldwin, Colin Scott, and Christopher Hood. Oxford: Oxford University Press, 1998.

NRC. Cryptography's Role in Securing the Information Society Committee to Study National Cryptography Policy, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, National Research Council, ed. Kenneth W. Dam and Herbert S. Lin. Washington, D.C.: National Academy Press, 1996.

NYT Staff. "Secrets Kept and Found." The New York Times, May 28 1998.

Orlikowski, W. "Learning from Notes: organizational issues in groupware implementation." A paper delivered at the Conference on Computer Supported Cooperative Work (CSCW) '92, Toronto, 1992b.

Orlikowski, W. "The duality of technology: Rethinking the Concept of Technology in Organizations." Organization Science, Volume 3, Number 3, 1992a, pp. 398-427.

Orlikowski, W. J., and Baroudi, J. J. "Studying Information Technology in Organizations: Research Approaches and Assumptions." Information Systems Research, Volume 2, Number 1, 1991, pp. 1-27.

Orlikowski, W., and Iacono, C. S. "Research Commentary: Desperately Seeking the "IT" in IT Research -- A Call to Theorizing the IT Artifact." Information Systems Research, Volume 12, Number 2, 2001, pp. 121-134.

OTA. Information Security and Privacy in Network Environments. Washington, D.C.: Office of Technology Assessment, Congress of the United States, 1994, OTA-TCT-606.

Peltzman, S. "The Economic Theory of Regulation after a Decade of Deregulation." In (reprinted) A Reader on Regulation, 1998, ed. Robert Baldwin, Colin Scott, and Christopher Hood. Oxford: Oxford University Press, 1989.

Pettigrew, A. M. "Longitudinal Field Research on Change: Theory and Practice." Organization Science, Volume 1, Number 3, 1990, pp. 267-291.

Politan, N. H. Re: United States v. Nicodemo S. Scarfo, et al. Newark, N.J.: United States District Court, 2001.

Porter, M. E., and van der Claas, L. "Toward a New Conception of the Environment-Competitiveness Relationship." The Journal of Economic Perspectives, Volume 9, Number 4, 1995, pp. 97-118.

Pouloudi, N., and Whitley, E. A. "Representing human and non–human stakeholders: On speaking with authority." In Organizational and social perspectives on information technology, 339-354. Aalborg, Denmark: Kluwer Press, 2000.

Prasad, P. "Systems of Meaning: Ethnography as a Methodology for the Study of Information Technologies." In Information Systems and Qualitative Research, ed. Allen S. Lee, J. Liebenau, and J. I. DeGross, 101-118. London: Chapman & Hall, 1997.

Pressman, A. "Attempt to Design 'Backdoors' Fails." Washington Post, June 26, 1998, 2:17pm 1998.

Privacy International et al. "Letter to the Editor of the Daily Telegraph: Dangerous Bill." Daily Telegraph, July 12 2000.

Regan, P. M. "From Clipper to Carnivore: Balancing Privacy, Law Enforcement and Industry Interests." A paper delivered at the American Political Science Association, San Francisco, CA, August 29-September 2 2001.

Reuters. " FBI confirms 'Magic Lantern' spy project." CNN.com, December 13 2001.
.

Rivest, R., Shamir, A., and Adleman, L. M. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." Communications of the ACM, Volume 21, Number 2, 1978, pp. 120-126.

Rosenberg, N. Inside the black box : technology and economics. Cambridge: Cambridge University Press, 1982.

Rotenberg, M. "What Larry Doesn't Get: Fair Information Practices and the Architecture of Privacy." Stanford Technology Law Review, 2000.

RSA Laboratories. RSA Laboratories Frequently Asked Questions. RSADSI, 1998.

Rubinstein, I. Testimony of Ira Rubinstein, Senior Corporate Attorney, Microsoft Corporation on behalf of the Business Software Alliance: IMMEDIATE NEED FOR EXPORT CONTROL RELIEF FOR SOFTWARE WITH ENCRYPTION CAPABILITIES. Washington DC: House Judiciary Committee, Subcommittee on Courts and Intellectual Property, 1997.

Schneier, B. "Secrecy, Security, and Obscurity." Cryptogram, May 15 2002.

Schneier, B. Applied Cryptography. 2nd ed. New York, NY: Wiley and Sons, 1996.

Schultze, U. "A Confessional Account of an Ethnography About Knowledge Work." MIS Quarterly, Volume 24, Number 1, 2000, pp. 1-39.

Sørensen, C., Whitley, E. A., Madon, S., Hosein, G., Johnstone, J., and Klyachko, D. "Cultivating recalcitrance in information systems research." In Realigning Research and Practice in Information Systems Development: The Social and Organizational Perspective, ed. Nancy L. Russo, Brian Fitzgerald, and Janice I. DeGross, 297-316. Boise, Idaho: Kluwer, 2001.

Sprinz, D., and Vaahtoranta, T. "The Interest-Based Explanation of International Environmental Policy." International Organization, Volume 48, Number 1, 1994, pp. 77-105.

Stake, R. E. "Case Studies." In Strategies of Qualitative Inquiry, ed. Norman K. Denzin and Yvonna S. Lincoln, 86-108. London: Sage Publications, 1998.

Steinbart, P. J., and Nath, R. "Problems and Issues in Management of International Data Communications Networks: The Experiences of American Companies." MIS Quarterly, Volume 16, Number 1, 1992, pp. 55-73.

Stephenson, N. Cryptonomicon: Avon Books, 1999.

Stigler, G. J. "Nobel Lecture: The Process and Progress of Economics." The Journal of Political Economy, Volume 91, Number 4, 1983, pp. 529-545.

Stigler, G. J. Chicago studies in political economy. Chicago: Chicago University Press, 1988.

Stinson, D. Cryptography: theory and practice. Boca Raton, Florida: CRC Press, Inc., 1995.

Strauss, A., and Corbin, J. "Grounded Theory Methodology." In Strategies of Qualitative Inquiry, ed. Norman K. Denzin and Yvonna S. Lincoln, 158-183. London: Sage Publications, 1998.

Straw, J. "Letter to the editor: Bill will not cause e-commerce to decamp." Financial Times, 15th June 2000.

Sullivan, J. "Free Love and Free Speech." Wired News, January 18 1999.

Sun, J.-M., and Pelkmans, J. "Regulatory competition in the single market." In A Reader on Regulation, ed. Robert Baldwin, Colin Scott, and Christopher Hood, 443-467. Oxford: Oxford University Press, 1998.

Thatcher, M. "Explaining Regulation Day 1 Sessions 4 and 5." A paper delivered at the Short Course on Regulation, The London School of Economics and Political Science, 11th-15th September 2000.

The White House. Statement by the Press Secretary. Washington: US Government, April 13 1993.

Trauth, E. M. "Achieving the Research Goal with Qualitative Methods: Lessons learned along the way." In Information Systems and Qualitative Research, ed. Allen S. Lee, Jonathan Liebenau, and Janice I. DeGross, 225-245. Boston: Kluwer Academic Publishers, 1997.

Trauth, E. M., and O'Connor, B. "A Study of the Interaction Between Information Technology and Society: An Illustration of Combined Qualitative Research Methods." In Information Systems Research: Contemporary Approaches and Emergent Traditions, ed. H.-E Nissen, H.K. Klein, and R. Hirscheim, 131-142. North-Holland: Elsevier Science Publishers B.V, 1991.

USACM. Codes, Keys and Conflicts: Issues in US Crypto Policy, ed. Special Panel of the ACM US Public Policy Committee. New York: Association for Computing Machinery, 1994.

van den Belt, H., and Rip, A. "The Nelson-Winter-Dosi model and synthetic dye chemistry." In The Social Construction of Technological Systems, ed. W. Bijker, T. P. Hughes, and T. Pinch, 135-158. Cambridge, Mass: MIT Press, 1987.

Vidgen, R., and McMaster, T. "Black Boxes, Non-Human Stakeholders and the Translation of IT Through Mediation." In Information Technology and Changes in Organizational Work, ed. W Orlikowski, G Walsham, M.R. Jones, and J.I. DeGross, 250-280. Cambridge: Chapman & Hall on behalf of the International Federation for Information Processing (IFIP), 1995.

Walsham, G. "Actor-Network Theory and IS Research: Current Status and Future Prospects." In Information Systems and Qualitative Research, ed. Allen S. Lee, Jonathan Liebenau, and Janice I. DeGross, 466-479. Philadelphia, PA: Chapman & Hall, 1997.

Walsham, G. "Interpretive case studies in IS research: nature and method." European Journal of Information Systems, Volume 4, 1995, pp. 74-81.

Walsham, G. "Organisational metaphors and information systems research." European Journal of Information Systems, Volume 1, Number 2, 1991, pp. 83-94.

Whitley, E. A., and Hosein, I. "Doing politics around electronic commerce: Opposing the Regulation of Investigatory Powers Bill." In Realigning Research and Practice in IS Development: The Social and Organisational Perspective, ed. Nancy Russo, Brian Fitzgerald, and Janice I. DeGross, 415-438. Boise, Idaho: Kluwer, 2001.

Williamson, M. "New star in orbit." IEE Review, September 1999, p.201-205.

Winner, L. Autonomous technology : technics-out-of-control as a theme in political thought. Reprinted in 1992 ed. Cambridge, MA: MIT Press, 1977.

Winner, L. The Whale and the Reactor: A Search for the Limits in an Age of High Technology. Chicago: University of Chicago Press, 1986.

Zmud, R. "Conducting and Publishing Practice-Driven Research." In Information Systems: Current Issues and Future Changes, ed. T.J. Larsen, L. Levine, and J.I. DeGross, 21-33. Laxenburg, Austria: International Federation of Information Processing, 1999.