Cryptography and Democracy : Dilemmas of Freedom

in Liberty eds., *Liberating Cyberspace: Civil Liberties, Human Rights, and the Internet*, London: Pluto Press, 1999, 81-125.

BY

Caspar Bowden, Foundation for Information Policy Research & Yaman Akdeniz, CyberLaw Research Unit, Centre for Criminal Justice Studies, University of Leeds

Please Cite as: Bowden, C., & Akdeniz, Y., "Cryptography and Democracy: Dilemmas of Freedom," in Liberty eds., *Liberating Cyberspace: Civil Liberties, Human Rights, and the Internet*, London: Pluto Press, 1999, 81-125.

1. Introduction

'As we prepare to enter a new century, our society stands on the threshold of a revolution as profound as that brought about by the invention of the printing press half a millennium ago.'[1] The revolution is the creation of a global infrastructure that can transmit voice, video and text in a single inter-operable medium. Confidential messages may be sent without prior arrangement between parties, and public directories used to authenticate authorship with digital signatures that cannot be forged. Digitised intellectual property can be marked by electronic copyright management systems to identify owners or consumers. The ubiquitous new medium could in time become the primary means of mass communication, subsuming the marketing of and payment for general goods and services.

The technologies for protection of confidentiality, digital payment, authentication of identity, and ownership of intellectual property are all based on the science of cryptography. In the past twenty years, a variety of elaborate (but mathematically precise) 'protocols' for cryptographic transactions have been invented with properties that are bewilderingly counter-intuitive. Perhaps because of popularisation of the ULTRA story,[2] there is a common lay assumption that fast computers can crack any code. This is false - the policy dilemmas arise from the brute fact that computers cannot prise open the 'strong' encryption now possible.

While professionals are baffled by contemplation of the social consequences of the interaction of these technologies, public opinion remains almost entirely uninformed about the nature, imminence, or *finality* of the decisions to be made. The finality arises from the inter-penetration of the new medium with every aspect of society. The new communications infrastructure will not be an isolated technology (say like nuclear power) which can be substituted or dispensed with, or a treaty obligation from which a sovereign state can withdraw. Basic technical choices affecting the degree of anonymity and confidentiality possible in mass-market systems, may actually determine (albeit in ways hard to predict) the evolution of democratic political culture.

---

1 'Communicating Britain's Future,' (The Labour Party, 1995).

Policy makers know that the Information Society will be built on these foundations. Governments may attempt to change policy in the future by legislation, but paradigmatic reform may be unenforceable, once a commercial and political grid, supporting an enormous weight of economic activity, is established internationally.

The growth of the information economy will be built on the regulated issue of "digital passports" by '**Certification Authorities**' and '**Trusted Third Parties**' (see below). Market forces will enforce a convergence towards inter-operability of signatures, encryption, electronic cash, and electronic copyright management systems ('ECMS'), that will occur in leaps and bounds as markets for new digital services are established.

The uniform technical standards of the new networks will be intrinsically capable of supporting computer-automated mass-surveillance and traffic-analysis of all digital communications. The potential scope and efficiency of feasible surveillance apparatus is without precedent - conventional techniques are limited by practical constraints. Should the cryptographic infrastructure be designed so that future implementation of mass or even selective surveillance is either possible, or impossible?

Inter-operable electronic copyright, payment, and signature systems could create cradle-to-grave personal audit trails of all transactions, and such information could be used for targeted micro-marketing, credit and insurance, copyright enforcement, and tax/benefit data matching.[3] Can abstract principles of Data Protection provide an effective check on abuse, or should these systems be designed with 'Privacy Enhancing Technologies', which could prevent data integration not authorised by the individual?

Attitudes to these questions often cut across orthodox left/right political allegiances. Cryptography offers the possibility of erecting strong bulwarks to privacy, if we so choose. Although 'Big Brother' has entered the language as a reference point, an unfortunate codicil to Orwell's legacy is the common assumption and a resigned acceptance that the computer abolished privacy long ago.

---

2 The Hut Six Story, Gordon Welchmann.

3 Social Security Administration (Fraud) Bill, London: HMSO, 1996. Under section 1.[116A](4)(b) 'amended or supplemented information' can be fed back to the original department, for purposes other than SS and HB enforcement. Section 2.(2) [116B].(1)(b)) creates secondary powers for data to be requested from any government department.

Who needs Cryptography?

Banks presently use encryption all around the world to process financial transactions. For example, the U.S. Department of the Treasury requires encryption of all U.S. electronic funds transfer messages[4]. Banks also use encryption to protect their customers PIN numbers at bank automated teller machines.

> 'As the economy continues to move away from cash transactions towards "digital cash", both customers and merchants will need the authentication provided by unforgeable digital signatures in order to prevent forgery and transact with confidence.'[5]

The security of electronic commerce is already an important issue for Internet users. Companies selling anything from flowers to books rely on credit card transactions (and increasingly electronic cash) secured by Internet browsers incorporating encryption techniques. However, because of US controls on the strength of encryption software that can be exported, browser versions for non-US use have designedly weak security which can be broken easily. These transactions remain vulnerable not only to isolated attack by hackers, but also to systematic compromise by well-resourced criminal organisations (or intelligence agencies mandated to engage in 'economic intelligence gathering').

Cryptography can also provide anonymity as well as confidentiality, essential for certain special interest groups, and was used on the Web sites of the Critical Path AIDS Project in the USA and the Samaritans in the UK. Internet anonymous remailers allow human rights monitors in repressive regimes to communicate without fear of persecution or reprisals.

2. A Primer on Cryptography

The word cryptography[6] comes from Greek word kryptos which means 'hidden' while graphia stands for 'writing'. Cryptography concerns ways in which the meaning of messages may be concealed so that only certain people can understand them, and

---

4 See Murphy, Gerald, U.S. Dep't of Treasury, Directive: Electronic Funds and Securities Transfer Policy - Message Authentication and Enhanced Security, No. 16-02, section 3 (Dec. 21, 1992).

5 Froomkin, A. Michael, "The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution" [1995] *U. Penn. L. Rev.* 143, 709-897 at page 720.

6 Bruce Schneier, *Applied Cryptography*, (John Wiley, 1996) is an excellent practical introduction to computer implementations.

methods of ensuring that the content of messages remains unaltered.

David Kahn traces the history of cryptography from ancient Egypt to the computer age.[7] During WWII, the first electro-mechanical computers were built for the ULTRA project, which allowed the British to read German communications enciphered with the Enigma machine.[8] They were specially designed to automate the task of exhaustively searching for the correct Enigma settings, assisted by various "cribs" (short-cuts deduced from previous analysis or lapses in security). An organisation was created to decrypt large volumes of intercepted traffic, and distribute the intelligence securely for operational use.

Codes

A **code** is the correspondence of a fixed repertoire of messages to a set of previously agreed symbols. In a computer, the alphabetic, numeric and punctuation characters comprising a message are each assigned a number between zero and 255 according to a conventional code (such as ASCII). A message can thus be represented as **bytes** - groups of eight binary digits (bits - 1s and 0s).[9] The ASCII representation of a message is not encrypted, because the code is well known. Even if a code is secret, it cannot encrypt a message that falls outside the agreed repertoire.

Ciphers

A cipher allows encryption of an *arbitrary* message using a general rule or scheme (algorithm) together with a key, to turn **plaintext** into **ciphertext**. The most secure cipher is the "one-time pad". This uses a random binary number as the key, and the algorithm acts on plaintext by flipping the bits ("exclusive-or") in positions where the one-time pad "key" is 1. Decryption applies the same rule to key and ciphertext, producing plaintext. Without the key, no information can be gleaned about the plaintext. The disadvantage of this method is that it requires a key (which must not be re-used – hence "one-time") as long as the message itself.

More complex ciphers may involve complicated sequences of substitutions and transpositions. In Julius Caesar's substitution cipher each letter of the original message

---

7 See Kahn, David, *The Codebreakers*, (New York: Macmillan Company, 1972).

8 See Kahn, David, *Seizing the Enigma*, (Boston: Houghton Mifflin, 1991).

9 e.g. 'Myrmidon' in ASCII is '01001101 01111001 01110010 01101101 01101001 01100100

is replaced with the letter three places beyond it in the alphabet. Transposition ciphers rearrange the order of characters. In these 'symmetric' ciphers both sender and receiver use the same key to scramble and unscramble the message.

If a key is reused, there is a risk that it may be deduced through statistical analysis of intercepted samples of ciphertext. This is much easier if a **cryptanalyst** ('code-breaker') can arrange for a hapless opponent to encrypt 'chosen plaintext' messages that systematically divulge clues. More elaborate cipher algorithms recycle a conveniently short key, but successively chain the output with the preceding block of ciphertext, to scramble any regularity. Nevertheless, various kinds of mathematical short-cut have been discovered to crack apparently robust algorithms, and ciphers may have certain weak keys or even an intentional back-door which makes cryptanalysis easy.

Ciphers for which the algorithm is known can in principle be broken by a brute-force attack, in which every possible key is tried - if the key is n-bits long, then there are 2^n possible key values. But however fast computers become, quite short keys can generate a number of combinations[10] astronomically beyond their reach. A cipher that cannot be broken by the brute-force or cunning (of a particular adversary) is termed '**strong'**.

Public Key Cryptography

All ciphers seem to suffer from the same drawback. Trusted couriers are needed to deliver keys to those wishing to send encrypted messages to each other. The key cannot be sent over the same channel as the message, because that channel is presumed insecure - otherwise why bother to encrypt? This difficulty is so obvious, and so apparently insurmountable, that when Whitfield Diffie and Martin Hellman solved the key distribution problem in 1976,[11] it completely revolutionised cryptography. Instead of using a single key that could both encrypt and decrypt a message, they proposed a scheme in which every individual has both a **public key** (which can be published in a directory) and a **private key** (which is kept secret).

If Alice wants to send a confidential message to Bob, she looks up Bob in a directory

---

01101111 01101110'.

10 A 128 bit key has 2^{128} = 340282366920938463463374607431768211456 possibilities.

11 W.Diffie & M.E.Hellman, 'New Directions in Cryptography', IEEE Trans.Inf.Th., vIT-22 n.6 Nov 1976.

and encrypts her message with his *public key* contained there, and sends it. When Bob receives the encrypted message, he decrypts it into plaintext with his *private* key. This is bafflingly simple - how is it done? How are the public and private key related? Why can't anyone else just look up Bob's public key as well, and use that to decrypt the (intercepted) message?

The trick is to use a mathematical 'one-way' function: once a message is encrypted with such a function, it cannot be decrypted with the same key used to encrypt. There is however a corresponding key (the private key), which will decrypt the message - but the calculation of the private key from the public key can be made arbitrarily time-consuming by sufficiently lengthening the keys.

This is a completely counter-intuitive notion, understandably alien to common-sense ideas of how codes and ciphers work. Nevertheless it means that completely secure communication can occur between two parties without prior negotiation of a shared secret key.

RSA

The system first used for public key (or **asymmetric**) cryptography is called **RSA** (after the inventors Rivest, Shamir and Adleman)[12] and was developed in 1977.[13] Two very long prime numbers are chosen at random, and these generate (but are not the same as) the public and private keys. It turns out that showing that a certain number is prime (i.e. has no smaller divisors) is much easier than actually finding the factors of a number which is not prime. The cryptanalyst's problem of finding the private key from the public key can be solved by factoring the product of the two primes (without knowing either - which would be trivial). The best known methods would take current computers millions of years for keys several hundred digits long.

If the invention of public key cryptography was indeed so revolutionary, why has it taken twenty years for these issues to come to a head? The reasons are various: the patenting (in the US) of the RSA algorithm, strict US export controls on cryptography

---

12 R.Rivest, A.Shamir and L.Adleman, 'A Method for Obtaining Digital Signatures and Public Key Cryptosystems', Comm. ACM, v.21 n.2, Feb 1978.

13 In fact GCHQ invented both RSA and Diffie-Hellman around 1971, but it was not disclosed until 1997. See 'The History of Non-Secret Encryption', http://www.cesg.gov.uk/storynse/htm.

and the strivings of intelligence agencies to preserve their national security interception capabilities.

Digital Signatures

Public key cryptography can also *authenticate* that a message originates (and has not been altered en route) from a person using a kind of **signature**. To send a signed message, Alice encrypts with *her private* key, before sending to Bob. This time Bob can only decrypt the message using Alice's *public* key (it works this way round as well), which he has to look up in a directory. If Bob can do this, it verifies Alice's signature, because the message must have been sent using her private key (which only she should know).

Note that in this example, anyone else can look up Alice's public key to decrypt the message (and thus verify the signature) as well, so the message is not confidential. A signed and secret message can be sent by layering the encryption protocol for signature inside that for confidentiality, however using the same public/private key-pair for both (only possible with the RSA system) has practical and regulatory disadvantages (see 'Self-certification' below).

Certification Authorities

Although trusted couriers are no longer needed for key delivery, a new type of key distribution problem arises with public key cryptography. If Alice looks up Bob's public key in a directory, how does she know that that key really belongs to Bob? An impostor might have published a phoney public key under Bob's name, hoping either to intercept messages sent to him (if it was a confidentiality key), or convince the unwary to accept forged documents (if it was a signature key).

The solution is for Bob to present his public key to someone who can reputably vouch for his identity – a **Certification Authority** (‘**CA’**) - and get them to (digitally) sign a **key certificate** which can be then be published. Anyone can verify that the public key attached to a certificate can safely be used, by validating the signature of the CA. The public signature key of the CA thus becomes the “gold standard” for routine checking of certificates issued, and may itself be certified in a ‘**hierarchy of trust**’ of ever more unimpeachable authorities. Certificates could equally be signed by (many different) individuals, on the basis of personal acquaintance, in a ‘**web-of-trust**’. However,

vouching for someone's identity is not the same as vouching for their honesty or diligence in performing identifications, so in a web or a hierarchy, a "chain" of certification is only as strong as the weakest link. Note that the private key of the end user is nowhere required or involved in the certification process.

Self-certification

The risks associated with compromise of a private key used for signature are substantially different from those for a key used for message secrecy. A person may therefore have two different pairs of keys (private/public), for separate confidentiality and signature use. In this case, there is actually no need for a CA to be involved in certifying the public key used for encryption. A user may "self-certify" their public encryption key by signing it with their own digital signature. If their signature is trusted (because the signature is certified by a CA and can thus be verified) then their self-signed encryption key should be trustworthy to the same extent.

Revocation

All certificates should be stamped with an expiry date, and new keys must be generated and re-certified before this date to prevent disruption of service. In fact any certification system must provide for the case of a private key becoming compromised, and propogate **revocation** of invalid certificates through the directories used to verify signatures. Should revocation be under the control of the key-owner or the certifier? If certification occurs through a hierarchy of trust, entire branches of the hierarchy could be disabled by revocation of a high-order certificate, which could be regarded either as a vulnerability, or a strategic lever of control. In contrast, a web-of-trust (in which a certificate is validated by multiple signatories) is immunised against single-points of attack or failure. In trust networks, the structure of revocation is a political issue.

Session keys

Software implementations of public key cryptography, involving operations on very large numbers, are relatively slow. Although chips to speed up the necessary mathematical operations are available, software running on today's PCs would take an inconveniently long time to prepare long messages. To get around this, **hybrid** cryptography uses a combination of conventional cipher and public key systems to get the best of both worlds. The idea is to choose a conventional cipher with a key-length resistant to brute-force attack, and encipher with a key *randomly chosen for each message* (a **session key**). The session key (e.g. 128 bits) is then itself encrypted with

public key cryptography (which can be done quickly because the key is much smaller than a typical message), and then attached to the end of the ciphertext. In other words, the receiver's public key is being used as a **key encryption key**. To decrypt the message, the receiver first detaches and then decrypts the session key with her private key, and then uses the session key to decipher the actual (long) message. Although seemingly a gratuitous complication (in an already complicated process) this works well, and allows messages to be encrypted and decrypted quickly, with the full strength and benefits of public key cryptography.

Pretty Good Privacy

In 1992 Phil Zimmerman, a US computer security consultant, created a complete implementation of RSA public key cryptography which could run on most computers, using a strong session key cipher. It allowed users to generate their own public and private keys, maintain a "key-ring" of signed certificates in a web-of-trust, and certify the keys of other users. Any Internet user could now send and receive electronic mail that could not be decrypted (as far as anyone knows) by the most skilled cryptanalysts using the most powerful computers. It was called 'Pretty Good Privacy' ('PGP').[14]

Phil Zimmerman's motive for creating the program was political and not for profit.[15] Zimmerman believes that the intrinsic susceptibility of digital communications to automated mass-surveillance is an unprecedented threat to civil liberties[16] and wishes to provide the public with a secure means of communication. The program has been used by human rights monitors inside countries with repressive political regimes, but also by criminals to conceal evidence.[17]

The disclosure or transfer of cryptographic software to a foreigner is illegal under the US ITAR[18] export regulations. Zimmerman never personally exported PGP, he created it, encouraged its use and distributed it to friends and colleagues, one of whom posted it to an Internet Usenet discussion group.[19] Later, improved and extended versions were

---

14 Philip R. Zimmerman, *The Official PGP User's Guide*, (MIT Press, 1995).

15 The program is now also available as a commercial product (http://www.pgp.com)

16 Philip R. Zimmermann, Testimony to the Subcommittee on Science, Technology, and Space of the US Senate Committee on Commerce, Science, and Transportation, 26 June 1996 <http://www.pgp.com/phil/phil-quotes.cgi>.

17 The Mob gets Wired - Crime Online, Time 23 Sep 1996.

18 See US International Traffic in Arms Regulation, 22 C.F.R. ss 120-130.

19 See Jonathan Wallace & Mark Mangan, *Sex, Laws, and Cyberspace*, (Henry Holt, 1996), page 42.

collaboratively produced by other programmers around the world.[20] Zimmerman was put under investigation, with a grand jury hearing evidence for about 28 months. A campaign was established for his defence, and the civil liberties issues achieved wide publicity on the Internet. After acquiring folk-hero status, the prosecution was finally dropped[21] by the Federal Government in January 1996 without explanation. These disputes are now moot, and PGP has become an international de facto standard for Internet public key cryptography. In 1997, the source program of the latest version was published in the form of a book, constitutionally protected under the First Amendment. The book was then scanned outside the US, and the program re-compiled, which allowed distribution of a free version on the Internet, and a "shrink-wrap" version for commercial use.

US Clipper Chip Proposals

In 1993, the Clinton administration announced the **Clipper** chip initiative (which is also known as the Escrowed Encryption Standard - '**EES'**). In response to concerns expressed by law enforcement and national security bodies that uncontrolled use of strong encryption for voice telephony and computer data could threaten the ability to intercept and monitor communications, the plan called for the incorporation of a hardware encryption chip into every telephone, fax machine, modem and computer (the chips for the latter actually called **Capstone**/**Fortezza**, although based on the same technology).

The concept was that a copy of the individual cipher key embedded in a tamper-proof chip (manufactured under government license), would be held in a database by a new independent judicial '**escrow**' agency[22] (a legal term for an honest broker), which would release the key copy to law enforcement agencies on presentation of a valid warrant. This would then enable decryption of intercepted traffic generated by the device containing the chip.

The encryption algorithm (**Skipjack**), designed by the National Security Agency, was to

---

20 Ståle Schumacher, The International PGP Home Page, <http://www.pgpi.com/>

21 See the CDT Policy Post Number 34, January 12, 1996 at http://www.cdt.org. See also [1996] *CUD* 8, 5 at <http://www.soci.niu.edu/~cudigest>.

22 The two government agencies, the National Institute of Standards and Technology ('NIST') and the Department of Treasury, would each hold half of the encryption key.

remain secret,[23] which raised concerns that it might contain an intentional or unintentional 'back-door' that could be exploited by government or others to achieve unauthorised decryption. The history of cryptography contains several examples of algorithms that were believed to be strong for many years, before finally yielding to attacks from academic cryptanalysts (e.g. the 'Knapsack' system of Diffie-Merkle-Hellman).

The policy was severely criticised on civil liberties, technical, and economic grounds.[24] There was a general objection that a future government might engage in 'Big Brother' mass-surveillance, a technical flaw was discovered in the design which could enable circumvention of escrow (i.e. communication could take place which the escrowed key could not decrypt), and industry objected that Clipper products would be unsaleable abroad.

The US Government in December 1995 presented a revised version of their Clipper Chip proposal which introduced the notion of key escrow achieved through software[25]. This idea was expanded in May 1996, in the document '*Achieving Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure.*'[26] A new "public key infrastructure" (**PKI**) would enable users of encryption clearly to identify the people they communicate with, and export restrictions would be lifted on cryptographic software which 'properly escrowed' confidentiality keys with an approved agent[27], where the underlying cipher system employs keys of no more than 56-bits. This is a 'belt-and-braces' approach, since it is generally believed that specially designed cipher-cracking computers, which may be available to governments (or other large organisations), can crack 56-bit ciphers in days.[28]

---

23 The original Clipper project is now defunct, and the SKIPJACK algorithm has recently been published (http://csrc.nist.gov/encryption/skipjack-kea.htm).

24 See generally Schneier, B., & Banisar, D., *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*, New York: John Wiley & Sons, 1997.

25 See Center for Democracy and Technology, 'Clinton Administration Continues to Push For Flawed Crypto Export Policy' from the Clipper II Archives at <http://www.cdt.org>

26 See the proposal at <http://www.epic.org/crypto/key_escrow/white_paper.html>

27 See the CDT Preliminary Analysis of 'Clipper III' Encryption Proposal, May 21, 1996 at <http://www.cdt.org>. See also Senator Conrad Burn's Response to the proposal, 'Burns: Clipper III Strikes Out' at <http://www.epic.org/crypto/key_escrow/burns_on_white_paper.html>.

28 The weakness of DES, a standard 56-bit commercial cipher, was recently demonstrated when hardware costing $250,000 cracked it in 3 days. See Electronic Frontier Foundation,: "EFF Builds DES Cracker that proves that Data Encryption Standard is insecure," July 17, 1998, at http://www.eff.org/descracker.html. See also EFF, *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*, (California: O'Reilly & Associates), July 1998.

Finding a foreign market for encryption products with key escrow under US control will be difficult, whatever the length of keys.[29] Political and commercial organisations might reasonably believe that US authorities would intercept their communications.[30]

Trusted Third Party

The term 'Trusted Third Party' is unfortunately ambiguous. It originally meant merely a Certification Authority (which has no technical or commercial need to escrow private keys) however the term is now usually synonymous with software escrow**,** for the simple reason it is a mandatory requirement of government proposals for regulation of TTPs.[31]

The role of a TTP/CA is to provide (for a fee) a certificate that authenticates (on the authority of the TTP organisation) that a public encryption key or a public digital signature key actually belongs to the named owner. TTPs can function as "escrow" agencies, by insisting that the private decryption key is surrendered to (or generated by) the TTP, and held in a database for safe-keeping. If a key-owner loses her private key, she can apply for a replacement copy from the TTP. A law enforcement agency could also apply for a copy of the private key with a judicial warrant, without the knowledge of the key owner.

Financial and legal institutions, telecommunications companies, Internet content vendors, and network service providers could all act as TTPs, although there is little consensus about how many a regulated market could support, the tariff structure, or the degree of vertical integration and conflict of interest which should be permitted. The Data Protection Registrar's Twelfth Annual Report stated that there are several problems to be resolved before setting up a TTP system:

> 'Who would supervise it; who would the TTPs be; what products be used; how could you stop users from bypassing the system ..... would a TTP be able to offer services on a European or even a global basis ?'[32]

---

29 Leonard Doyle, 'Spooks All Set to Hack it on the Superhighway' *Independent*, May 2, 1994 reports that: 'The US plan for a Clipper Chip has raised fears among European businesses that sensitive information would no longer be secret if it were vetted by the CIA or the FBI.'

30 Michael Froomkin, 'The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution', at 817.

31 Paper On Regulatory Intent Concerning Use Of Encryption On Public Networks, DTI, June 10 1996, <http://dtiinfo1.dti.gov.uk/cii/encrypt/>.

32 Data Protection Registrar, Twelfth Annual Report, H.C. 574, June 1996, London: HMSO, page 52.

Two Kinds Of Trust

The meaning of 'trust' is radically different for a CA and an escrowing TTP. The CA must take appropriate care before certifying identity, to guarantee that only the named key holder can decrypt messages (in the case of confidentiality keys), or that the key holder has signed a document (in the case of signature keys). Thus the legal liability of a CA can be controlled by a clear statement of the reliance to be placed on its procedures for ascertaining identity, and its demonstrable conformance to those procedures. The key holder's privacy is never at risk. In contrast, if a TTP holds private confidentiality keys, immeasurable damage can be caused to the key owner – privacy can be compromised.

The provision of certified keys for confidentiality and digital signatures are separable problems - indeed there is a compelling reason why they should be accomplished separately under any putative escrow regime. If a government were able to obtain access to a private key used for signatures, documents and transactions purportedly originating from the key owner could be forged. There is general agreement that this possibility would fatally discredit judicial and public confidence in digital signatures.[33]

Key Recovery

If messages are sent outside the jurisdiction covering the TTP, a foreign territory must apply for 'extradition' of an escrowed key. This may make either side uncomfortable. Schemes have been proposed allowing **recovery** of the plaintext of individual messages without escrow, by attaching a Law Enforcement Access Field ("LEAF" - effectively the session key encrypted under a recovery agent's public key), but these do not address civil liberties concerns any better, and are difficult to make tamper-proof in software.

"Royal Holloway" TTP

If however there is a TTP in each jurisdiction, then keys can be recovered without the involvement of foreign jurisprudence. However, this requires both TTPs to remain 'synchronised', with identical databases of escrowed keys, which would involve frequent updating (as keys change), over an ultra-secure channel.

---

[33] 'On Solutions to the Key Escrow Problem', Mark P Hoyle and Chris J Mitchell, Information Security Group, Royal Holloway Univ. London (pre-print).

Cryptologists at Royal Holloway College (“**RHC”**) have proposed a TTP design[34] which obviates this awkward operational requirement. Instead of keeping an escrow database of (randomly generated) individual keys, the two RHC TTPs employ a *single* ‘shared secret key’ (like a master-key) and a ‘key-generating function’, from which each user’s individual keys are generated (taking the key-holder’s name as parameter). There is therefore no need to keep an escrow database at all, and thus no synchronisation problem. If a private key needs to be recovered, it can be regenerated at will by either TTP. Provided only the two TTPs know the secret master-key, this arrangement is as secure as maintaining a groaning database full of individual keys.

This cuts both ways however. If there is concern that keys might leak (to intelligence agencies, corporate spies or criminals), the shared secret key is a jackpot (which would fit on the back of a lottery ticket), allowing decryption of all traffic between all patrons of that pair of TTPs. Perhaps the inconvenience of dual escrow databases is to be preferred.

The RHC system has been adopted as the basis for the ‘Cloud Cover’ scheme advocated by CESG (the Communications Electronics Security Group – the ‘defence’ division of GCHQ) for the protection of UK Government communications. The scheme has been severely criticised[35] for its signature-key escrow design (which could permit centralised alteration of official document records) and its rigidly hierarchical approach to key distribution (making major departmental re-organisation very costly). CESG has been inviting private companies to produce implementations of Cloud Cover “on spec,” with a view to their wider use in quasi-government organisations (without offering explicit guarantees about its official adoption).

Key-splitting

It is possible to divide the escrow of keys between more than one TTP. This provides some security against the malfeasance of a single individual or agency. It is also possible to produce split keys with any desired degree of redundancy, so that possession of a threshold number of fragments permits reconstruction of the entire key.

---

34 C.J.Mitchell, ‘The Royal Holloway TTP-based key escrow scheme’, Information Security Technical Report, Vol.1 No.1, Elsevier/Zergo, ftp.dcs.rhbnc.ac.uk /pub/Chris.Mitchell istr_a2.ps

35 The GCHQ Protocol and its Problems, Ross Anderson and Michael Rowe, Cambridge Computer Laboratory (<http://www.cl.cam.ac.uk/users/mrr/casm/casm.html>)

3. Surveillance, Anonymity, and Traffic Analysis

> *'There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug into your wire whenever they wanted to. You had to live - did live, from habit that became instinct - in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinised.'*[36]

What use is a morass of raw digital intercepts? Why should anyone believe that a government could marshall the resources for their analysis, or that the products of that analysis could be useful?

Traffic Analysis

Traffic analysis refers to the study of the who-is-talking-to-whom, rather than what-they-are-saying. By analysing call-signs, frequencies, flurries of activity, military signals intelligence ('SIGINT') can deduce a great deal about order of battle and movements, without any ability to decipher message content. Civil law enforcement also relies on traffic analysis, for example to trace a drug-dealer's contacts (and their contacts) from a telephone log.[37] Computerised analysis of traffic associations is a potent weapon in the law-enforcement armoury, but is prejudicial to civil liberties unless carefully targeted.

Mass Surveillance

> *'Mass surveillance is the surveillance of groups of people, usually large groups. In general, the reason for investigation or monitoring is to identify individuals who belong to some particular class of interest to the surveillance organizations.'*[38]

The public key infrastructure will tag every message and transaction with a digital signature. Specialised programs for investigating relationships latent in large volumes of

---

36 George Orwell, 'Nineteen Eighty-Four', (Secker & Warburg, 1949). The FSB (successors to the KGB) have proposed that all Internet Service Providers in Russia install high-capacity tapping lines from their equipment direct to a monitoring centre, allowing immediate access to all Internet traffic of subscribers. See Meek, J., "Big Brother is kind enough to collect - and read - your e-mail for you," *The Sydney Morning Herald*, July 25, 1998.

37 The Sci Files, BBC2 transmitted 3rd March 1997.

38 Roger A. Clarke, 'Information Technology and Dataveillance', in Computerization and Controversy: Value Conflicts and Social Choices, ed. Charles Dunlop and Rob Kling (San Diego, CA: Academic Press, Inc., 1991), pg. 498.

unstructured text are already widely used by intelligence agencies.[39] Should any government ever have the possibility of trawling through and automatically analysing the 'national telephone log' of the Superhighway?

Computer Profiling

> *'This technique [computer profiling] is used primarily for law enforcement purposes to locate potential violators when there is a general idea about the characteristics of offending behaviour, but no precise information on the violators....Profiling involves the correlation of information to determine how closely persons or events fit previously determined violation prototypes. Statistical selection methods and inductive logic are used to determine indicators of behaviour patterns related to the occurrence of a certain activity (e.g., persons most likely to under-report taxable income or persons most likely to engage in illegal drug activity).'*[40]

This is a powerful shortcut to compiling a list of suspects - profiling can be combined with traffic analysis and ad-hoc rules ('heuristics') to list individuals deemed suspicious by association, without any capability for decrypting intercepted messages.

Personal Surveillance

> *'Personal surveillance is the surveillance of an identified person. In general, a specific reason exists for the investigation or monitoring.'*[41]

Heuristic profiling could be the basis for selecting *which* subjects were promising targets, and constitute prima facie evidence for a key-recovery warrant to be granted.

Anonymous Mail

Internet privacy activists have developed experimental anonymous remailer programs which circumvent traffic analysis. An anonymous remailer is simply a computer service that forwards e-mails or files to other addresses over the Internet. But the remailer also strips off the 'header' part of the message, which shows where it came from and who sent it. All a traffic analyst can tell is that the sender has sent a message to a remailer, and that (perhaps another) remailer has sent a message to someone else. Sender and receiver cannot be connected (assuming a reasonable throughput of messages).

---

39 See <http://www.ptizan.com.au/memex-tx.html>.

40 Office of Information and Privacy Commissioner/Ontario. 'An Overview of Computer Matching, Its Privacy Implications, and the Regulatory Schemes of Select Jurisdictions.' Government Information Quarterly. Vol. 9, Number 1; 1992; pg. 38.

41 Roger A. Clarke, 'Information Technology and Dataveillance', in Computerization and Controversy: Value Conflicts and Social Choices, ed. Charles Dunlop and Rob Kling (San Diego, CA: Academic Press, Inc., 1991), pg. 498.

The most untraceable implementations (e.g. MixMaster)[42] use public key cryptography to chain together several remailers, which allows unprecedented anonymity both to groups who wish to communicate in complete privacy[43] and to "whistle-blowers" who have reason to fear persecution if their identity became known.[44] According to Raymond Wacks, 'it facilitates participation in the political process which an individual may otherwise wish to spurn.'[45]

One of the best-known anonymous remailers on the Internet ('anon.penet.fi') run for more than three years by Johann Helsingius was closed in August 1996 following allegations by the UK Observer newspaper that it contributed to the distribution of child pornography.[46] Among its users were Amnesty International, and the Samaritans. West Mercia Police also used it as the basis of their 'Crimestoppers' scheme.[47] Contrary to the newspaper's allegations, the sending of pictures through the remailer had been disabled for two years.[48]

In the US, the Supreme Court[49] recently stated that 'an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment' and 'the anonymity of an author is not ordinarily a sufficient reason to exclude her work product from the protections of the First Amendment.'

Anonymity is important both to free speech and privacy.[50] A public key infrastructure

---

42 Lance Cottrel, Mixmaster FAQ, <http://www.obscura.com/~loki/remailer/mixmaster-faq.html>.

43 Froomkin, 'The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution', at 818.

44 See the written evidence submitted by the Christian Action Research and Education (CARE) to the House of Lords, Select Committee on Science and Technology, 'Information Society: Agenda for Action in the UK', Session 1995-96, 5th Report, London: HMSO, 31 March 1996, page 187.

45 Raymond Wacks, 'Privacy in Cyberspace' presented at the Society of Public Teachers of Law (SPTL) Seminars for 1996 - Pressing Problems in the Law: Privacy, 29 June 1996.

46 Another reason was a Finnish court's recent decision in favour of the Scientologists that Helsingus had to provide some of the users' names. See for more information and the full press release on <http://www.penet.fi/>

47 See 'Dirty Anoraks 2' from *Private Eye*, 20 September 1996, No. 907, at page 6.

48 *ibid.*

49 *McIntyre v. Ohio Elections Commission* 115 S.Ct. 1511, (1995).

50 See the ACLU challenge in *ACLU v Miller* to a Georgia law restricting free speech on the Internet. ACLU and others successfully argued that the law is unconstitutionally vague and overbroad because it bars online users from using pseudonyms or communicating anonymously over the Internet. See the ACLU web site for more details at <http://www.aclu.org>.

would identify the nominal source and destination of messages. The Internet Watch Foundation (formerly known as Safety-Net),[51] recently endorsed by the UK Government, sees anonymity on the Internet as a danger, stating:

> '... [A]nonymous servers that operate in the UK [should] record details of identity and make this available to the Police, when needed, under Section 28 (3) of the Data Protection Act (which deals with the disclosure of information for the purpose of prevention of crime).'[52]

A key aspect of the Safety-Net approach is that users take responsibility for material they post on the Internet; that it is important to be able to trace the originators of child pornography and other illegal material. But on the other hand, groups such as the Critical Path AIDS Project, the Samaritans, and Stop Prisoner Rape depend on anonymity for the avoidance of social stigma. Dissident political movements may also need to access and supply sensitive information without risking identification.

Privacy Enhancing Technologies

Absolute anonymity may create unacceptable possibilities for criminal abuse for some types of transaction (e.g. e-cash ransom payments); on the other hand, universal traceability of all messages creates 'Big Brother' traffic analysis risks, even if the content of messages is encrypted. 'Privacy Enhancing Technologies' may provide a combination of last-resort traceability, whilst protecting against intrusive traffic analysis. In many cases, the identity of a data subject need not be known at all (except when suspected of crime), or only by a restricted number of people, but information from different records belonging to the same individual needs to be matched - for example medical records passing through a number of hands in the course of treatment. In these cases an alias or pseudonym can be used. The pseudonym is bound to the true identity through an 'identity protector', with access cryptographically limited to those with proper authorisation.

---

[51] Safety-Net, supported by the UK Government was announced on September 23, 1996. Safety-Net has an e-mail, telephone and fax hot-line from October 1, 1996 and online users will be able to report materials related to child pornography and other obscene materials. See the Safety-Net proposal, 'Rating, Reporting, Responsibility, For Child Pornography & Illegal Material on the Internet' adopted and recommended by the Executive Committee of ISPA - Internet Services Providers Association, LINX - London Internet Exchange and The Internet Watch Foundation at <http://dtiinfo1.dti.gov.uk/safety-net/r3.htm.>

[52] Safety-Net proposal 1996, para 30.

4. Civil Liberties

Since the Clipper initiative, there has been vigorous debate on escrow in the US by non-governmental organisations such as Computer Professionals for Social Responsibility (‘**CPSR’**), the Electronic Frontier Foundation (‘**EFF’**), and the Electronic Privacy Information Centre (‘**EPIC’**). Although most of the Internet community are by now to some degree aware of the issues (for example via campaign banners on many World Wide Web pages), there is scant understanding of these issues amongst the general public, especially outside the US. The general position of non-governmental organisations has been to oppose escrow. It should be noted that Cyber-Rights & Cyber-Liberties (UK) has lead opposition to the UK government’s TTP escrow proposals since its announcement and its response to the DTI consultation paper was endorsed by 15 organisations including the CPSR, EFF and the American Civil Liberties Union.[53]

Chilling Effects

Most people would accept the need for democratic governments to intercept communications on a limited scale, for detection and investigation of crime, and for ‘defence of the realm’. According to the FBI, wiretapping is crucial to effective law enforcement:

> ‘If the FBI and local police were to loose the ability to tap telephones because of the widespread use of strong-cryptography, the country would be unable to protect itself against terrorism, violent crime, foreign threats, drug trafficking, espionage, kidnapping, and other crimes.’[54]

Without this capability, governments would be less able to protect the safety of the public, and this in itself would constitute an infringement of civil liberties. The question is not whether any such interception is wrong, but whether it is safe to entrust all future governments in perpetuity with an unprecedented technical capability for mass surveillance. The state strategy seems naive as it assumes that criminals will use encryption tools that can be decrypted by law enforcement bodies. But government capabilities for automated (and archived) large-scale surveillance could have a chilling effect on the private expression of political opinions by the law-abiding. Although the Internet community is presently a politically negligible minority, as the convergence of

---

[53] See Ashley Craddock, ‘Rights Groups Denounce UK Crypto Paper,’ Wired News, 30 May 1997, at <http://www.wired.com/news/politics/story/4175.html>.

electronic media proceeds, there are plausible scenarios for serious and cumulative erosion of the democratic process. It is a 'sea-change' in the relationship of the citizen to the state.

The Slippery Slope

> *''Domestic espionage is the hidden underside of political history. It may be immensely important. It is possible that without it we would be a very different country from what we are today. We might have a different religion, a different queen, or a different political system. We might be a satellite of a French or German or Russian empire. We could even have a Labour government.'*[55]

The case for stringent technical limits on surveillance is essentially a 'slippery slope' argument. In one sense, this argument is not new: civil liberties campaigners have always argued that interception of mail and telephone communications carries a risk of escalating abuse. However the scale of such interception is intrinsically limited: the bureaucracy and expense of opening letters and transcribing conversations, ensures that any abuse can only occur on a small scale. Large-scale domestic surveillance has hitherto been impractical.In contrast, the ECHELON[56] system can trawl digital communications secretly, centrally, to an increasing degree automatically, at feasible operational cost[57]. The present coverage of ECHELON is unknown, but the EU and US have harmonised arrangements for direct government access to public telecommunications networks.[58]

David Herson, the ex-GCHQ official from DGXIII of the European Commission, with responsibility for piloting TTP systems to create standards for 'European Trusted Services' ('**ETS'**), expresses 'justifiable and implicit faith in the reasonable behaviour of the law enforcement and national security authorities' in democratic societies.[59] Further, according to Herson, 'occasional lapses….will…eventually come to light'. However these remarks sit uneasily with his remarkably candid view of policy motivations, given in an unofficial interview: 'Law enforcement is a protective shield for all the other

---

54 FBI Director Louis Freeh, Address at the Executives' Club of Chicago, Feb. 17, 1994, at13.

55 Bernard Porter, *Plots and Paranoia: A history of political espionage in Britain 1790-1988*, (Unwin, 1989).

56 See European Parliament Scientific And Technological Options Assessment ("STOA") Report, "An Appraisal of the Technologies of Political Control: A consultation document," (PE 166 499/Final), 6 January 1998, written by Wright, S., (Omega Foundation, Manchester). An online copy is available at http://jya.com/stoa-atpc.htm.

57 Nicky Hager, *Secret Power*, , New Zealand: Craig Potton Publishing, 1996.

58 Resolution of the Council of the European Union, 17 January 1995, published 4 November 1996 (C 329/1-6) in the Official Journal of the European Communities.

59 David Herson, European Commission DGXIII, 'Ethical TTPs - a New Security Approach', Information Security Technical Report, Vol.1 No.1, Elsevier/Zergo.

governmental activities…we are talking about foreign intelligence…Law enforcement is a smoke screen.'[60]

Security authorities argue that flexible options for large-scale surveillance are needed for intelligence-led operations to counter organised crime, or proliferation of weapons of mass destruction. But if the design of the new communications infrastructure is predicated on an absolute capability to counter such threats, the resulting apparatus is indistinguishable from that required to anticipate, subvert, and neutralise political dissent. Economic upheaval and social unrest, shocking terrorist incidents, or national emergency could progressively or suddenly widen the use of such capabilities, either with Parliamentary consent or covertly authorised under Crown Prerogative. At what point does the qualitative efficiency of surveillance invalidate the democratic legitimacy it is used to protect?

Therefore the crux of the argument is that the *new* 'slippery slope' is not only much *steeper* (because analysis of digital intercepts can be automated), but it does not '*flatten out*', in fact there would actually be economies of scale with increasing coverage. Whether this is perceived as a categorical difference, or one of degree, will sharply affect opinions about whether procedural and legal safeguards are adequate to prevent abuse in the indefinite future, or whether the infrastructure itself should be designed to be technically incapable of mass-monitoring.

Are there alternatives to escrow?

Is it possible to design an infrastructure that only has the **technical** capacity for surveillance on a limited scale, comparable with present arrangements? If not, should we simply accept the introduction of surveillance architecture as necessary, and trust that democratic continuity will never allow its abuse? What are the precise risks, technical and political, in doing so? If technical safeguards cannot be found, but granting governments a mass-surveillance capability is deemed too dangerous, can and should judicial and law-enforcement procedures be revised to compensate for loss of existing means of interception? Alternatives to escrow might include:

---

[60] David Herson - Head of SOGIS, Senior Officers' Group on Information Security (EU) : Interview in Paris, September 25, 1996, Kurt Westh Nielsen (Engineering Weekly) and Jérôme Thorel (<http://www.cs.berkeley.edu/~daw/GCHQ/herson.htm>)

- Covert installation of software or hardware bugging devices in a suspect's computer which capture passwords and keys – such technologies will in any case be needed to intercept Mafia and terrorist communications that are not key-escrowed, and for military "InfoWar" purposes.
- making failure to comply with a judicial decryption warrant (requiring disclosure of a private key) a specific offence.
- legal admissibility of intercepted communications as evidence in court proceedings, already widely used in the US. Currently intercepts can only be used for intelligence purposes in the UK.

This combination of measures could be reasonably effective, and formulated with civil liberties safeguards, but could not be abused to achieve large-scale surveillance.

6. Would Escrow Work?

Steganography

The concept of randomness is subtly connected with cryptography. When analog signals (e.g. sound samples, photographs) are converted to a digital code, the numbers representing the properties of the real world contain a degree of '*noise*' (imprecision about the particular loudness, pitch, shade of colour) which is random. Without a key to make sense of it, an encrypted message also 'looks' like a random number or noise. This means that it is possible to camouflage an encrypted message by distributing it in the noise of the digital representation of a sound or picture.

This technique of camouflage is known as **steganography,**[61] and it means that a hidden message can be concealed in any digital data that contains noise. The consequence is that escrow of encryption keys can be circumvented by sending sound, pictures or video, with a hidden message sprinkled into the noisy cracks created by digitisation. Done properly, this cannot be detected or proven.[62]

---

[61] Johannes Trimethius (Abbot of Sponheim), Steganographia. See also Information Hiding, First International Workshop Cambridge UK May/June 1996, ed. Ross Anderson, Springer Lecture Notes in Computer Science 1174.

[62] See also "The Steganographic File System" for stored data, in which the existence of a particular file cannot be proven unless both the filename and password are known

The policy implication for law enforcement is that serious "bad hats" will escape any escrow net. Escrow cannot be justified on the grounds that it will enable interception of the internal communications of the Mafia, or professional terrorists. Any competent and well-funded organisation can easily establish secure, hidden channels.

Both pro- and anti-escrow advocates recognise that circumvention of any escrow regime is technically possible, and will become easier as strong encryption tools inevitably proliferate. Nothing can technically prevent data being encrypted again an unescrowed key, concealed with steganography, and sent via anonymous remailers.

Advocates of escrow point out that even if Mafia and terrorist organisations are able to circumvent escrow in their internal communications, they must still communicate externally with law-abiding organisations. However, the permanent records and co-operation of legitimate organisations are already available to investigators – the argument is about whether near **real-time** traffic-analysis/interception/decryption is justifiable, given the dangers for civil liberties. Both sides agree what is important is whether the majority of communication systems become escrowed, and (remarkably) foresee a similar conclusion: if the most important criminals will escape the escrow net, then eventually a ban on unescrowed strong encryption must follow. Official statements[63] support this reasoning.

A Strategically Destabilising Initiative ?[64]

> *'….no administration can bind future administrations, and Congress can change a law at any time. More importantly, widespread acceptance of escrowed encryption, even if voluntary, would put into place an infrastructure that would support such a policy change. Thus, the possibility that a future administration and/or Congress might support prohibitions on unescrowed encryption cannot be dismissed'*[65]

(http://www.cl.cam.ac.uk/ftp/users/rja14/sfs3.ps.gz)

63 'Technical solutions, such as they are, will only work if they are incorporated into all encryption products. To ensure that this occurs, legislation mandating the use of Government-approved encryption products or adherence to Government encryption criteria is required.' See 'Encryption: The Threat, Applications and Potential Solutions' FBI briefing document to National Security Council, February 1993 (obtained by EPIC under FOI).

64 'Empirical testing against small-scale threats is a testing scenario more similar to defending the US against Soviet retaliation after a largely successful American first strike than it is to defending against a Soviet first strike'.Herbert Lin, Software for Ballistic Missile Defence, p.68, Centre for International Studies, MIT 1985.

65 Kenneth Dam and Herbert Lin (ed.), 'Cryptography's Role in Securing the Information Society', National Research Council, Washington, D.C. 1996 (<http://www.replay.com/mirror/nrc/>).

With an escrow infrastructure in place, compliance with a ban on unauthorised double-encryption could at least be partially enforced by the deterrent effect of random sampling, to see if decryption with escrowed keys produced plaintext (this process could be automated). Although steganography could circumvent a ban (unless transmission of all material not susceptible to unambiguous interpretation – e.g. poetry, painting, and journals of the *Society for the Exchange of Random Numbers* – were also banned) this logical absurdity has not inhibited at least one Western European government from banning unauthorised encryption.[66]

Inter-operability

If TTPs or CAs are licensed, the exact specification of the protocols permitted will determine whether the ultimate infrastructure leans toward facilitation of surveillance, or protection of privacy. A huge range exists between, on the one hand Certification Authorities that only serve to authenticate digital signatures and encryption keys, and at the other extreme 'single-master-key' (**'RHC'**) escrow TTPs. The jurisdictional problems presented by international access to escrowed keys also add immense complications. If escrow is to work, standards must be created for sharing directories, excluding or barring access to non-escrowed certificates, and searching and linking directories on a global scale.[67] Law enforcement and intelligence agencies will advocate rigid controls to maximise their operational capability. Civil libertarians will argue against any escrow, or many safeguards for access, to ensure that abuse is difficult, isolated, and hard to conceal.

Electronic Warrants

The DTI envisages a system of electronic warrants to authorise lawful access. The warrant would be e-mailed to the desk of a Secretary of State, approved with a digital signature, and forwarded to the correct Trusted Third Party via a 'central repository' (see DTI Proposals below). The TTP must respond with the key within one hour to meet its licensing obligations (insufficient time to challenge a warrant in court). GCHQ presently intercepts under non-specific warrants,[68] which permit unlimited trawling of

---

66 "loi 90-1170 du 29 Decembre 1990": export or use of encryption equipment must be previously declared when used only for authentication, and previously authorised by the Prime Minister in all other cases, with penalties of fines of up to 500 000F and three months in jail.

67 Internet Engineering Task Force, Architecture for Public-Key Infrastructure Working Group, Draft Nov 1996, pki-tg@opengroup.org

68 Intelligence Services Act 1994, Section 5.

foreign communications.[69] Domestic communications may also be intercepted in support of the security and intelligence services. Warranted interception with technical safeguards to prevent abuse including key-splitting, time-bounding, and technically robust audit trails on escrow access might preclude real-time interception, and may therefore be resisted by intelligence and law-enforcement agencies.

Costs and Risks

In May 1997, a group of independent experts released a report that examined the risks and implications of government proposals for key-recovery systems. The authors of the report are recognised authorities in the fields of cryptography and computer security, including Ross Anderson, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, and Bruce Schneier. The report, entitled '*The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption,*'[70] cautions that 'the deployment of a general key-recovery-based encryption infrastructure to meet law enforcement's stated requirements will result in substantial sacrifices in security and cost to the end user. Building a secure infrastructure of the breathtaking scale and complexity demanded by these requirements is far beyond the experience and current competency of the field.'

Drawing a sharp distinction between government requirements for key recovery and the types of recovery systems users want, the report found that government key recovery systems will produce:[71]

- **New Vulnerabilities And Risks** - Key recovery systems make encryption systems less secure by 'adding a new and vulnerable path to the unauthorised recovery of data' where one need never exist. Such backdoor paths remove the guaranteed security of encryption systems and create new 'high-value targets' for attack in key recovery centres.
- **New Complexities** - Key recovery will require a vast infrastructure of recovery

---

69 See Nick Taylor and Clive Walker, "Bugs in the System," [1996] *Journal of Civil Liberties* 2, 105-124 at 112.

70 See the updated version of A report by an Ad Hoc Group of Cryptographers and Computer Scientists, *The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*, CDT Digital Issues No:3, Washington, June 1998, at http://www.cdt.org/crypto/risks98 .

71 See for a summary of the 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' Report in Centre for Democracy and Technology Policy Post, Vol 3 (6), May 21, 1997, at <http://www.cdt.org/>.

agents and government oversight bodies to manage access to the billions of keys that must be recoverable. 'The field of cryptography has no experience in deploying secure systems of this scope and complexity.'

- **New Costs** - Key recovery will cost 'billions of dollars' to deploy, making encryption security both expensive and inconvenient.
- **New Targets for Attack** - Key recovery agents will maintain databases that hold, in centralised collections, the keys to the information and communications their customers most value. In many systems, the theft of a single private key (or small set of keys) could unlock much or all of the data of a company or individual.

6. UK Policy

Since 1994, a committee of permanent officials[72] has formulated UK encryption policy, providing unified advice to Ministers. Since 1995, the consistent aim of UK and US policy has been to introduce systems for ubiquitous "key recovery", intended to maintain covert access to electronic communications. The policy has never been debated by Parliament, or scrutinised by any Select Committee. After unsuccessful attempts by representatives of GCHQ to persuade the OECD to adopt 'Royal Holloway' TTPs as an international standard,[73] the Department of Trade and Industry was assigned the lead role, and announced in June 1996 its intention to regulate the provision of encryption services to the public,[74] stating that:

> 'It is not the intention of the Government to regulate the private use of encryption. It will, however, ensure that organisations and bodies wishing to provide encryption services to the public will be appropriately licensed.'[75]

Labour Party Policy

'Communicating Britain's Future' set out the pre-election policy of the Labour Party on encryption:[76]

---

72 The committee is chaired by the Cabinet Office, with representatives from the DTI, Home Office, Foreign Office, Treasury, GCHQ/CESG, Security Service and SIS.

73 Private information from those present at OECD meetings.

74 See Yaman Akdeniz, 'UK Government Policy on Encryption' [1997] Web Journal of Current Legal Issues 1.

75 See Paper On Regulatory Intent Concerning Use Of Encryption On Public Networks, DTI, June 10, 1996 at para 8.

76 'Communicating Britain's Future', (The Labour Party 1995) was removed in June 98 from its official website (http://www.labour.org.uk/views/info-highway/content.html), but is now available at http://www.liberty.org.uk/cacib/legal/crypto/labour2.html.

> 'We do not accept the "Clipper chip" argument developed in the United States for the authorities to be able to swoop down on any encrypted message at will and unscramble it. 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.'

If this amounts to a generic rejection of escrow, it appears that Labour Party intended solely to penalise a refusal to comply with a demand to decrypt under judicial warrant. The Labour Party further argued that attempts to control the use of encryption technology were "wrong in principle, unworkable in practice, and damaging to the long-term economic value of the information networks…. It is not necessary to criminalise a large section of the network-using public to control the activities of a very small minority of law-breakers."[77]

Mandatory Licensing - DTI Consultation

The DTI published the Consultation Paper[78] *'Licensing of Trusted Third Parties for the Provision of Encryption Services'* on 19th March 1997 (two days before a General Election was called). The paper was a detailed proposal for legislation in the first session[79] of a new Parliament, with a consultation period overlapping the election campaign, and expiring at the end of May. The timing of the announcement might uncharitably be construed as an attempt to present a new Government with a policy *fait accompli*,[80] but not apparently through the political direction of the previous administration[81].

The pre-amble to the Consultation Paper introduced the proposals in the context of the Government's Information Society Initiative, with laudable aims for the promotion of electronic commerce, educational networks, and better delivery of government services. However the subsequent exposition of the linkage between these goals and regulation of encryption services is parochial and deftly obscure. The US is only mentioned twice and

---

77 The policy document, available on the Labour Party web site since 1995, was removed in June 1998. It has since been re-posted on other sites. For example see the Campaign Against Censorship of the Internet in Britain at http://www.liberty.org.uk/cacib/legal/crypto/labour2.html.

78 See Cyber-Rights & Cyber-Liberties (UK) below for further information and for a critique of the DTI Consultation Paper. See also Dr Brian Gladman's home page at <http://www.seven77.demon.co.uk>. See also Akdeniz Y et al ,'Cryptography and Liberty:'Can the Trusted Third Parties be Trusted ? A Critique of the Recent UK Proposals', 1997 (2) The Journal of Information, Law and Technology (JILT), at <http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/default.htm>.

79 DTI Consultation paper, Annex F.

80 The Conservative Party would also face political difficulties questioning the proposals in opposition.

81 Conversation between one of the authors (CB) and a Labour spokesperson, 27th March 1997.

the Clipper Chip not at all, nor is there any reference to the four years of vigorous controversy that it ignited. There is no acknowledgement of the tremendous outcry against escrow from the Internet community, and the overwhelming opposition of academic cryptographers, the business sector, and civil liberties groups.[82] The exclusion of human rights organisations from the deliberations[83] of the OECD "Ad-Hoc Group of Experts" is also passed by. The inference to be drawn from the drafting is that the DTI attached little weight to the views of the broad coalition opposed to escrow.

The proposals are formulated in such a way that the most significant condition is only implicitly stated. **Public "encryption services" would be <u>prohibited</u>, unless they incorporated key escrow (or key recovery),…**

> "…whether provided free or not, which involves any or all of the following cryptographic functionality - key management, key recovery, key certification, key storage, message integrity (through the use of digital signatures), key generation, time stamping, or key revocation services (whether for integrity or confidentiality), which are offered in a manner which allows a client to determine a choice of cryptographic key or allows the client a choice of recipient/s."

The DTI (initially) described their framework as *voluntary* because "those wishing to use any other cryptographic solutions can continue to do so, but they will not be able to benefit from the convenience, and interoperability of licensed TTPs". Without mechanisms to establish trust, this is analogous to saying that friends may freely converse in private, but public meetings can only be arranged in venues wired for eavesdropping.

The key owner would thus be obliged indirectly to pay the costs of the TTP meeting much more stringent licensing criteria, and the TTP's insurance against negligent disclosure or employee malfeasance. Moreover the absolute amount of any damages claim will be limited by statute, and the TTP indemnified against claims arising from government access. The DTI also suggested that contracts made with digital signatures might only be presumed valid if certified by licensed TTPs.[84]

---

82 See Cyber-Rights & Cyber-Liberties (UK) 'First Report on UK Encryption Policy: Response to the DTI Consultation Paper,' Comment, 1997 (2) The Journal of Information, Law and Technology (JILT).

83 Organisations opposed to escrow arranged a parallel conference (http://www.epic.org/events/crypto_paris/) and eventually secured a hearing.

84 See the DTI Consultation paper, paras. 52, 53

Without compulsory key escrow, competition between CAs will ensure that basic certification is available, from a plurality of organisations, for low cost. With key escrow, the choice of TTPs will be limited to those able to apply economies of scale (or cross-subsidise) the costs of licensing, perhaps a handful (after market shakeouts) of large financial, telecommunications, or publishing organisations.

The natural model for certification services is that users will select as CAs (for particular purposes) organisations with which they have a pre-existing affiliation or fiduciary relationship (solicitors, accountants, political or professional associations, trade unions). Such organisations would benefit from the good will established by long-standing trust relationships with their clients or members. This commercial franchise would be expropriated by mandatory TTP licensing with escrow, as the marketing of value-added services is skewed in favour of larger combines. In the Information Society should government, or the public, decide who is to be trusted?

The paper also states that 'encryption services by unlicensed TTPs outside the UK will be prohibited', without suggesting how this extra-territoriality could be enforced. Section VI stated that legislation similar to the Interception of Communications Act ("IOCA") will be introduced for the recovery of keys. But the intended scope is much wider than IOCA because it will cover not only information in transit, but also 'lawful access to data **stored** and encrypted by the clients of the licensed TTPs'.

For the purposes of legal access, the paper proposes that a 'central repository' be established to 'act as a single point of contact for interfacing between a licensed TTP and the security, intelligence and law enforcement agencies who have obtained a warrant requiring access to a client's private encryption keys.' The report '*The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption*' expressly warns of the hazards[85] of concentrating keys in centralised repositories. They present an irresistible target for penetration, and there are documented instances of unauthorised access to every kind of military, police and corporate system gained through lax security or suborned employees.

---

[85] See 'The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption' Report mentioned above.

7. Recent Developments

OECD

In March 1997, while not taking sides on the benefits or drawbacks of key escrow, the OECD issued cryptography recommendations that warn against "unjustified obstacles to international trade and the development of information and communications networks (8th principle)" and "legislation which limits user choice. (2nd principle)."[86] The 5th principle stated that:

> The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

The 6th principle refrained from recommending government access to keys, allowing only that "national cryptography policies **may** allow access to cryptographic keys or encrypted data". The 6th OECD principle concludes that "these policies must respect the other principles contained in the guidelines to the greatest extent possible".

United States

Several bills have been stalled in Congress for more than a year, undergoing contradictory revisions from various sub-committees. There are three major encryption related bills currently pending through the US Congress:

- The "Security and Freedom Through Encryption Act" (SAFE, HR 695), which rejects both domestic controls on strong encryption, and regulatory inducements to use trusted third-parties or key-recovery agents, while liberalising export controls.
- The "E-Privacy Act" (S. 2067), provides that personal confidential information, such as health and financial data, should be securely encrypted, intends to liberalise export controls, and establishes a "NET Center" to develop computer penetration techniques for eavesdropping to assist Federal, State and local law enforcement authorities.
- The "Secure Public Networks Act" (S.909, aka "McCain-Kerrey"), coerces domestic use of "third party" key-recovery agents through voluntary licensing linked to regulatory incentives and liabilities, and stipulates key-recovery as a requirement

[86] See OECD Cryptography Policy Guidelines: Recommendation of the Council Concerning Guidelines for Cryptography Policy, at <http://www.oecd.org/dsti/iccp/crypto_e.html>, 27 March 1997.

for all government financed research into future Internet architectures.

If UK policy continues to shadow that of the US, S.909 may prove to be a model for the forthcoming "Secure Electronic Commerce Bill" through the UK Parliament (below).

The FBI continues vigorously to assert an absolute requirement for law-enforcement to have covert access to private keys. Diffie and Landau offer critical scrutiny of their arguments,[87] suggesting that the FBI has expediently confounded statistics on the efficacy of microphone versus wiretap surveillance, to extrapolate a stronger case.

European Commission

In October 1997, the European Commission published "Towards A European Framework For Digital Signatures And Encryption"[88]. The Commission's communication paper, "in contrast to the UK initiatives and despite years of US attempts to push the 'government access to keys' idea overseas, finds key escrow and key recovery systems to be inefficient and ineffective."[89] According to the Communication paper:

> "nobody can be effectively prevented from encrypting data….by simply downloading strong encryption software from the Internet. As a result restricting the use of encryption could well prevent law-abiding companies and citizens from protecting themselves against criminal attacks. It would not however prevent totally criminals from using these technologies."

The European Commission further called on the Member States to avoid disproportionate national restrictions, "to ensure that the development of electronic commerce in the Internal Market is not hindered and to facilitate the free circulation and use of encryption products and services".

This communication was followed by a May 1998 "Directive on a Common Framework for Electronic Signatures"[90]. The directive highlights the problem that:

---

87 Diffie, W., & Landau, S., Privacy on the Line: The Politics of Wiretapping and Encryption, London: MIT Press, 1998.

88 European Commission Communication, "Towards A European Framework for Digital Signatures And Encryption," Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions ensuring Security and Trust in Electronic Communication, COM (97) 503, October 1997, at <http://www.ispo.cec.be/eif/policy/97503toc.html>.

89 Akdeniz, Y., "No Chance for Key Recovery: Encryption and International Principles of Human and Political Rights," (1998) Web Journal of Current Legal Issues 1.

90 Proposal for a European Parliament and Council Directive on a common framework for electronic signatures (European Commission) - Communication from the Commission to the European

> "…different initiatives in the Member States lead to a divergent legal situation.... the relevant regulations, or the lack of them, will be different to the extent that the functioning of the Internal Market in the field of electronic signatures is going to be endangered…Further uncertainty results from different liability rules and the risk of uncertain jurisdiction concerning liability where services are provided among different Member States."

The proposed solution of the European Commission is that "the legal recognition of electronic signatures should be based upon objective, transparent, non-discriminatory and proportional criteria and not to be linked to any authorisation or accreditation of the service provider involved". Therefore, according to the European Commission:

> "Common requirements for certification service providers would support the cross-border recognition of signatures and certificates within the European Community."

The proposals of the Commission have direct consequence for the suggestion in para.53 of the DTI Consultation paper that a presumption of legal validity be accorded to signatures certified by a licensed TTP/CA. If the onus of proof were on the signer to rebut validity, rather than on the counter-party to establish it, this would provide a powerful incentive in commercial transactions to prefer signatures made with licensed certificates. Even if the acceptability of unlicensed signature certificates could be established through a test-case in common law, would legislation granting a preferred status to licensed certificates be regarded as "discriminatory", and therefore in breach of the Directive?

The Directive only addresses certification of keys used for signature. In the early phases of e-commerce, it may be anticipated that for convenience, the public will prefer to obtain signature and encryption technology from a "one-stop shop". If licenses to certify digital signatures were only available to organisations that operated key-escrow/recovery for their encryption services, and signature certificates were only presumed valid if licensed, market forces would strongly coerce adoption of the "voluntary" regime.

Responses to DTI Consultation

An official "Summary of Responses" to the March 1997 consultation paper was

---

Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: Proposal for a European Parliament and Council Directive on a common framework for electronic signatures COM(1998) 297, Final, May 13, 1998. See http://www.ispo.cec.be/eif/policy/com98297.html.

published by the DTI in April 1998, at the same time as the "Secure Electronic Commerce" statement (below). The summary tabulated responses to the specific questions asked in the consultation. However, since many responses disagreed with the basic premise that facilitating e-commerce requires access to private keys under third-party control, on which views were not sought, it would be unreliable to infer any consensus on dependent issues. The summary acknowledged that:

> "The issue of access to keys for law enforcement purposes attracted by far the most comment - particularly from individuals. Much of it was fundamentally opposed to the whole concept of lawful access."
>
> - "Many of the more technical responses questioned the effectiveness, or even the feasibility, of the key escrow proposals in the paper"'

Voluntary Licensing - "Secure Electronic Commerce"[91]

The Labour Government on 27th April 1998 announced its intention to "introduce legislation to license Trusted Third Parties, Certification Authorities and Key Recovery Agents" and "such licensing arrangements will be voluntary, as business has requested". Organisations facilitating encryption services will be "encouraged" to seek licences, but can only do so if they "make recovery of keys (or other information protecting the secrecy of the information) possible.

The statement refers to a "clear policy differentiation between digital signatures and encryption", but whether an organisation can get a license to issue signature certificates, if it also wishes to offer encryption services without key-recovery, remains inscrutable. Pressed on this point, the DTI has said that the issue raises "consumer protection" concerns which may require "Chinese walls".[92]

The Home Office will introduce legislation to enable law enforcement agencies "to obtain a warrant for lawful access to information necessary to decrypt the content of communications or stored data (in effect, the encryption key)". The new powers will apply to anybody holding this information, including the user.

---

91 Department of Trade and Industry, Secure Electronic Commerce Statement, 27 April, 1998 is available at http://www.dti.gov.uk/CII/ana27p.html. See for a critique of the new proposals in Akdeniz, Y., & Walker, C.P., "UK Government Policy on Encryption: Trust is the Key?" (1998) *Journal of Civil Liberties* 110-116.

92 Nigel Hickson, DTI, "Scrambling for Safety," conference, 29th May 1998.

Strategic Export Controls

Cryptographic research and development, whether academic or commercial, requires frequent exchanges of source code, compiled code, abstract discussion, and mathematical analysis. This is commonly done via e-mail or the World Wide Web. Cryptographic methods (and research into "attacks" on such methods) are intrinsic to the protection of intellectual property, securing the cyber-infrastructure, privacy and protection of personal data, and the enabling of electronic commerce.

A DTI White Paper on Strategic Export Controls[93] was published in July 1998, primarily dealing with Scott Report[94] recommendations concerning proliferation of technologies for weapons of mass destruction. However, the DTI paper also contains proposals for extending export controls to "intangibles", that is information carried electronically, rather than on physical media. Section 3.2.1 proposes that:

> " new legislation should provide it with the power to control the transfer of technology, whatever the means of transfer.

This power would cover transmission by fax, and e-mail over the Internet (or organisations' intranets). "Documents transferred abroad containing controlled technology should be subject to export licensing requirements, whether exported physically or in electronic form."

The reference to "controlled technology", in contrast to other sections of the White Paper, is not qualified or related to weapons of mass destruction, and therefore applies to cryptography.[95] Hypothetically, a researcher e-mailing a colleague abroad with implementations of (or even mathematical remarks bearing on) cryptography would be in legal jeopardy, unless they obtained export license approval to do so.

The secondary powers created under 3.2.1 would also allow the Government to ban oral discussions and dissemination of abstract mathematical research, without further primary legislation, although the paper incongruously acknowledged that:

> "…it is right that controls on the transfer of information orally or through personal demonstration should be limited to the areas of greatest concern, in

---

93 DTI, White Paper: Strategic Export Controls, July 1998, http://www.dti.gov.uk/export.control/.

94 See Sir Richard Scott, Report of the Inquiry into the Export of Defence Equipment and Dual-Use Goods to Iraq and Related Prosecutions, London: HMSO, July 1996, HC 115 (95/96).

95 Current Export Control Lists is available at http://www.dti.gov.uk/export.control/

> view of the difficulties of licensing such transfers, both for applicants and for the licensing authority, and given also that there are sensitivities in relation to free speech and academic freedom"

Elsewhere there is reference to Government support for parallel measures at EU and Wassenaar level.[96] The intention is to put the encryption "genie back in the bottle", by criminalising international development and electronic dissemination of non-approved encryption software (presumably that which lacks key-recovery), and thus contravenes Labour's pre-election policy. The combined effect would be to deter world-class researchers from working in Britain, inhibit innovation and dissemination of knowledge necessary to secure the cyber-infrastructure, and create sweeping powers to limit academic freedom of expression, leading to a predictable decline in a strategic economic sector. Moreover the policy is unenforceable as encryption and steganography could be used to distribute intangible "controlled technology" undetectably. It would be a tragic irony if enforcement of a ban on the dissemination of cryptography became the raison-d'être for the kind of Internet surveillance apparatus which motivated Phil Zimmermann to create PGP in the first place.

6. CONCLUSION

The central difficulty underlying the manoeuvres of the pro- and anti-escrow lobbies is that there is a genuine dilemma: current technology really *does not admit striking a balance*; voluntary measures only make sense as a prelude to later prohibitions. The *realpolitik* view of the Internet community is that the DTI proposals are the product of a joint UK and US strategy: "voluntary" escrow is *designed* to be unstable, and squeeze out non-escrowed systems competing outside the legal protection of a regulatory umbrella. It places Britain at the sharp end of promoting US policy in Europe.

The forthcoming Secure Electronic Commerce legislation will only bestow a "safe and secure" license of government approval on those TTPs that can recover the decryption key of their subscribers. The supposed attraction depends on the canard that organisations or individuals who lose their keys need the service provider to retrieve a copy. But everyone can - and should - backup their key (good software insists on it), and keep a copy in a safe place anyway, just as everyone should keep a backup copy of

---

[96] See the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies at http://www.wassenaar.org/.

the data itself. Key recovery is a useful facility, but there is no need for the end-user to forfeit custody.

If a critical mass of the infrastructure adopts licensing, a future government could claw its way to a position of blanket key recovery later: keys expire or can be instantly revoked, and government could insist on recovery compliance for renewal. It remains to be seen how many players in the nascent information economy opt for licensing, or whether they will allow their customers custody of their own keys and the responsibility of keeping a backup.

The new policy statement contains enough ambiguity for the DTI to gauge the degree of dissent before defining carrots-and-sticks in the licensing restrictions, or possibly to defer questions of detail to a regulator created by primary legislation. Despite several years of UK lobbying at the OECD and European Commission, few democratic countries appear keen to have strong limits on the domestic use of strong encryption. Only Belarus, China, France, Israel, Pakistan, Russia and Singapore currently restrict domestic use of cryptography.[97]

The Home Office plans to introduce legislation to allow keys to be subpoenaed under warrant, whether covertly from a service provider operating key-recovery, or from the end-user, which will raise difficult questions. What will constitute prima facie grounds for issue of a warrant, to recover evidence that by definition is unknown? Will a judge be able to draw adverse inference from a suspect's refusal (or inability) to produce a key to unlock information which the prosecution believes to be incriminating? Suppose a suspect has genuinely lost their key? In any event, given the likely proliferation of steganography techniques, the prosecution may be unable to demonstrate the existence of any encrypted data at all. The new legislation will be introduced at a time of renewed unease about oversight and safeguards governing conventional forms of surveillance.[98]

In the US, the current two-year relaxation on export of 56-bit non-escrowed encryption expires this year, and key-recovery systems that can feasibly be deployed globally and inter-operably are no nearer realisation. Proposals for a "NET Center", a national facility

---

[97] See GILC, Cryptography and Liberty: An International Survey of Encryption Policy, Washington DC, February 1998, at <http://www.gilc.org/crypto/crypto-survey.html>.

to develop software bugging devices which can be inserted (possibly remotely) into targeted computers to defeat encryption, may be seen to offer a better solution.

The fork in the road is clear. One path leads to an infrastructure capable of an unprecedented degree of state surveillance limited only by perpetual government self-restraint; the other leads to a dilution of power and strengthening of privacy, but with compensatory reforms to assist law-enforcement. Without independent expert scrutiny and public debate of the law-enforcement case, escrow may happen by default.

Background Information about the Authors

CASPAR BOWDEN (cb@fipr.org) is Director of the Foundation for Information Policy Research (http://www.fipr.org), an independent non-profit organisation which studies the interaction between information technology and society, identifies technical developments with significant social impact, and commissions research into public policy alternatives. He was formerly a consultant specialising in Internet security and e-commerce, senior researcher of an option-arbitrage trading firm, a financial strategist with Goldman Sachs, and chief algorithm designer for a virtual reality software house.

YAMAN AKDENIZ (lawya@cyber-rights.org) is currently a full-time Ph.D. student at the CyberLaw Research Unit, Centre for Criminal Justice Studies, University of Leeds, and his thesis title is "The Governance of the Internet". He has written several articles related to the Internet and is also the founder of Cyber-Rights & Cyber-Liberties (UK) (http://www.cyber-rights.org), a non-profit civil liberties organisation, which opposes the DTI encryption initiatives. Its main purpose is to promote free speech and privacy on the Internet, and it is a member of the Global Internet Liberty Campaign.

[98] JUSTICE, "Under surveillance: covert policing and human rights standards," July 1998.