

https://dspace.org/

The Collision of Regulatory Convergence and Divergence: Updating Policies of Surveillance and Information Technology

Hosein, Ian

2001-12-15

LINK Centre, University of the Witwatersrand (Wits), Johannesburg

http://hdl.handle.net/10539/19835

Hosein, I. (2001). The collision of regulatory convergence and divergence: Updating policies of surveillance and information technology. The Southern African Journal of Information and Communication (SAJIC), 2. https://doi.org/10.23962/10539/19835

Downloaded from a DSpace repository. https://dspace.org/

The Southern African Journal of Information and Communication - Issue 2, 2001

The Collision of Regulatory Convergence and Divergence: Updating Policies of Surveillance and Information Technology

Ian Hosein, Department of Information Systems, The London School of Economics and Political Science

Abstract

Regulation theory rarely considers the disruptive capacity of technology, nor regulation in the sole interest of government. This paper will investigate the capacity of technology to disrupt regulatory regimes surrounding surveillance and communications infrastructure in various countries. As policy regimes are updated to meet new challenges, through the creation of new policy habitats, new powers are created despite protests and claims of technological neutrality. However, the capacity to interpret technology does not end: technology will disrupt even the new habitat, requiring renegotiation and re-settlements. Such negotiations often occur at the international level; some of these processes will be reviewed and critiqued. Considering the contingent nature of technology policy, this paper then recommends some ways forward when considering new national policies, such as the process that South Africa is about to embark on.

Technology, interests and statutory powers

Despite arguments even in liberal economies such as the US about hesitating to regulate the nascent on-line industry (1), there are many movements towards legislation on information and communications technologies in the interests of the state. Particularly, governments have been committed for quite some time in working towards ensuring that their surveillance and investigative capabilities are *maintained* in the "digital age". Consider how governments tried to control the proliferation and use of cryptography (2) under the justification and concern:

> Encryption, as a practical matter, diminishes the power of law enforcement to do its job, and we seek only the way to maintain the original status quo. The consequences of our losing the ability to wiretap would be enormous. (3)

The US policy on controlling market access to cryptography eventually weakened allowing for market liberalisation, particularly because "maintaining the status quo" was considered to be onerous on industry, and in direct conflict with individual rights, including the right to privacy; if not also infeasible.

Similarly, in the United Kingdom when the controversial surveillance-enabling statute, the Regulation of Investigatory Powers Bill was introduced to the House of Commons, the Home Office Minister stated

> Jack Straw: This is an important Bill, and represents a significant step forward for the protection of human rights in this country. Human rights considerations have dominated its drafting. None of the law enforcement activities specified in the Bill is new. What is new is that, for the first time, the use of these techniques will be properly regulated by law and externally supervised. That will serve to ensure that law enforcement and other operations

> are consistent with the duties imposed on public authorities by the European convention on human rights and by the Human Rights Act 1998. (4)

In the course of a long debate, it was finally acknowledged that the powers were indeed new, and the consistency with the Human Rights Act was not clear. When the RIP Bill reached the House of Lords, the Lords Home Office Minister stated

> Although, strictly speaking, the [forced decryption] power is new, it arises only as a response to developments in technology. Technology has the potential to limit considerably the capabilities of law enforcement and other agencies in preventing crime. The [forced decryption] power in the Bill will go some way towards redressing the balance. (5)

Unlike the US policy on cryptography (key escrow particularly), the RIP Bill became law, receiving Royal Assent in July 2000, despite industry and NGO concerns regarding costs and individual rights. (6)

As old traditions such as interception of communications, search and seizure, and access to communications traffic/transactional data are *adapted* or updated to meet the technological challenges of digital communications infrastructure, the required powers are not a case of maintaining old powers, but rather are increases in powers due to the *nature of the technology itself* (7). This article will show how new technology *disrupted* old statutory powers and will follow some new government policies to deal with this problem. However, this article will argue that these new policies result in greater powers than previously held, again because of the nature of the technology itself. South Africa has slowly developed its *cybercrime* statutory proposals (8) as it awaited the outcome of the Council of Europe (CoE) Draft Convention on Cybercrime (9). This article will end with warning notes to countries about to embark on a national process, drawn from experiences with the CoE, the G8, and various national processes.

Technology as a disruption of the status quo

Contemporary literature in most disciplines discusses technology as a disruptive force to the status quo. New technologies harm the environment; new technologies help the environment but change policies (consider Kyoto). New technologies transform the way organisations operate, or management structures (consider Business Process Re-engineering). Even the regulation literature notes that information technologies can change the nature of regulated industries, as in Peltzman (10) on the sources of pressure for deregulation, being

> ... changes in the 'politics' and changes in the 'economics' of the regulated industries. Political change includes such things as shifts in the relative political power of contending groups and changes in the underlying organization and information technologies (p.108).

Peltzman continues that technology is a disruptive force on regulations such as in interest-rate regulation (p.121) to telecommunications regulation (p.117).

Likewise, Hood (11) [1994, p. 11] reports on various theories on the reversals of policy, including the cause of a "loss of policy habitat" that can be a result of structural changes such as the change of technology. This purported *habitat* consists of the particular social structures that existed at the time of policy formation; technology can force a change in this habitat. Unfortunately such lines of investigation tend to focus on post-industrial society theories that overplay the role of society, or otherwise treat technology as deterministic, and as a result suffers from the valid critiques of such theories (p.12). Hood also argues

> And social change is not necessarily an independent factor from which everything else

> stems. It may itself be a product of other policies, designed to 'shape' preferences. [...] Such explanations are often claimed by their critics to be too 'technocentric', leaving too little room for the autonomous dynamics of politics (pp.12-13).

However, even as he moves on to investigate other theories, such as Chicago School interest-based theories for policy reversals, he notes that interest-based views also lack clear articulations of the role played by "broader sociotechnical developments", since few accounts "put this element at centre stage and it seems at best to have been part of the background" (p.36). This article intends to bring the technology into the foreground, but without attributing deterministic status to the technology either; the interests of **both** the human and non-human actors are essential (12) (13). Therefore, placing the technology in the foreground is the immediate task; and the search for more regarding its *disruptive* role may lead to a better understanding of regulatory issues generally.

What is it, therefore, with technology that causes such regulatory change? Let us look specifically at the procedural powers being discussed, and the technological infrastructures that are changing.

Towards new interception and access to transactional data regimes

Traditional telephony, i.e., plain old telephone system which operated through circuit-switching, *allowed for* alligator clips to be attached to lines and clear and simple interception. Likewise, transactional data was not difficult to accumulate: who calls who, for how long, at what time of the day, are all recorded in some form by the telcos anyway. As the infrastructure became more and more complex, interception regimes became more detailed. There are three significant technological developments that affected the powers of investigation: digital switches involving circuit-switched technology; packet-switched communication infrastructure, such as the Internet and digital circuit-switched communication, such as mobile phones.

- **Digital switches** made interception and access to transactional data difficult because of the complexity and speed at which switches would operate. Concerned with this development in the US, the Department of Justice negotiated with Industry and the Electronic Freedom Frontier (14) to find a solution: the 1996 Communications Assistance for Law Enforcement Act (CALEA). CALEA required intercept capability and access to transactional data be built in to switching technology; and the US Government would pay for all such changes made by 1995, and 500 million USD in subsidies for 1995 to 1998. CALEA was restricted to circuit-switching technologies such as the plain-old-telephone system, though subsequently extended to mobile communications; the negotiators intentionally avoided dealing with internet communications on that occasion. (15)

- **Packet-switched communications infrastructures**, such as the Internet pose greater problems to interception capabilities and access to transactional data. The technological challenges are numerous [2000, p. 6] (16) and the resulting costs are up for debate, sometimes heated (17). Predominant challenges to intercepting e-mail include identifying data streams, identifying users, cross-border searching, and tapping specific data streams without intercepting all streams (and thus failing the European Convention on Human Rights requirements on proportionality and specificity). Traffic/transactional data is a new conundrum of its own: what is transactional data within this technological environment? Is it every website that a suspect visits or is it the details to specific e-mails? What of web-based mail? And traffic data collection also has its own costs issues, particularly storage requirements that are non-trivial.

- While the US chose to concentrate specifically on **circuit-switched communications** under CALEA, many other governments are working on policies of *technological neutrality*. The UK, for

example, chose to *update* its Interception of Communications Act 1985 with the RIP Act 2001 by referring to *communications services providers*, as such a term emcompassed Internet Service Providers, Mobile Phone service providers, and traditional telephone companies, whereas the 1985 act referred only to public telecommunications operators. The costs may be reimbursed for the intercept capability development at *some* CSPs, from a likely 20 million pounds set aside by the Home Office. Likewise, the Dutch Telecommunications Act 1996 makes no distinction between different telecommunication networks or services, and as a result its laws requiring intercept capability, apply to all communications infrastructure, without regard to costs incurred by industry. The Australians also have a common view of technological neutrality: all infrastructures are built equal, as are all warrants (paid by government) and capability requirements (paid by industry).

Towards securing access to secured communications

A key advantage to digital communications from the perspective of security is that they can be encrypted with limited effects on efficiency. Mobile telephone communications that are digital are encrypted between the handset and the base station. Likewise, e-mails can be encrypted to the recipient, rendering communications difficult to decrypt in transit. Previous government policies such as Key Escrow or Key Recovery have proved unsuccessful, as well as attempts to limit the existence or export of cryptographic products have also proved problematic, partly because of their importance in establishing trust and confidence (18) in electronic commerce particularly (19).

This situation has been of some concern to governments, particularly owing to their policy failures, and also owing to their continued insistence on being able to gain access to all communications, irrespective of the medium and security measures applied. Under the spectre of terrorism, paedophiles, and people and drugs trafficking, the UK Government was the first Western government to implement the statutory power for forced decryption, or forced disclosure of decryption keys. That is, under Chapter III of the RIP Act 2000, law enforcement authorities can force an individual to hand over their key used to protect communications, as well as force decryption of communications that have been intercepted; failure to do so may result in a two-year sentence (seven years in a similar policy in India).

Disruption leading to a new habitat

As a result of changing technologies, some governments have been moving to create new policies, or alter older ones, in order to maintain their powers. This changes the structure of the habitat, however, the socio-technical environment will inevitably change as a result, possibly with new challenges.

Governments wish to maintain the status quo with regards to their interception, access to transactional data, and ability to read the product of interceptions. If the South African government wishes to maintain its capabilities and ensure the status quo, it may have to consider similar policies. However, there are associated risks, as the technology remains disruptive.

Technology as a disruptive factor

Technology disrupting the policy habitat of traditional surveillance was the grounds for new policies and a new habitat. However, the result is that the technology remains disruptive.

Disruption of civil liberties

The arising controversy and concern from these policies of interception, access to transactional data, and cryptographic keys are linked directly to the technological infrastructure and also its disruptive capacity.

The difficulties and costs behind intercepting and accumulating transactional data at digital-switches were due to the costs involved in building such capabilities. The costs of intercepting and accumulating transactional data of mobile telephony are only now being understood, particularly as non-public agreements between mobile phone developers and government agencies are being uncovered for GSM (20) that was forcibly weakened, and even Third Generation mobile phones (21) that appear to have been designed for interception.

Interception capabilities aside, there are the arising risks, as introduced by the US FBI, of "black boxes" such as the controversial Carnivore systems (recently renamed DCS1000). Carnivore is a system introduced at ISPs in the US who are unable to intercept traffic; Carnivore, when attached to the network, is promised to isolate the specific data flow of interest and be able to completely monitor all email communications and all websites, conversations, etc., that occurred while installed. A furore arose when this was made public - from both the civil liberties and technological standpoints. The technological concerns included: the challenges of isolating and reconstructing the intended traffic of a specific individual without confusing it with other traffic; that Carnivore might damage ISP networks because the one-size-fits-all approach of Carnivore does not match ISP architectures that always vary; and the lack of openness to ensure that the warrant request and the system configuration are directly mapped. As two leading computer security experts state: "Unfortunately, there's no systematic way to be sure that any system as complex and sensitive as Carnivore works as it is supposed to." (22)

From these technological concerns about Carnivore also arise the civil liberties concerns; particularly that are argued as

> The Carnivore system gives law enforcement email interception capabilities that were never contemplated when Congress passed the Electronic Communications Privacy Act (ECPA) … Carnivore raises new legal issues that cry out for Congressional attention if we are to preserve Fourth Amendment rights in the digital age.

Civil libertarians are concerned directly with the technology, as they continue

> But unlike the operation of a traditional a pen register, trap and trace device, or wiretap of a conventional phone line, Carnivore gives the FBI access to all traffic over the ISP's network, not just the communications to or from a particular target. Carnivore, which is capable of analyzing millions of messages per second, purportedly retains only the messages of the specified target, although this process takes place without scrutiny of either the ISP or a court (23). Moreover, civil libertarians raise a subtle point that has significant implications regarding transactional data. In reporting regarding a previous testimony to the House on the issue [a witness] detailed his client's concerns that a trap and trace order in the context of the Internet revealed information that Congress did not contemplate when it authorized their limited use. In the traditional telephone context, those orders reveal nothing more than the numbers dialed to or from a single telephone line. In the Internet context, these orders and certainly Carnivore, are likely involve ascertaining the suspect's e-mail address, as well as header information that may provide information regarding the content of the communication.

Such devices give more than just that - if transactional data access is extended beyond traditional communications, it may consist of mapping out exactly which websites and files were accessed during a session. If defined in this way, it is a significant increase in the powers of law enforcement, as it is akin to monitoring someone walking down a High Street, looking at exactly what they look at, which books they review, which shoes they want to buy, and whatever else catches their eye.

Finally, the Government Access to Keys (GAK) power gives rise to risks to civil liberties. If governments access a private-decryption key of an individual, they will be able to decrypt all past traffic encrypted to that key, and all future traffic as well. If GAK policies allow access to keys also used for signatures (which is not the case in the UK), governments could then digitally sign documents in the name of the suspect. Because of the structure of the technology, this impacts individual rights again as this time individuals are forced to participate in the investigation into their life, regardless of their guilt or innocence. That is, law enforcement agents will show up at their door and request their keys, or for them to hand over decrypted data. This is a highly controversial power, however; particularly on grounds of burden-of-proof and self-incrimination which may conflict with European Convention on Human Rights and resulting jurisprudence. (24)

As a result, just as technology may have changed and disrupted previous government capabilities and policies, technology under a new policy habitat (be it specific such as CALEA or *neutral* such as in Australia and the Netherlands, or new generalised policies as within the UK) can work to be even more invasive than before; and thus a disruption of civil liberties. Moreover, technology may be designed specifically for the new policy habitat, that of renewed government surveillance, thereby minimising risks and costs while still producing product. This appears to be case with the next-generation mobile phones that have intercept capabilities designed within the protocols. Regardless of this, cost issues must also be considered.

Disruptions to new policy habitat

Technology does not necessarily become mute the moment a new habitat is created, as there are still limitations to this new policy habitat. Technologies can still be disruptive to new policy, particularly under the creation of "substitute products just outside of the regulatory 'ring-fence' ", as Hood explains

> If regulation follows the classic 'client politics' pattern, with costs diffused among a scattered group of consumers and benefits concentrated on a small, well-organized producer group, there may be a point at which unregulated producers start to offer near-substitutes to the regulated product. Such a move could trigger a dynamic process which causes the whole regulatory structure to unwind, culminating in a situation in which the original 'client politics' group start to lead the move to deregulation.

The US subsidy scenario for CALEA and telcos (non-ISP) resulted in a client politics environment with a fence: telcos have to adhere to CALEA, but ISPs do not. Moreover, cable companies now provide Internet capabilities, and they fall under the Cable Act rather than CALEA. It is only natural that the US Government will wish to extend its policy to reach these other industries (and for telcos to be unhappy until this is done). It in fact attempted to do this in the summer of 2000, but the legislative schedule did not permit it. This is a case of regulatory convergence. CALEA could perhaps be extended without requiring its demise, but this would require a new settlement.

However, if non-US regulated service providers could also provide access for American citizens, then the capacity to intercept communications through required intercept capabilities is legally lost. Even then, CALEA has reached out beyond. In one case, the FBI blocked TMI, a Canadian satellite company, from providing services to US users; a settlement arose with an agreement that TMI's switch would be on U.S. soil (25). Another interesting situation, arose with NTT's acquisition of Verio, a US-based telecommunications provider (including Internet). On the grounds of an espionage risk, because the Japanese NTT would have access to U.S. government wiretapping activity and could present an espionage risk, the US Government at first opposed the merger. This was the first time national-security reviews similar to those surrounding past aerospace and defence deals have been applied to an international Internet acquisition. (26)

CALEA does not cover Internet traffic. CALEA was not intended to, as it does not cover what it calls "information services", the most prominent of which is "electronic messaging" – e-mail, instant messaging, etc. It could be extended, but it would face opposition. Rather, in 1999, the Department of Justice in the US decided to deal with the messaging problem in 1999 by approaching the Internet Engineering Task Force, asking this open body that develops standards for the Internet, to set standards that allows for intercept capability. After an open debate, the measure was rejected by the membership of the IETF. Carnivore then arrived. It appears that the disruptive force of technology arose and created a new infrastructure that did not fit the shape and mould of a specific regulation like CALEA.

With more *technology neutral* policies, a ring-fence also exists, but it is not in the form of a specific medium. Because these are neutral policies that state that communications infrastructure must allow for intercept capability, this includes the Internet. However, in situations such as these, three forms of opposition arose from the technology. First, the inordinate costs, second technological circumvention, and third, regulatory arbitrage/competition.

- **Inordinate costs**: consider the situation in the Netherlands, where the government was among the first to advocate interception capabilities at ISPs under the guise of neutrality. Immediately there was significant resistance to creating interception capabilities at ISPs: ISP associations argued that the high costs and complexity would result in putting small and medium-sized service providers out of business (27). Australia has also had to deal with this; the costs and burden upon the operators have proved more difficult and expensive than anticipated. As a result, the carriers in Australia were given both a waiver from the requirement for several years and, it is understood, a subsidy towards the cost, which was not part of the original settlement. In a sense, the complexity of networks and the costs *resisted* the new policy habitat, established under the 1996 Telecommunications Act.

- **Technological circumvention:** Products and services such as Anonymizer.com, Hushmail, and the Freedom Network already pose a theoretical challenge for governments to ascertain transactional data and intercept communications. All three services offer e-mail that is off-shore, or secured in a manner that makes interception impractical. Government Access to Keys, however, still is a possibility to some extent within these products and services. However, the mass investment in fencing-in industry to comply with the new policy habitat could be to no avail if the determined criminal wished to act using such protection. Moreover, an intelligent criminal could circumvent all of these new powers without the use of these products and services, such as described in (28), and other methods are possible to circumvent Carnivore-like systems as well.

- **Regulatory arbitrage/competition:** In the United Kingdom, when the RIP Act was about to pass the House of Lords, a number of ISPs announced that they were going to move off-shore (outside of the 'fence-ring') in order to continue to provide reliable service to their clientele. While the current status of these threats remains unknown, at least one financial institution is moving all decryption keys off-shore so that they can not be accessed by the UK Government. Such international arbitrage can be done because of the nature of the Internet itself: acting at a distance is at times as simple as acting immediately (29). So a decryption key that exists off-shore can be accessed by an appropriate user with relative ease to accessing it from the user's hard drive, but the former method prevents leakage to government agencies as most other countries do not have a GAK policy.

New legislation and powers could be created to force compliance, as occurred with the TMI and NTT situations in the US, and technology can be banned such as the Freedom Network and Anonymizer. However, limiting access to services in other countries may be very difficult for governments to implement, particularly when these same governments are competing to be the worlds' best places for

electronic commerce, as they see the economic benefits of openness. The alternative solution is to ensure that the world becomes consistent with the national policies. This would prevent regulatory competition.

International arbitrage and settlement

After a long and heated battle within Parliament, the RIP Act was passed in July 2001. The debate in Parliament surrounded the disruptive capacity of technology, and the concerns about human rights and costs. In these last days of debate, a number of companies warned that they would move off-shore, supporting a case argued by a report from the British Chambers of Commerce. Relieved that it was about to be passed, the main Home Office Minister responsible for the Bill closed off the debate with the following statement

> Mr. Clarke: After the Bill receives Royal Assent, we shall work with the industry - and the Opposition, if they are willing - to promote it both in this country and internationally. Given the comments made in the overseas media, we must explain clearly what the Bill is and is not, and why we do not believe it poses a threat to e-commerce in Britain; on the contrary, it will help to achieve the Government's aim of a strong and secure e-commerce economy, to which we are all committed.
>
> Propaganda is needed, and I hope that the whole House will help to promote the interests of this country's businesses when the time comes. (30)

Insistent on not appearing as isolated in demanding such new powers, the Home Office often argued that it was acting completely consistently with the OECD guidelines on cryptography policy, with the CoE draft convention on cybercrime, the work of the G8 Lyon Group on hi-tech crime, EU Justice and Home Affairs Committee, and various countries including the US, the Netherlands, and Australia. (31) (32)

The Internet can enable users to send data across many countries, and this is also why it threatens executive powers of governments. Users can receive their messages from a server held in another country. So long as this is possible, it renders national powers of interception and access to transactional data challenging. If messages cannot be intercepted, then access to keys is moot (except in the case of stored data). Such activity can be controlled, i.e. data flows between countries may be shut down, but the technological systems (33) are disruptive: users can connect (at cost) through other countries or non-regulated access points, and the economy would not look approvingly on restricting data flows in the age of e-commerce. This is the problem-space of the work of the G8 and the Council of Europe, particularly as they try to harmonise investigative powers and allow for mutual legal assistance across borders to overcome the technological challenges that remain the new policy habitat.

G-8 World Tour: Lyon, Paris, Berlin, Tokyo ...

At a summit in Halifax, Canada in 1995, the G7 created the Lyon Group, a Senior Experts Group on Organised Crime, which later expanded its tasks to include Transnational Crime, Terrorism, and Hi-Tech issues. In a July 1996, meeting in Paris, the Group of 8 agreed on matters including

> 6. Note the risk of terrorists using electronic or wire communications systems and networks to carry out criminal acts and the need to find means, consistent with national law, to prevent such criminality.
>
> 11. Accelerate consultations, in appropriate bilateral or multilateral fora, on the use of encryption that allows, when necessary, lawful government access to data and communications in order to, inter alia, prevent or investigate acts of terrorism, while

protecting the privacy of legitimate communications. (34)

This was followed by a 1997 Meeting in Denver (35) where a ten-point statement of principles included

- There must be no safe havens for those who abuse information technologies.
- Investigation and prosecution of international high-tech crimes must be co-ordinated among all concerned States, regardless of where harm has occurred.
- Legal systems should permit the preservation of, and quick access to, electronic data, which are often critical to the successful investigation of crime.
- To the extent practicable, information and telecommunications systems should be designed to help prevent and detect network abuse, and should also facilitate the tracing of criminals and the collection of evidence.

An action plan was agreed on that included

- Develop expedited procedures for obtaining traffic data from all communications carriers in the chain of a communication and study ways to expedite the passing of this data internationally.
- Work jointly with industry to ensure that new technologies facilitate our effort to combat high-tech crime to preserving and collecting critical evidence.

This mandate for co-operation with industry led to the Paris and Berlin summits of May and October 2000, and the Tokyo summit of May 2001, where industry representatives met with government representatives to discuss initiatives. Because of the disruptive technology of the Internet, and the associated costs accumulated by data collection and interception capabilities, the G8 acknowledged that it had to include industry within negotiations.

These industry-government summits concentrated primarily on four topic areas. Two, specific to the issues covered within this article include

Data Retention

To discuss issues associated with the feasibility of transactional data retention, and the degree to which these may facilitate the public safety mandate. This was met with firm opposition from industry particularly due to costs and data protection considerations. (36)

Data Preservation

To discuss problems associated with locating and identifying criminal communications that cross national borders, and the role that transactional data preservation can play in addressing those problems. This was met with scepticism, due in part to the challenges associated with identification of criminals (creating a user-IPnumber bind). (37)

Again the costs and effectiveness issues arise. Unless the design of systems can incorporate government interests then the costs will continue even as the effectiveness concerns abate; industry, however, appears resilient (at least openly) in designing systems that are embedded with surveillance capabilites, at least without subsidies. This is particularly difficult to do in a transnational manner.

The G8 is continuing its work, and lately has been quite open regarding its concerns about data protection regulations that limit access to transactional data. That is, by data protection regulation, ISPs are meant to delete or make anonymous any transactional data that they hold when it is no longer needed for network billing and efficiency purposes. One proposal from the UK law enforcement agencies promoted the idea of removing this regulatory requirement, and substituting a retention of all transactional data for seven years (one year at ISP, six more at a government site) (38). Further proposals have come forward from the EU Police Cooperation Working Party, requesting reconsideration of data protection regulations (39).

Again the cost and privacy concerns arise, as disruption by the technology continues. The costs of retaining transactional data are considered high, moreover because this data must also be stored and backed-up. The invasiveness of this data has given rise to significant concerns for data protection experts, who continue to argue against it because of the level of detail and invasiveness. (40) (41)

Council of Europe on cybercrime

Not entirely separate from the G8 process is the work of the CoE. Since 1997 this 43-member state organisation (and the observer states including the US and Canada) has been working on a convention on cybercrime. Only in April 2000 did it publicly release a draft (version 19), and since then has released four more drafts (as of June 2001, version 27 is the most current).

This convention has three intentions:

- harmonise substantive law across the member states,
- harmonise procedural powers, and
- create a standard for mutual legal assistance.

The process of development, however, has been fraught with controversy about exclusivity, and lack of concern for costs (42) and civil liberties. (43) (44)

While this convention does not require transactional data to be retained, in other ways its powers goes well beyond those proposed by the G8 in risks regarding costs and civil liberties. For example, it requires that signatory states have the following procedural powers (relating to this article),

> **Interception and real-time access to traffic data (Art. 21, 20)**
>
> Countries must either require intercept capabilities or allow for technical devices to do the interception (similar to Carnivore, presumably (45)).
>
> **Access to secured data (Art 19.4)**
>
> An ambiguous statement that states that authorities may require individuals who know how a resource is secured to assist in un-securing this resource. Although ambiguous, the UK Home Office stated clearly that RIP Act was justified as the CoE also required lawful access to encrypted data . 19.4 is thus ambiguously stating the case for GAK and self-incrimination.

Additionally, the mutual assistance regime set up within the convention fails to harmonise safeguards and protections usually associated with due process. There are not even consistent requirements for dual-criminality. As a result, countries can pursue criminals in other countries using techniques such as access to traffic data and access to secured data. This is so, even without the "crime" being a crime in the

country enacting the powers.

Just as the UK justified the RIP Act using the G8 and the CoE, industry and NGOs are also worried that this same rationale will be used in other countries, at least immediately within the CoE. These two initiatives do not consider the disruptive nature of the technology, the costs and the civil liberties risks are ill-considered, and similarly the clear possibility of circumvention. The momentum behind the CoE convention is practically unstoppable, however, particularly as there has been no wide consultation allowing for input that might well change the form or nature of the convention. Through the force of ideas, this convention on cybercrime could be signed as early as September 2001. Once this is done, national parliaments will have to implement the provisions in law with limited consultation again, naturally as 'it is required to be done', -- as the UK was the first to invoke. This Nuremberg defence may work; but sceptics will point that this may have been part of the plan all along.

Summary and implications for technology policy: technology *Acts*

We are still left with this idea of disruptive technologies. Owing to the disruptive technology, the policy habitat of traditional surveillance techniques needed to be updated to *maintain the status quo*. However, in updating these powers, greater powers were granted through access to more invasive data (such as transactional data, and/or the Carnivore problem) or to powers previously considered in direct conflict with human rights (access to keys and secured data); this was *necessary* and implicated by the disruptive technology.

However, *structural* issues arose. Old regulations such as the US Cable Act (and even CALEA) and Data Protection conflict with the new regulations or the new habitat; updates are naturally proposed, again because of the disruptive technology. Cost concerns and civil liberties became issues. These concerns led to reconsideration of even the new policies, as occurred in the Netherlands and Australia regarding ISPs and interception with respect to costs; and with Carnivore with respect to individual rights. Such an unfavourable new policy habitat was being proposed that the costs and client concerns prompted some industry actors to consider moving off-shore, giving rise to regulatory arbitrate, which is again enabled by the disruptive technology.

Faced with the threat of disruptive technology that allows industry to move off-shore and criminals to transact across borders with impunity, propaganda was needed to ensure that other countries adopt the same regulations. The G8 and the CoE have been active in harmonisation of procedural powers such as interception, traffic data, and lawful access to secured data. In attempting to create a new global policy habitat they are realising that it is easier to harmonise powers than to harmonise civil liberties and cost structures; as a result the new global policy habitat leaves civil liberties and costs behind. Yet the force behind the idea of international conventions on cybercrime may be enough to stabilise the new global policy habitat despite all these detracting features. The *force of ideas* of international conventions and agreements also leaves behind democratic process, through ambiguity and through the imposition placed on governments to change its laws *regardless of public consultation.*

Implications for national policies

As any new country moves towards considering *updates* to its procedural laws involving surveillance to deal with disruptive technology, this article aims to point to a few reasons to consider carefully the path, the articulations, and the measures.

***Updates* to *maintain the status quo* are not honest**

Surveillance within new technological infrastructure involves an new policy habitat, with new

repercussions regarding human rights and cost structures. The UK first stated that lawful access to secured data was not new; then realised that it was. Likewise, the US has stated for some time now that the CoE convention does not require changing any laws; they are now realising that this may not be the case. We are discussing new powers under new regimes, with new access to new data and new structures. While everything is almost the same, so much is different.

The choice between *technology neutral* and *technology specific* policy is not clear-cut

The US pursued specific regulations under CALEA and is facing a situation where they may need to be updated to meet requirements of new infrastructure. Some solace can be founding that at least there was a negotiated settlement, no matter how complex: the US policy is the only policy with a clear subsidy mechanism, even though it is insufficient. A *technology neutral* approach is dishonest as it ignores the differences in technological implementations, costs, and effects on civil liberties. Consider how Australia and the Netherlands did not even allow for subsidies, then realised that re-consideration was required for Internet infrastructure. If the choice is between simplicity and honesty, choose the road less travelled.

Negotiated settlements are ideal, but often they are neither *negotiated* nor a *settlement*

The UK invoked the CoE and the G8 as a justification for the RIP Act, despite the fact that neither the CoE or the G8 was at that time *negotiated*, or *settled*. Inviting all the interested players to the table is of course ideal; this the G8 and the CoE failed to do. Therefore avoid the temptation to invoke the G8 or the CoE, otherwise a national policy will be nothing but the representation of the force of ideas coming from these trans-national institutions, rather than being democratically designed and nationally decided. Sovereignty appears to be more ideal.

***Settlements* are not likely to occur**

The technology remains disruptive; it continues have the capacity for recalcitrance. Technology policy is as much about technology as it is policy; likewise social structures and technological structures maintain equal capacities of autonomy. Much as regulations and treaties may fail, technology may force renegotiations. We are dealing with a technological structure that appears to be changing at an increasing rate. As a result, settlements are contingent, not permanent. Even if attempts are made to control the outcome of technologies, it is rarely possible in a democratic state to control the use of technologies in ways that were not intended; the cryptography policy debates should act as a lessons learnt on this abstract issue.

Recognise regulatory arbitrage, divergence, and convergence within settlements

New regulations will collide with old regulations. The US is realising that CALEA and the Cable Act may well collide. Carnivore may also be in conflict with constitutional protections of the rights of the individual, or at least with ECPA. In Europe, the data protection regulations are on a clear collision course with the interests of retention of transactional data at ISPs. And GAK may collide with the European Convention on Human Rights.

The collisions may be favourable, but governments rarely deal with the Internet and technology in a manner that protects the rights of the individual. Rather, with fears spurred by issues such as child pornography, drug trafficking, terrorism, and hacking, old protections can easily be rationalised away. Yet we must realise: as much as these protections of rights are from an older time, these very same crimes existed in that time as well, and somehow we found it within ourselves to create those protections. Of course the technology is disruptive so we must question everything again, but particularly because the

technology also disrupts these rights as well, we cannot let our immediate doubts and fears get the better of us and our processes. We were once wise, we must remain so.

Technology may change our policy structures, the policy habitats, and so we develop new policies. We must recognise that these new policies involve new capacities, again because of the technology, and these new capacities may conflict with old values and older capacities. Finding a settlement within this environment is not easy, but a negotiated settlement is required. Otherwise we will not be left to *choose the outcome*, and closed processes through technology or trans-national agreements will do it for us.

Ian (Gus) Hosein is a Visiting Fellow in the Department of Information Systems at the London School of Economics. He is also a Senior Fellow in Privacy International, a London-based human rights group; a member of the Advisory Council for the Foundation of Information Policy Research, a UK-based policy organisation; and Technology Policy Advisor to Zero-Knowledge Systems, a Montreal-based privacy technology firm. More information is available on http://is.lse.ac.uk/staff/hosein

---

Endnotes

1 Armey, D. 2001. Letter to the House of Representatives: Privacy: For those who live in glass houses.

2 Electronic Privacy Information Center, 2000. Cryptography & Liberty 2000. Washington DC.

3 Reno, J. 1996. Law Enforcement in Cyberspace Address By The Honorable Janet Reno, United States Attorney General. Presented to the Commonwealth Club of California: San Francisco.

4 Hansard, House of Commons 6th March, 2000 (Second Reading).

5 Hansard, House of Lords 25th May, 2000 (Second Reading).

6 BCC, 2000. The economic impact of the Regulation of Investigatory Powers Bill: An independent report prepared for the British Chambers of Commerce. British Chambers of Commerce: London.

7 Hosein, I., A Discourse on Interests in Technology, Policy, and Surveillance. in The LINK Inaugural ICT 2000: Innovation, Delivery and Development conference. 2000. University of Witswatersrand, Johannesburg, South Africa.

8 South African Law Commission, 2001. Computer-Related Crime: Preliminary Proposals For Reform In Respect Of Unauthorised Access To Computers, Unauthorised Modification Of Computer Data And Software Applications And Related Procedural Aspects.

9 Council of Europe, 2001. Draft Convention on Cybercrime, version 27 with convention and Explanatory Memorandum. Strasbourg.

10 Peltzman, S. 1989. The Economic Theory of Regulation after a Decade of Deregulation. Brookings Papers on Microeconomics.

11 Hood, C. 1994. Explaining Economic Policy Reversals. Buckingham, England: Open University

Press.

12 Latour, B. 1991. Technology is society made durable, in Sociology of Monsters: Essays on Power, Technology, and Domination, J. Law, Editor. Routledge: London, England. p. 103-131.

13 Latour, B. 2000. When things strike back: A possible contribution of science studies to the social sciences. British Journal of Sociology. 51(1): p. 107-124.

14 Van Bakel, R.. How Good People Helped make a Bad Law, in Wired. February, 1996.

15 Steinhardt, B., Letter to Declan McCullagh and the Politech Mailing list: ACLU's Barry Steinhardt on CALEA, IETF, and wiretapping. 1999.

16 Smith Group, 2000. Technical and cost issues associated with interception of communications at certain Communication Service Providers. Report commissioned by the UK Home Office.

17 Whitley, E. and Hosein, I. 2001. Doing politics around electronic commerce: Opposing the Regulation of Investigatory Powers Bill. in Proceedings of the International Federation of Information Processing 8.2 Conference. Idaho.

18 National Research Council, et al., Cryptography's Role in Securing the Information Society. 1996, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, National Research Council. p. 676.

19 Industry Canada Task Force on Electronic Commerce, 1998. A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society. Government of Canada: Ottawa. p. 42.

20 Briceno, M., Goldberg, I. and Wagner, D. 1998. A pedagogical implementation of A5/1. Smartcard Developers Association.

21 European Telecommunications Standards Institute, 1999. Technical Specification Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful Interception Architecture and Functions (3G TS 33.107 version 3.0.0 Release 1999).

22 Blaze, M. and Bellovin, S.M. INSIDE RISKS 124: Tapping, Tapping On My Network Door. Communications of the ACM, 2000 (October 2000).

23 Murphy, L.W., Steinhardt, B. and Nojeim, G.T. 2000. Letter to the Chairman and Ranking Member of the House Judiciary Committee. American Civil Liberties Union: Washington, DC.

24 Beatson, J. and Eicke, T. 1999. In The Matter Of The Draft Electronic Communications Bill And In The Matter Of A Human Rights Audit For Justice And FIPR. http://www.fipr.org/ecomm99/ecommaud.html.

25 Morton, P. 1999. TMI sets precedent with U.S. deal -- Wins security clearance: Telecom firm agrees to wiretaps -- but not on Canadians, in The Financial Post.

26 King, N. and Cloud, D.S. 2000. U.S. Pushes to Resolve Debate on NTT-Verio, in US National Newspaper. p. pp. A2-A14.

27 Buuren, J.v. 2001. Dutch Government and ISP's Reach Compromise On Interception of The Internet, in Heise Online.

28 Brown, I. and Gladman, B. 2000. Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses. Foundation for Information Policy Research.

29 Gilder, G., Happy Birthday Wired: It's been a weird five years, in Wired Magazine. 1998.

30 Hansard 2000, House of Commons July 26 2000. 31 Home Office, 2000. Major Inaccuracies: British Chambers of Commerce The Economic Impact of the Regualtion of Investigatory Powers Bill Report.

32 Home Office, 2000. Myths and misunderstandings: Other Countries. Home Office.

33 Hughes, T.P. 1994. Technological Momentum, in Does Technology Drive History? The Dilemma of Technological Determinism., M.R. Smith and L. Marx, Editors. MIT Press: London.

34 Group of 8, 1996. Ministerial Conference on Terrorism: Agreement on 25 Measures. Paris, France.

35 Group of 8, 1997 Meeting of Justice and Interior Ministers. Washington DC.

36 Data Protection Working Party, 1999. Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes. European Commission: Brussels.

37 Clayton, R.. 2000. The Limits of Traceability. Cambridge University.

38 Gaspar, R.. 2000. Looking to the Future: Clarity on Communications Data Retention Law; A submission to the Home Office for Legislation on Data Retention. On behalf of ACPO and ACPO(S); HM Customs & Excise; Security Service; Secret Intelligence Service; and GCHQ.

39 Police Cooperation Working Party of the Council of The European Union, 2001. NOTE from : the Swedish delegation to : Police Cooperation Working Party, No. prev. doc. : 12855/1/00 ENFOPOL 71 ECO 316 REV 1Subject : Draft Council conclusions on the importance of considering the needs of law enforcement authorities when working out Community legislation. Brussels.

40 Data Protection Working Party, 2000. Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 - COM (2000) 385. European Commission: Brussels.

41 Data Protection Working Party, 2001. Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime. European Commission: Brussels.

42 European Public Telecommunications Network Operators 2001. Press Release: Telecoms Operators concerned by draft Cybercrime Convention.

43 Global Internet Liberty Campaign, 2000. Member Letter on Council of Europe Convention on Cybercrime.

44 Global Internet Liberty Campaign, 2000. Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2.

45 Privacy International and A.C.L.U, 2001. Letter of concerns regarding version 27 of CoE Convention on Cybercrime.

References

Armey, D. 2001. Letter to the House of Representatives: Privacy: For those who live in glass houses.

BCC, 2000. The economic impact of the Regulation of Investigatory Powers Bill: An independent report prepared for the British Chambers of Commerce. British Chambers of Commerce: London.

Beatson, J. and Eicke, T. 1999. In The Matter Of The Draft Electronic Communications Bill And In The Matter Of A Human Rights Audit For Justice And FIPR. http://www.fipr.org/ecomm99/ecommaud.html.

Blaze, M. and Bellovin, S.M. INSIDE RISKS 124: Tapping, Tapping On My Network Door. Communications of the ACM, 2000 (October 2000).

Briceno, M., Goldberg, I. and Wagner, D. 1998. A pedagogical implementation of A5/1. Smartcard Developers Association.

Brown, I. and Gladman, B. 2000. Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses. Foundation for Information Policy Research.

Buuren, J.v. 2001. Dutch Government and ISP's Reach Compromise On Interception of The Internet, in Heise Online.

Clayton, R.. 2000. The Limits of Traceability. Cambridge University.

Council of Europe, 2001. Draft Convention on Cybercrime, version 27 with convention and Explanatory Memorandum. Strasbourg.

Data Protection Working Party, 1999. Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes. European Commission: Brussels.

Data Protection Working Party, 2000. Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 - COM (2000) 385. European Commission: Brussels.

Data Protection Working Party, 2001. Opinion 4/2001 on the Council of Europe's Draft Convention on Cyber-crime. European Commission: Brussels.

Electronic Privacy Information Center, 2000. Cryptography & Liberty 2000. Washington DC.

European Public Telecommunications Network Operators 2001. Press Release: Telecoms Operators concerned by draft Cybercrime Convention.

European Telecommunications Standards Institute, 1999. Technical Specification Universal Mobile Telecommunications System (UMTS); 3G Security; Lawful Interception Architecture and Functions (3G

TS 33.107 version 3.0.0 Release 1999).

Gaspar, R.. 2000. Looking to the Future: Clarity on Communications Data Retention Law; A submission to the Home Office for Legislation on Data Retention. On behalf of ACPO and ACPO(S); HM Customs & Excise; Security Service; Secret Intelligence Service; and GCHQ.

Gilder, G., Happy Birthday Wired: It's been a weird five years, in Wired Magazine. 1998.

Global Internet Liberty Campaign, 2000. Member Letter on Council of Europe Convention on Cyber-Crime Version 24.2.

Global Internet Liberty Campaign, 2000. Member Letter on Council of Europe Convention on Cybercrime.

Group of 8, 1996. Ministerial Conference on Terrorism: Agreement on 25 Measures. Paris, France.

Group of 8, 1997 Meeting of Justice and Interior Ministers. Washington DC.

Hansard 2000, House of Commons July 26 2000.

Hansard, House of Commons 6th March, 2000 (Second Reading).

Hansard, House of Lords 25th May, 2000 (Second Reading).

Home Office, 2000. Major Inaccuracies: British Chambers of Commerce The Economic Impact of the Regualtion of Investigatory Powers Bill Report.

Home Office, 2000. Myths and misunderstandings: Other Countries. Home Office.

Hood, C. 1994. Explaining Economic Policy Reversals. Buckingham, England: Open University Press.

Hosein, I., A Discourse on Interests in Technology, Policy, and Surveillance. in The LINK Inaugural ICT 2000: Innovation, Delivery and Development conference. 2000. University of Witswatersrand, Johannesburg, South Africa.

Hughes, T.P. 1994. Technological Momentum, in Does Technology Drive History? The Dilemma of Technological Determinism., M.R. Smith and L. Marx, Editors. MIT Press: London.

Industry Canada Task Force on Electronic Commerce, 1998. A Cryptography Policy Framework for Electronic Commerce: Building Canada's Information Economy and Society. Government of Canada: Ottawa. p. 42.

King, N. and Cloud, D.S. 2000. U.S. Pushes to Resolve Debate on NTT-Verio, in US National Newspaper. p. pp. A2-A14.

Latour, B. 1991. Technology is society made durable, in Sociology of Monsters: Essays on Power, Technology, and Domination, J. Law, Editor. Routledge: London, England. p. 103-131.

Latour, B. 2000. When things strike back: A possible contribution of science studies to the social sciences. British Journal of Sociology. 51(1): p. 107-124.

Morton, P. 1999. TMI sets precedent with U.S. deal -- Wins security clearance: Telecom firm agrees to wiretaps -- but not on Canadians, in The Financial Post.

Murphy, L.W., Steinhardt, B. and Nojeim, G.T. 2000. Letter to the Chairman and Ranking Member of the House Judiciary Committee. American Civil Liberties Union: Washington, DC.

National Research Council, et al., Cryptography's Role in Securing the Information Society. 1996, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, National Research Council. p. 676.

Peltzman, S. 1989. The Economic Theory of Regulation after a Decade of Deregulation. Brookings Papers on Microeconomics.

Police Cooperation Working Party of the Council of The European Union, 2001. NOTE from : the Swedish delegation to : Police Cooperation Working Party, No. prev. doc. : 12855/1/00 ENFOPOL 71 ECO 316 REV 1Subject : Draft Council conclusions on the importance of considering the needs of law enforcement authorities when working out Community legislation. Brussels.

Privacy International and A.C.L.U, 2001. Letter of concerns regarding version 27 of CoE Convention on Cybercrime.

Reno, J. 1996. Law Enforcement in Cyberspace Address By The Honorable Janet Reno, United States Attorney General. Presented to the Commonwealth Club of California: San Francisco.

Smith Group, 2000. Technical and cost issues associated with interception of communications at certain Communication Service Providers. Report commissioned by the UK Home Office.

South African Law Commission, 2001. Computer-Related Crime: Preliminary Proposals For Reform In Respect Of Unauthorised Access To Computers, Unauthorised Modification Of Computer Data And Software Applications And Related Procedural Aspects.

Steinhardt, B., Letter to Declan McCullagh and the Politech Mailing list: ACLU's Barry Steinhardt on CALEA, IETF, and wiretapping. 1999.

Van Bakel, R.. How Good People Helped make a Bad Law, in Wired. February, 1996.

Whitley, E. and Hosein, I. 2001. Doing politics around electronic commerce: Opposing the Regulation of Investigatory Powers Bill. in Proceedings of the International Federation of Information Processing 8.2 Conference. Idaho.