Privacy and Cyberspace: Questioning the Need for Harmonisation

Gus Hosein, Privacy International

When speaking of contemporary policies and civil liberties, it is easy to sound dramatic. This may be due to civil libertarians' need for drama. I can easily say things such as "Never before have fundamental rights such as the right to privacy been under siege." It would not be an unfair statement, just a little loud.

Such a broad dramatic stroke fails to identify the subtlety in the policy decisions arising from governments, however. The travesties of justice are different today in our evolved democracies. The strategies are more subtle, often evading the notice of policy experts and certainly the general population, and non-discriminatory. This prevents us from easily painting the picture of a poor old minority who is being caged and surveilled unjustly by the Big Brother State.

The new policy environment is sophisticated. Surveillance is now wide-spread, yet its effects are not well known. As a matter of course, in almost all of our activities we are under surveillance. Yet the laws and policies implementing these practices are innocuous and inaccessible. The political processes that establish these processes are foreign to most. And the role that technology plays is poorly understood.

This discussion paper will look into the case of communications surveillance powers. In particular I will refer to the Council of Europe Cybercrime Convention, as well as the EU initiatives on communications data retention. The former is a treaty developed by the Council of Europe to ensure that all ratifying states implement similar powers of investigations, i.e. to harmonise powers of surveillance. Similarly, the EU is working hard to develop a regime for communications data retention, that regulates communications service providers (telephone companies, ISPs, mobile phone companies) compelling them to retain their customers' usage patterns for an extended period of time.

Both these programmes are part of what many would call a 'new security environment'. We need to understand the sophistication and subtleties of this 'new' policy environment. In particular, these policies are promoted under the perceived need for harmonisation. It is frequently argued that because the world has gone global, so must our laws. This is a dangerous form of logic, and this report will dispute such an approach.

On the Council of Europe

There is a clear logic for developing an international treaty on cybercrime. If our policy challenges are international in nature, and the infrastructure of trade and communications is also global, then, as the logic goes, we need global solutions developed by international fora. And these international fora are eager to be active and relevant.

The Council of Europe, the 45 member state international treaty-making body has laboured to create the Convention on Cybercrime since 1997. The CoE convention

on Cybercrime (ETS 185) consists of three components: a set of substantive crimes to be enshrined in law that includes hacking, child pornography, and copyright circumvention; a set of surveillance capacities that ratifying countries are expected to enable for use by their law enforcement authorities; and a regime for mutual legal assistance and extradition amongst ratifying countries.

Harmonising substantive criminal law may sound simple, but the reality is that every country has a different legal regime. One country may criminalize indecent speech; another may take another view of what qualifies as 'indecent'. For instance, in Japan the definition of child porn is significantly less restrictive than in most other countries. For the most part, the CoE disregards these national differences and demands standardization of law.

On the standardization of surveillance capacities, the CoE requires that all countries pass laws to empower their law enforcement agencies with new resources and tools. Key powers include the ability to permit law enforcement officials to gain access to data held on a computer, or to compel service providers to provide the ability for law enforcement officials to gain access to real-time communications and communications traffic data. Constitutionally, search and seizure powers differ across the world, and in particular, there are certain aspects of communications that are often safeguarded more carefully in some countries than other. Harmonising these powers ignores these differences in favour of a simplified and possibly unconstitutional regime in a number of countries.

The last component of the CoE convention is most alarming: the creation of a broad mutual legal assistance agreement. Cooperation is particularly problematic as the convention tries to do away with traditional concerns for dual criminality. In fact, it dissuades and sometimes prevents countries from refusing assistance to another country on these grounds. The convention may create situations where a country will be required to collect evidence on an individual without any contravention of domestic law.

The convention was drafted by a group of representatives from national departments of justice and home affairs, most notably Canada, France, Germany, the United Kingdom, and the United States. As a result of the formulation and consultation processes, the convention represents the interests of law enforcement agencies while all but ignoring privacy and civil liberties protections.

Drafted in relative secrecy from 1997-2000, a consultation process was opened in April 2000. Few changes were achieved in the consultation stage, despite the activities of representatives from industry and civil society. A number of international industry and civil society organisations opposed the convention on a number of grounds, including the formulation process, invasiveness, costs and burdens, lack of due process provisions, and the presence of ambiguous language within the body of the convention.

The CoE responded to these appeals by promising repeatedly that the opportunity for consultation and democratic participation would arise on a case-by-case basis at the national level at the time of signing and ratification. The U.S. deserves much recognition for being one of the only countries to respect this, in part.

The case of the United States

The U.S. was one of the only countries to actively solicit comments from industry and civil liberties organizations. This initiative was led by the U.S. Department of Justice. Similarly initiatives did not arise in other countries. The Justice Department reached out continually to companies, prompting the development of coalitions and responses that were then taken to future CoE committee meetings. The Justice department also solicited comments from and responded to concerns of non-governmental organisations in the U.S. and beyond.

Unfortunately, the legislative debate to date in the U.S. has been relatively limited. When the Convention was introduced to the Senate Foreign Relations Committee, the chair of the committee, Senator Richard Lugar, stated immediately that, along with other three other international treaties under consideration in that same hearing,

> "I commend the U.S. officials who have worked on these agreements for negotiating documents that command wide support. Some of these agreements are the product of years of dedication and patient negotiations. Prompt ratification of these agreements will help the United States continue to play a leadership role in international law enforcement and will advance the security of Americans at home and abroad."

For what it is worth, there is extensive uncertainty regarding the Convention coming from industry and non-governmental organizations, particularly on the lack of consultation in its development; and the U.S. Government is aware of this. This is what makes Senator Lugar's comments so defining of these dynamics in the 'new' security environment: even during the negotiation process the U.S. had tried to be open (and was the only country to do so, to my knowledge) but then during the ratification process, just when the U.S. procedure is most rigorous, the Chair of the Committee is calling for 'prompt' ratification and is bundling the convention with two other international agreements. International agreements and 'international leadership' are now reducing national deliberation.

It is unfair to focus on the U.S. All other countries that have ratified the convention held very little discussion within national parliaments. Rather, the debate was minimized by claims of 'international cooperation' and 'international obligations' and the logic of harmonisation. The problems with skirting through national dynamics will be discussed in detail in the next section.

Communications Data Retention

Data retention is the epitome of this new policy environment. After all, it is merely a policy that tweaks privacy law to require telephone companies to keep the records they hold on individual users. This appears small, innocuous because it regulates companies, not individuals. It seems benign, particularly as it is said to cause worry only to child pornographers, terrorists, and drug dealers. And it only appears to be a listing of telephone numbers you have dialled, and the addresses that you registered with the phone company. This is essentially the policy that the European Commission is pushing for adoption, under pressure from the Council of the European Union.

The Council of the European Union is the collection of all the ministers and presidents from within the EU. They have been pushing for an EU-wide agreement, a ‘framework decision’, on data retention. This would compel every member state of the EU to adopt data retention in national law. The current proposals vary, but generally the Council is looking for a retention period of 1-3 years.

Although it sounds so reasonable, it is dangerous but for subtle reasons. Simply put, data retention is an invasive and illegal practice with illusory benefits. And to date, the paths to data retention have involved illegitimate policy processes. This has generated a fragmented regulatory landscape in Europe, where some countries do require retention for 3 to 5 years, others have voluntary regimes, though some parliaments have rejected data retention outright.

Policies on data retention regularly conceal how sensitive this data is. It is often assumed that this is merely logging of telephone calls made and received. With the change in technologies, 'traffic data' ends up being a remarkable source of information, peering into the deepest details of an individual's personal life. This is often ignored, however.

Changes in markets and technologies have changed the types of data that are qualified as 'traffic data'. Current traffic data is substantially different from telephone traffic data of old. Traffic data now may disclose intimate details of the lives, choices, and preferences of individuals.

In the days of plain old telephone systems (POTS), traffic data was simple: numbers called, calling numbers, etc. This data was not considered overly sensitive or invasive into the private life of the individual, and therefore only required minimal constraint. Judicial warrants were not required, oversight was minimal in fact, and reporting of the use of such powers was frugal. An additional factor was that traffic data was stored by telephone companies and in turn was available for access by law enforcement agencies, while content was not: traffic data was available, legally less sensitive, and so, lawfully accessible.

Since then, however, there have been a number of advances in technologies and markets. The greatest changes can be seen in digital communications, such as through mobile telephony, internet access over telephone lines, wireless communications, and internet transactions. The constitution of 'traffic data' differs for each of these technologies. These changes in technology make it increasingly difficult to differentiate legally between what is communications 'traffic data' and what is actual communications content.

Another form of traffic data is that which appears at the application level of interactions on the Internet. This type of data includes the names of servers to which the user tried to connect, possibly limited to IP addresses but easily resolvable to servers such as aids.helpline.org, and in some cases unless carefully delineated by law, URLs such as http://www.usdoj.gov/ag/trainingmanual.htm may be collected through web proxies and treated as traffic data. Monitoring the DNS traffic from a home connection will inform upon much of what the people inside may be doing.

Data mining can provide sufficient information to draw a map of human relationships and movements. When we keep track of all activities of any given individual while she is on-line we are able to see every resource with which she came into contact. When this information is collected over a period of time, we are able to track common habits but also 'suspicious' activity. Asking for all of the traffic data of an individual for a four week period in order to investigate a crime is the equivalent of having had an investigator track every movement of a suspect for that given month, watching which bookstores she entered, what documents she looked at, what homes she visited, and who she spoke with. And consider the non-suspect individual: she must conduct her on-line affairs knowing full well that in the eventuality that the State or some other entity has an interest in her, all of her activities are being recorded for future analysis.

Increasing the amount of information available to parties in an investigation of any type does not necessarily lead to more certainty. In fact, the gains *may be* illusory. Communications service providers, especially broadband providers, are dealing with immense amounts of data through their pipelines. The computer systems that are collecting this information inherently lack accuracy and reliability. This lack of accuracy might lead to in-depth investigations of the behaviour of innocent users, just because some bits are missing from the ISP records.

We often presume that traffic data is immediately useful, and that retention will have only positive effects on the conduct of society, civil liberties concerns aside. The illusion of benefits to security must be offset with some realities: that traffic data does not easily link to individual conduct, this policy is linked with the increased identification requirements, and there are significant technological and financial ramifications to this policy.

The costs of retaining data can be prohibitive, and the amount of data therefore differs based on the market structure, the form of services provided, amongst other considerations. Free-ISPs may collect caller-ID information, but they do not have credit card details to verify the information of subscribers that other providers have. Individuals who run wire-less routers are sharing their internet connections with others in their neighbourhood, while the ISP that provides the fixed line service is not likely to know any better, nor will the individual have a recorded log of such activities. The market structure is sufficiently complex that it is hard to imagine a one-retention-policy-fits-all could ever apply, even within the same sector, e.g. ISPs, or mobile-telephony, or VoIP providers.

To retain this data solely for law enforcement purposes is a significant cost that will be incurred by all service providers, and this burden will be shifted to the consumer. The cost is not just storage-related, however; it is also about granting access to all this data upon request. According to a representative from America On-Line (AOL), speaking to UK Parliamentarians on the idea of 1 year voluntary retention, a retention policy would involve storing 100 CDs a day, leading to costs of £40 million to set up the system and £14 million in operating costs.

It is possible that the side effect of this policy is to enforce 'reasonable' conduct. According to the London Internet Exchange, "the ability to trace actions back to their source will, in itself, discourage unreasonable behaviour." If the by-product of retention is that it discourages unreasonable behaviour because of the fear of the recording of all of our conduct within the Information Society, then it will have

significant effects on the ways in which we conduct our lives. If a mobile phone company is required to record all phone transactions for three years, individuals may be less likely to use the phone for making 'private' yet completely legal calls. If all transactions with services on-line are to be recorded regularly for the purpose of ensuring traceability in case of crimes, the purpose may be to promote 'responsible' behaviour and to minimize transactions with pornographic or other 'controversial' content. This is when retention starts to interfere with our general conduct, and other civil liberties apart from privacy alone.

Any retention of traffic data should be specific to an individual and a case. Personal data should never be collected 'just in case', but only if there is a specific reason, i.e. in law enforcement, if there is specific, reasonable suspicion against a specific individual. The retention of this information under policy envisioned by the Framework Decision is surveillance as a result of state action, and it thus fails the limits on state action as under European law.

The data retention regime envisaged by the EU, and now appearing in various forms in Member States, is unlawful. Article 8 of the European Convention on Human Rights (ECHR) guarantees every individual the right to respect for his or her private life, subject only to narrow exceptions where government action is imperative. Interference with the privacy rights of every user of European-based communications services cannot be justified under the limited exceptions envisaged by Article 8 because it is neither consistent with the rule of law nor necessary in a democratic society.

The indiscriminate collection of traffic data offends a core principle of the rule of law: that citizens should have notice of the circumstances in which the State may conduct surveillance, so that they can regulate their behaviour to avoid unwanted intrusions. Moreover, the data retention requirement would be so extensive as to be out of all proportion to the law enforcement objectives served.

In establishing privacy laws and directives, and even in the process of developing the Information Society throughout the 1990s, the European Union often acted in a manner that promoted the rights of the individuals. Now the EU risks heading in the opposite direction.

And it is being spurred to action by inappropriate forces. The main proponents of the European standardising policy are France, Sweden, the UK and Ireland. Why are Ireland and the United Kingdom seeking this policy at the EU when neither country has an open mandatory data retention regime at home? In fact the opposition to these policies, when deliberated within national Parliaments, amongst industry and civil society, and monitored by the media, is remarkably high in these Member States. But these governments are pursuing this policy through the EU. Using the European Union as a forum for policy laundering is unacceptable.

The case of Ireland

In an effort to reconcile its policy laundering tendencies with the lack of a national law on retention, the Government has succeeded in quietly implementing data retention into its Criminal Justice (Terrorist Offences) bill (now an Act).

This Bill itself was first introduced in December 2002, and made slow progress. It was introduced to the Seanad in February 2005, and in Committee stage, retention was added to the bill. The bill was passed shortly afterwards, after limited debate on the measure.

The amendments call for data retention at all fixed line and mobile phone service providers for 3 years.

The purpose behind the amendments was to, according to the Minister for Justice, Malcolm McDowell, "give a solid basis in Irish law to the retention of communication data and to protect people in a way that is not done at the moment." He argued that this information "is an essential aid .. in the fight against crime and in combating terrorism and, ... the protection and security of the State."

The Minister argued that this information is generated by phone companies for charging purposes. Although there are laws that permit access to this information by law enforcement agencies, there was previously no legal requirement to retain it.

In April 2002, the Minister for Public Enterprise issued directions at the request of the Minister of Justice to oblige communications service providers to retain data for at least three years. The Government argued that this was a necessary temporary bridging of the gap between the transposition of the EU Directive on privacy and electronic communications into Irish law. This is misleading because the 2002 Directive did not require data retention.

The transposition into law was approved in March 2002, and providers were required to retain the data for the full three years. The legislation was never published, however, as they were subject to a "gagging order" requiring that the service providers not disclose the fact of the directions were made. Eventually the details were leaked, and the documentation accessed under the Irish Freedom of Information Act.

The results from the FOI request by Karlin Lillington of the Irish Times finds that the Government has long been aware of the dubious legal standing of retention in Ireland, and so should have rectified it at an earlier date. Instead, they waited for a strategic moment in 2005.

In January 2005 the Irish Data Protection Commissioner, Joseph Meade, issued an order to service providers to erase data that is more than six months old, as of May of 2005. The Commissioner argued that the temporary directions were in force for too long without legal mandate. The Government interpreted this as a requirement to move forward with primary legislation calling for retention. The Minister of Justice argued

> “Without some contrary action being taken, the initiative by the Data Protection Commissioner would, if the telecommunications companies accepted its validity, seriously undermine the ability of the Garda Sý´ocha´na to investigate criminal activity, including terrorism and to protect the security of the State.”

According to the Minister of Justice, the Attorney General also advised that the Data Protection Commissioner may have been acting outside of his powers.

Shortly afterwards, in response to the case of Director of Public Prosecutions v. Murphy on January 21 2005 the Attorney General argued that in order to ensure the admissibility of telecommunications data as evidence, retention should be placed on legal standing through primary legislation with safeguards against the possible misuse of the data.

The Government contends that service providers need this legislation because of a current conflict of obligations. The Government believes that service providers are compelled to retain data for 36 months under section 110 of the Postal and Telecommunications Act 1983; but the Data Protection Commissioner's notice required them to delete this data after six months.

On January 27 2005 the Minister of Justice announced his intent to comply with 'international obligations' and to help fight terrorism through introducing a policy on data retention.

> “I indicated that one of the things I propose to do with regard to Committee Stage amendments is to deal with the question of data retention in so far as it is necessary to underpin the fight against international terrorism. It is desirable that our law on this matter should be beyond debate. It should never be a question of differing interpretations, let us say, for example, between the Data Commissioner and the Minister for Communications, Marine and Natural Resources, as to what is or is not a legitimate use of the power to require telecommunications companies to keep records of communications so that they can afterwards be examined in the context of criminal investigations. The Bill is largely to do with the introduction of provisions into Irish law to extend our law in an adequate way to deal with international terrorism, as is required by various international instruments to which we are party.”

Such international obligations do not exist, however, despite the great attempts by the Irish Government to create these international obligations in the first instance.

With the court decision and the decision by the Data Protection Commissioner, the Government felt compelled to act. It also felt it should act swiftly, because of the Parliamentary timetable. With the May deadline imposed by the Data Protection Commissioner, and with St. Patrick's Day and the Easter Holidays, the Minister for Justice argued that

> “If I were to provide for all of this in a separate Bill it would be doubtful if I could meet the 5 May deadline. I can say for a certainty that it is cognate to this Bill in that any effort to monitor international terrorism or to counter it would fall flat on its face if on 5 May, telecommunications data was to become erased automatically after six months. Any effort to look back over a reasonable period, which is 36 months in the Government’s view, would become impossible if the telecommunications companies

> accepted the validity of the directive they have now received from the Information Commissioner."

So it was decided, apparently 'after long consideration' that the Government should "take advantage of this legislative vehicle to insert these new provisions into our law."

The Government accepted that its strategy to launder this policy through the EU was facing some challenges. As the Minister of Justice admitted,

> "I had hoped to avail of the European basis for making rules in this area but it did not materialise."

When it held the presidency of the EU the government pushed the 'framework decision' that would compel all service providers of all types (telephone, mobile, internet, etc.) to retain data for up to three years. As mentioned above, this initiative was also pushed by the French, Swedish, and British governments. In the summer of 2004, however, the European Commission decided to intervene in this Council process arguing that it was a first pillar issue since it deals with industry rather than just policing, and thus internal market considerations were required. This slowed down the initiative.

The Minister of Justice found this to be a frustrating situation, however.

> "The framework decision ran into difficulties with the European Commission. It is difficult to understand exactly what has happened to the framework decision but it appears that the commissioner is of the strong view that data retention should be dealt with in the first pillar of the European Union treaties, that is the same pillar as data protection and communications. While it is probably safe to assume that the framework decision in its present form is moribund, we do not know what proposal will take its place. The Commission has apparently promised a first pillar on data retention but, whatever the outcome, it seems that any EU initiative will not now take place in a time frame that would allow me to meet the May deadline set by the Data Protection Commissioner. Faced with that I must act now before 5 May. There is no EU cavalry coming down the hill to help me. I must sort out this conflict."

The 'EU cavalry' is facing increased trouble, so having failed at the strategy of policy laundering the Minister of Justice relied on obscuring the policy to minimize debate.

When the debate had moved back to the lower House, the Justice Minister lamented this situation.

> "Deputies may be aware that an EU framework decision on data retention was published last year following the terrorist bombings in Madrid. The decision, which arose from a declaration on combating terrorism, instructed the European Council to adopt an instrument on data retention by June 2005. The framework decision, which was a response to the declaration, encountered some technical

> difficulties during the negotiations on it. It is doubtful, regardless of whether the framework decision or an alternative instrument is eventually agreed, that it will be possible to adopt any instrument by June of this year. It is normal to await agreement on such international instruments before preparing implementing legislation. If the Data Protection Commissioner had not acted as he did and if the EU had not encountered the difficulties I have mentioned, different options would have been open to me."

Instead, they concealed the policy in an old bill just before it was to be passed, with little debate.

In the last minutes before the amendments were approved in the lower house, one dissenting voice raised concerns regarding the lack of debate. According to Sinn Fein TD, Aengus O'Snodaigh:

> "I particularly oppose the new section which the Minister has introduced concerning traffic data retention. This is not only because it infringes the right to privacy, has fundamental and significant human rights implications and the Human Rights Commission has not had an opportunity to give its opinion on this and other amendments, but also because it is another instance of the Government making an illegal practice legal retrospectively, similar to the Health (Amendment) (No.2) Bill. I oppose it because of the manner in which the Minister is inserting these sections into this legislation by stealth at a late stage, which is anti-democratic.
>
> My office never received the amendments and on inquiry was initially told that they would be published only this morning. That was misinformation. They were not available electronically. They were not in the internal mail this morning and the General Office informed me they were not circulated at all. They had got stuck in that office whose staff did not seem to be aware they had them. I cannot speak for other Deputies but I had only two hours in which to peruse these proposals. Human error or not, this is not acceptable. The debate should at the very least have been postponed on that basis as well as on the basis of my other points. ...
>
> The Minister also said that the legislation would be subject to the normal rigours of passage through the Oireachtas, including Committee Stage scrutiny. The Minister misled the Dáil and possibly also the Seanad and the public in this regard. I do not accept his reason for introducing these amendments at this stage. The safeguards in which he places great faith are not adequate."

Shortly thereafter, the amendments were passed.

The Government argues that retention occurs anyways, because phone companies need to this data.

> “If there was no retention of this type everybody could say they never made, say, 5,000 telephone calls during that month. The telecos have to be in a position to say that one did made the calls and these are the telephone transactions one made at a particular time. They have to amass the data even from a defensive point of view, otherwise every bill would be disputed. People would say their bill looked steep and that they did not use their phone often and challenge the telecos to prove the contrary. The telecos have to be in a position to say that one’s telephone was used X number of times for international calls and X number of times for local locals and to show the times and dates.”

As such, all that is considered in these debates are the logs of the phone calls, not the more problematic information such as location data, even though it is implicated within the law.

This is yet another case of a law on communications data retention being passed without careful consideration of the nature of the data being retained. Without understanding the nature of the data, which could include our general movements over a span of three years, it is harder to understand how invasive this practice is.

On the period of retention, the Government was unwilling to accept that 6 months is sufficient, as decreed by the Data Protection Commissioner. According to the Minister of Justice,

> “The issue is first, whether that kind of material can be stored indefinitely and if there is an increased cost and, second, if the Data Protection Commissioner arrives at a view regarding, say, a six-month period but without a statutory authority, what would be the implications for the investigation of serious crime from my perspective? I must ask myself that question. The Commissioner is entitled to his view but I have to take a different view into account. All in all, I believe that 36 months is an appropriate period. I do not believe there is much difference between six months and 36 months. If my privacy is in some way infringed by having the information on file or on a hard disk for six months, I do not regard it as a great reassurance to me to know that it is erased after six months rather than 36 months. It would not change my sense of wellbeing to know that an additional period of time had not elapsed before the data was destroyed.”

He later continues,

> “In my view whether the period is six months or 36 months makes very little difference. I do not think that with these safeguards in particular it is a matter of great importance. I have always been unimpressed by the arguments that material deleted after a period of time increases one’s dignity and rights as a human being. This notion that if, for instance, I gave a fingerprint which is destroyed after some specified period of time does not really worry me. I am aware of a contrary opinion which worries about a big brother state

> amassing information indefinitely about everybody. The 36-month period is what the Government favours."

This regime will certainly be questioned as to its compliance with the European Convention on Human Rights.

The purposes for retention are ever growing, while the purposes for access are well beyond those, and that this is an act of policy laundering intent on circumventing and ignoring national deliberative processes.

The situation in the UK is equally interesting, though I will not go into full detail at this moment. After much deliberation, the UK Government managed to get a 'voluntary' regime of data retention, where companies would voluntarily retain data that is only collected in the first place. Additionally, varying types of data would be retained for varying amounts of time. In a sense, it is a much more evolved policy on data retention. The EU Framework, and the debates in Ireland, lack this sense of sophistication.

Chilling Speech through Mass Surveillance

The disclosure of personal information is ever-increasing, and the investigations of conduct on-line are also on the rise. A number of cases have emerged world-wide where courts have ordered the disclosure of the identities of internet-posters, e-mailers, and mere users. Frequently data is also seized, servers are shut down. Copyright rules that require the release of subscriber information of suspected file sharers only makes matters worse for the protection of personal privacy. To date, it is estimated that over 2400 subpoenas have been filed by the Music and Recording industry in the U.S. alone. This is for access to account information, and in some cases, other forms of data held by ISPs.

One of the most interesting cases arose in the United States District Court for the Eastern District of Pennsylvania, between BMG Music and 203 anonymous and unrelated individuals. The recording industry claims that the defendants have made copyrighted music available on their computers for download by others on the Internet. The challenge, however, is that in some jurisdictions, particularly in the U.S., anonymous speech is constitutionally protected. As such, a subpoena for the subscriber information is subject to qualified privilege. Arguably, ascertaining the identity of these individuals would have a chilling effect on anonymous speech: Internet speakers would know that they could be identified by persons who merely allege wrongdoing, without necessarily having any intention of carrying through with actual litigation.

This same logic would apply to access to any form of data held on ISPs. Yet, we continue to develop international standards and practices that compel service providers to disclose to law enforcement authorities the identity of individuals who are using communications services, or to monitor the users of a service. This disclosure does not end with subscriber information; it also includes traffic data.

Access to this traffic data is problematic from the perspective of privacy protection. According to the European Commission's expert party on Privacy and Data Protection, traffic data and modern communication infrastructures are increasingly sensitive.

> “A feature of telecommunications networks and of the Internet in particular is their potential to generate a huge quantity of transactional data (the data generated in order to ensure the correct connections). The possibilities for interactive use of the networks (a defining characteristic of many Internet services) increases the amount of transactional data yet further. When consulting an on-line newspaper, the user 'interacts' by choosing the pages he wishes to read. These choices create a 'click stream' of transactional data. By contrast more traditional news and information services are consumed much more passively (television for example), with interactivity being limited to the off-line world of newspaper shops and libraries.”

This growth of data is now worsening due to other policy developments.

The Council of Europe and the EU’s policies permit the mass surveillance of individuals, and enable the sharing of this personal information across borders. Mobile phone internet data may now be transferred between French authorities and U.S. authorities investigating criminal activity. The list of IP addresses that interacted with a server in the United Kingdom are retained systematically by the service provider, and handed over to local authorities with minimal restraint, and may be shared with foreign authorities with even less due process.

The general public appears relatively unaware of these regimes for mass surveillance. When the first cases of copyright infringement eventually break through into the public domain, however, and a Briton’s internet usage over a period of years is disclosed in a court to show how an individual shared a song with users around the world, and the investigative data is shared with claimants in the U.S., only then will we get a full grip of this dire situation. Then a number of cards will fall, as users become aware of the level of surveillance out there, the internet service providers continue to deal with mounting regulatory burdens; it is possible that all that is good about cyberspace may disintegrate as our interactions become chilled by surveillance and our economies harmed by state compulsiveness.

Questioning Harmony?

The logic of international co-operation and harmonisation is truly compelling. A diversity of rules in the world makes the world more complicated and fragmented. The new security environment must deal with trans-border flows of data and technologies. Therefore international solutions are necessary. And we need to harmonise our policies across borders at the same time.

At a recent roundtable of legal experts and academics, successive speakers repeated the need for harmonisation in order to deal with cybercrime. Some of the speakers were actually prosecutors in a past life and explained the challenges in dealing with cases of malicious hacking. Yet they spoke of harmonisation as a simple and necessary process, so I decided to intervene and ask a simple question: maybe we should not presume automatically that harmonisation is the ideal outcome? The silence that filled the room was one of shock, and horror. After a deep breath everyone continued to talk with some trepidation, wondering if they had really heard what they had heard. I imagine that those who encounter aliens on dark desert highways react the same way.

In this new environment, if it is indeed new, let alone a settled 'environment', we presume safely that the more we cooperate and the more we harmonise our rules, the better things are. We forget that every country has its own rules not by some freak of nature but rather through a legislative process. In some countries the legislative process is more thorough than others, but that is another point for another time.

Where there is a legislative process, it is quite possible that different results emerge. Just in the U.S. alone the laws vary greatly between states. In the EU, the situation is similarly fragmented. From alcohol regulations to driving licences, from tobacco taxes to water quality standards, the established rules are all specific to each political system. After all, this is the nature of democratic systems: the process is the way through which rules are decided. Local interests influence the outcomes of decisions, and they are debated within parliaments and congresses.

What we are now seeing in this new environment is the rise of the benign 'international', and the compelled need to co-operate, harmonise, and standardise. Congresses and Parliaments are not debating at length key issues because of their seemingly benign nature as international standards. Governments pursue policies internationally in order to establish standards that they can then bring home as seemingly benign international instruments. Governments speak of the need to harmonise as a reason to change national law, and this goes against all the prior deliberation that may have occurred. That is, the U.S. Congress considers the ratification of the CoE convention as trivial; the Irish Government is hailing the EU cavalry, and the British Government is likely to appeal to the trend in 'harmonisation' to undo its existing contract with British ISPs and telcos on voluntary data retention.

We must stop seeing harmonisation as a good in itself. It is in fact quite an illiberal practice. It says that 'because our neighbour has this policy, so must we'. This means that our neighbour is making our decisions for us. Or in the realm of globalised-policy-making, it means that international institutions are deciding policies that are to be implemented without scrutiny in national parliaments. If you are even more cynical, you would instead say that Governments are pursuing policy in international institutions to then bring them back home under the guise of an international obligation, rendering Parliaments and Congresses powerless to object.

This is not happening for all policy-issues. Great controversy reigns over international policies on trade, accounting standards, the environment, working standards, and human rights. Yet in the realm of investigative powers, increased surveillance, and the reduction of privacy, little controversy arises in many of these international institutions. Those around the table agreeing on data retention and investigative powers do not invite contention or controversy. Often those who would bring such things are left outside, notably industry and non-governmental organizations. Apart from the exceptional case in the United States with the positive work of the Department of Justice, little else has arisen in the form of positive engagement on these issues.

Until positive engagement becomes the norm as Governments negotiate international rules on surveillance and other activities that have the potential to

chill cyberspace, we must cease to seek harmony and instead revel in our diversity.

Gus Hosein

June 2005

About the Author

Gus Hosein is a Senior Fellow with Privacy International, a London-based non-governmental organisation. At PI he directs the *Terrorism and the Open Society* Programme, and is the co-ordinator of the *Policy Laundering* Project in association with the American Civil Liberties Union and Statewatch. He is a Visiting Fellow in the Department of Information Systems at the London School of Economics and Political Science. At the LSE he lectures on the politics of the Information Society, technology, regulation, law, and policy. He holds a PhD from the University of London and a B.Math from the University of Waterloo. For more information please see http://personal.lse.ac.uk/hosein