2007

Internet Governance and Privacy

Dr Gus Hosein

rits nupef rits IDRC CRDI

Internet Governance and Privacy

Dr Gus Hosein

VISITING FELLOW

Information Systems and Innovation Group, the Department of Managment

The London School of Economics and Political Science

http://personal.lse.ac.uk/hosein

After more than a decade in this field I can finally conclude that privacy is confusing. Perhaps 'confusing' isn't the right term, but it certainly is not a clear-cut domain. Unlike other domains such as the regulation of online content, the digital divide, or even environmental policy, the field of privacy consists of a constantly changing set of actors and institutions, technologies and opportunities, alignments and coalitions, and of course, threats.

As an academic, I am supposed to use such levels of analytics to describe the complexity of a policy field. But as someone who has worked in the privacy world as an advocate I can also conclude that the right to privacy also confounds many, and sometimes even me.

Consider the latest controversies that my colleagues and I at Privacy International had to consider, in the two weeks around the writing of this paper:

• we filed a legal complaint to the Ontario privacy commissioner claiming that the city of Toronto's plans to install over 10,000 cameras across its transit network had not sufficiently passed the 'necessity test'. We provided the privacy regulator with the results of studies from the UK and Berlin that showed that CCTV cameras were not as effective as promised. A media storm arose around the story, which was certainly a nice result particularly since the funding for this surveillance plan was approved with little public debate. Despite all of this, however, we have been receiving a number of angry emails from Canadians complaining that their right to safety is more important than the selfish right to privacy.

• in the UK we have been working with a number of other organisations trying to get a change in the current practices for the collection of DNA samples from suspected criminals. The UK has the world's largest DNA database, where anyone who is arrested for a crime has his or her sample taken for addition to the DNA database. We have long argued that this is a problematic practice because even if someone is acquitted, the DNA profile remains on the database. Additionally, the profile of one individual can be used to identify a number of other individuals because of 'familial searching', resulting in many more millions of people being placed on this database. In October 2007, news emerged

that a masked rapist was finally tracked down 14 years after the crime, not because his DNA was on the database (he had otherwise lived a crime-record free life) but because the DNA of a family member was on the database.

• in the U.S., the Bush Administration managed to push a law through an otherwise-hostile Congress that allowed the National Security Agency to intercept communications that happen to pass through the U.S. Because of the history and design of global telecommunications, much of the world's traffic actually passes through networks owned and operated by U.S. companies. The law permits the NSA to gain access to records without the need for a court order. Many commentators in the U.S. saw this as a practical solution because, they argued, U.S. constitutional rights apply only to U.S. citizens and residents, and the communications of other countries' citizens that happen to be passing through the U.S. and are under the jurisdiction of U.S. law enforcement agencies. It is entirely possible that most communications from Latin America to Europe or Africa pass through 'U.S. networks'. It is quite likely that webmails from one French citizen to another French citizen, Brazilian to another Brazilian, etc., go through U.S. networks because they go through the U.S. servers of companies like Google and Microsoft. Yet awareness of this legal development outside of the U.S. is low, and it is not as though foreign governments or officials have any jurisdiction over U.S. networks anyways. Meanwhile there is intense but localised discussion within the U.S. policy circles, but a highly political dynamic results in Congress approving the legislation.

In the face of odds and facts like these, privacy advocates are expected to advocate a consistent line on such a controversial and complex topic. And in all these stories, the privacy advocate comes off looking like the wrongdoer. It is not my purpose in this paper to find some sympathy for the privacy advocate. Rather, my goal is to show that although privacy is a highly controversial and complex field, its complexity and the controversies is what makes it so important. In fact, my real point is that this is a rich policy environment that deserves greater attention from researchers, students, and policy-makers in internet governance.

The richness of dynamism of this field comes not only from the privacy horror stories. We are starting to see what happens when privacy is poorly considered, or when public debate and policy deliberation is stifled in the name of security. We've seen this in the wider world of public policy already.

It comes as little surprise that there have been leaps and bounds in recent years for the advancement of security. The policy environment has promoted advances in surveillance law, policies, and technologies. Finally we are also starting to see the failures of these policies too. Vast amount of funds and resources have been expended on new technologies under the promise that they would work, and now we realise that this may not be the case. Referring back to the cases above:

• numerous studies show that there are serious problems with CCTV infrastructures, and in fact CCTV policy-making tends to be driven by political bravura rather than need. For instance, in the Canadian case, a new Federal government wanted to show its resolve on security after taking office so rushed through funding for securing transit networks across Canada without even thinking about appropriate uses of those funds.

• the collection and retention of DNA has resulted in 75% of the young black male population being on the database; even a child as young as 9 months old, and over 10,000 children are now on this criminal database, causing politicians of all political stripes to call this policy into question. In fact, the earlier policy of the government was to seek a national DNA database by stealth by slowly getting every individual on the database; but now it is being forced to pull away from this position after mounting public concern.

• the Bush Administration has now admitted that it oversold its case for the change in U.S. policy on interception when it tried to point out that recent arrests in Europe were only made possible by the interceptions in the U.S., when this was not in fact the case.

The world is now a different place after the prior rush-to-legislation that we've seen previously, and policies are being debated more thoroughly. Facts are no longer taken at face value and we are now questioning a policy's effectiveness.

Despite this turn of events in other policy arenas, internet governance discussions continue to ignore privacy. Discussions at UN summits always contain language about terrorism, crime, and security, and always ignore the problems in the emerging policies, and rarely consider the challenges of ensuring privacy. This is surprising considering the number of policy options and alternatives that we could be discussing, if only a discussion was taking place. Of course privacy is complex and controversial. But without engaging on these issues we are failing to even have the necessary debate.

There are a number of likely answers to this conundrum as to why internet governance summits ignore privacy. These include:

1. geopolitics of getting countries to agree on privacy when it is arguably only a Western phenomenon

2. lower priority of privacy in the face of security

3. lack of available policy instruments to throw at the problem

The rest of this paper will show that these are merely excuses for not taking privacy seriously.

I. Privacy as a Western value

At conferences and meetings around the world I am often taken aside by a non-Westerner who tries to explain why I am naive to believe that privacy is a universal right. He or she often explains how his or her society does not see privacy as an important issue and that privacy is a selfish right that has no place in communalistic societies outside of the West. To date I have been given this exact same speech by citizens of: China, Egypt, India, Iran, Japan, South Korea, Thailand, and Zimbabwe. I list these countries not as some form of global-representation polling but rather to show the commonalities in this stated feeling about privacy despite the differences amongst these nations, states, and societies. Speaking on behalf of their people, I was told that these countries have no need or interest in privacy law.

I usually get quite frustrated in these situations. I find it unfathomable, as a Western-born and raised male, that one could have no interest in privacy. Whether it is privacy from one's parents and friends through one's youth, the selective disclosure of personal information to friends as we build up the trust relationships, the development of one's sexuality and the awkwardness and evolution that surrounds it, or more generally the psychological need for seclusion from time to time; I am so ignorant of the world that I can not understand whole societies not needing these processes. But I must be forgiven for my assumptions about the state of humanity because I am not a sociologist nor an anthropologist.

I am, however, a student of politics and technology. Even the classic political mind would look at these disparate states and societies and ask how a political system can survive without the right to privacy? The rights to organise to petition one's government relies on the ability of those petitioners to organise against a possibly antagonistic state. This is exactly why, for instance, in the U.S. the right to privacy took a giant leap forward during the civil rights movement in the 1960s when the state of Alabama demanded that all organisations, including the National Association for the Advancement of Colored People (the Reverend Martin Luther King Jr's organisation) disclose their membership lists to the government; the U.S. Supreme Court recognised that political movements require some form of privacy and rejected Alabama's right to know the political tastes and affiliations of its citizens.

Every political system, even those with a single party, will face petitioners and these petitioners need the space and the autonomy to organise and act without being under the watchful eye. Student groups in Iran, opposition parties in India, Egypt and Zimbabwe, migrants in Thailand, and religious institutions (or cults) in China may feel some need for privacy.

Such a need for autonomy is endemic to politics, even if not to culture. This is why privacy is recognised in Article 12 of the Universal Declaration of Human Rights, a document drafted by individuals from around the world and signed by states of all types of cultures. Rhoda Howard and Jack Donnelly declare the purpose for its inclusion within the Declaration:

"The right to privacy (Article 12) even more explicitly aims to guarantee the capacity to realize personal visions of a life worthy of a human being.[1]"

I am not trying to be imperialistic by arguing that because it is there within that document and thus it must be enforced around the world. Rather, I am merely stating that it is there because it was recognised as necessary by people from around the world.

I am willing to accept that I may not yet have won this debate because different countries and their cultures must be able to choose their own paths. But as I mentioned previously, I am also a student of technology. While cultures may vary

1 Rhoda Howard and Jack Donnelly, in Micheline Ishay's The Human Rights Reader: Major Political Writings, Essays, Speeches, and Documents from the Bible to the Present. London: Routledge, 1997.

we are seeing increasingly that technologies are not. The same technologies that are implemented in the U.S. and in Western Europe are seeing themselves implemented in Africa, Asia and Central Europe. Yet the same risks in implementing these technologies in the West do not disappear just because they are being implemented in different cultures. Data-breaches, poor policy deliberation and the resulting waste of resources is possible anywhere. So when the U.S. implemented vast fingerprinting regimes at its borders without adequate policy deliberation and are now realising that vast amounts of funds have been wasted on a scheme that does not work effectively and is insecure; are we saying that these same troubles will not befall Japan as it embarks on a path to follow the U.S. using the same political rhetoric of protecting ones' borders against terrorist elements?

But beyond the mere technology policy process, what about the human and cultural issues behind technology transfer? I would again argue that because we are seeing the same technology in a variety of contexts and cultures then the risks of ignoring the privacy risks of these technologies will create problems across all these same contexts and cultures, regardless of their differences. In the 1960s, with the threat of increased 'data processing' and the storage of personal information on 'data bases', Alan Westin famously defined informational self-determination and privacy as

"the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. (...) [It is] the desire of people to choose freely under what circumstances and to what extent they will expose themselves, their attitude and their behaviour to others.[2]"

That is, individuals must be allowed to choose what information is made available about themselves, and under which circumstances. Westin saw this principle under threat by new technologies. To say that this is merely a right permitted to those in the West is to deny essential choices to individuals around the world.

Everywhere that technology stretches we see similar challenges. The need to protect the identity of a blogger in the U.S. against copyright infringement is similar to the need to protect the name of a blogger in China (where there is a national database of all bloggers) or in Egypt (where the name of a gay blogger has been disclosed to the government). Anyone who tries to argue with me and say that what someone says publicly about his political or sexual persuasions in one country should be made illegal in another due to cultural differences is again attacking the foundations of what it means to be human and what it is to have some autonomy.

So, returning to the lack of action on privacy and internet governance, it is insufficient to argue that privacy is a Western concept that does not deserve special recognition and discussion at the international level. The UN, in particular, can not ignore this issue because its very founding

2 Alan F. Westin, Privacy and Freedom, New York: Atheneum, 1967

documents speak of the importance of privacy and a universal concept. But beyond that, case after case is emerging of the abuse of the political processes in countries around the world, in the West, East, North and South. With technologies stretching across these borders we see similar and familiar methods of repression and oppression and we can not just sign this all away by saying that every country has a different culture.

2. Over-riding security

Despite all of these cultural concerns around the world I find it amazing how leaders speak publicly with such ease on how countries must learn to co-operate on security matters. The UN process is full of such statements as every year at the General Assembly we hear speech after speech from diplomats and heads of state about the need to advance the cause of security. This was also the case at the UN summits on the information society where in the field of internet governance much more activity went into security discussions than in most other policy domains.

Sure, it is fun to speak about security nowadays — it is as though you are on the side of the angels when you do so. In the old days it used to be said that no IT manager ever got fired for buying IBM computers. Now politicians believe that the prevailing mood is such that no politician or bureaucrat got disciplined for voting or authorising new security policies and technologies.

But these are all overly simplistic positions even in today's societies.

First, gaining international agreement on security policies is incredibly difficult even for countries who agree with one another on many other things. We've seen negotiations on security policies break down in all types of areas. Despite all the rhetoric on terrorism the UN, for instance, the UN is unable to agree on the definition of terrorism or terrorist group. There are different lists of terrorists and terrorist groups in every country around the world. This problem is not limited to terrorism. Definitions of crimes differ around the world, which often prevents co-operation and the establishment of a single legal regime even amongst neighbouring states.

Even when co-operation does take place it often leads to problems. For years the Council of Europe worked on a cybercrime convention. It was heralded the world round as a key step forward in the governance of security and the internet. Under this notion a number of non CoE countries are now trying to implement the convention into their national law despite the fact that most Council of Europe countries have not yet gotten around to it five years later.

We also hear frequent calls for industry and government cooperation on these same matters. It is often assumed that these two sectors share many concerns in common. This too couldn't be further from the truth. For years the G8 held meetings with industry officials from around the world on internet security and eventually the initiative was dissolved because of a lack of agreement. Even within industry you find varying views on what is security, e.gs. is it the protection of computer systems even from legitimate hacking for research purposes? Does 'system' include copyright protection scheme? Yet we continue to spend vast

amount of time listening to rhetoric within the UN processes on internet governance that co-operation is needed, almost as though the UN has not been paying attention to all the failed policy processes around the world.

Second, the political dynamics of security are now changing. We are learning more about the systems that were developed and rushed out in the name of security. Vast national infrastructures to promote security and prevent terrorist attacks are now being questioned. Politicians and officials are being linked with specific systems are no longer being heralded at the polls. Companies are now being identified with vast surveillance schemes that were conducted at the behest of government plans and are being punished by regulators and by customers.

For instance, in June 2006 media organisations discovered that the Society for Worldwide Interbank Financial Telecommunication (SWIFT) was disclosing vast mounts of data regarding bank transfers to the U.S. Treasury. SWIFT is a co-operative of financial institutions; although individuals use their service, their true customers are banks. In this case, privacy regulators around the world found that SWIFT was in breach of law. More interestingly, geopolitical issues were raised (what if the Chinese Government was to gain access to this same data?) and SWIFT's customers, i.e. the banks, started placing pressure on SWIFT to alter its ways. SWIFT's CEO had to retire early, and the organisation is redesigning its network infrastructure and moving its operations to Switzerland to avoid controversy.

Yet we still spend so much of our time speaking about the need for security and security policy. How much more time at internet governance meetings must be expended calling for security co-operation while ignoring the intricacies of doing so, while continuing to ignore privacy as though it is too difficult a concept to deal with? Meanwhile, polls and consumer surveys continue to remind policy makers that individuals are concerned about privacy. Confidence in electronic commerce and participation in the information society hinges on individuals' trusting the other parties in communications and transactions. Both privacy and security policies are key enabler of trust, yet so little action is taking place on privacy while instead our policy processes continue to focus only on flawed perceptions of security.

3. Lack of policy options

If security is so difficult to agree upon within actual international instruments and policy language, we often conclude that privacy is equally difficult to enforce. This is not necessarily true. There is a significant consensus on the need to protect privacy, and there is a general consensus on the means to do so. Since the 1960s we've had a system of regulation to manage personal information. This system of regulation was implemented into international agreements through such bodies as the the Council of Europe in its 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data; and the Organization for Economic Cooperation and Development (OECD) and its 1980 Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data. They both set out specific rules covering the handling of electronic data. These rules describe personal information as data that are afforded protection at every step from collection to storage and dissemination.

The positive obligation to protect privacy and personal information has taken the form of 'data protection', and is often used to protect individual privacy against abuse from both public agencies and private companies. The first modern data protection law in the world was enacted in the Land of Hesse in Germany in 1970. This was followed by national laws in Sweden (1973), Germany (1977), and France (1978). These laws eventually led to a harmonising European Union directive of 1995, the EU Data Protection Directive 95/46/EU.

Data protection rules hinge on the Fair Information Practices. These were developed in the late 1960s in response to the threat of secret databases holding vast amounts of information on individuals. In simple terms the fair information practices place requirements on 'controllers' (collectors of personal information), so that

- personal data should be collected only for specified, explicit and legitimate purposes

- the persons concerned should be informed about such purposes and the identity of the controller

- any person concerned should have a right of access to his/her data and the opportunity to change or delete data which is incorrect and

- if something goes wrong, appropriate remedies should be available to put things right, including compensation of damages through the competent national courts.

In essence, data should be collected with informed consent of the individual; processed fairly and lawfully, for limited purposes and limited use, and retained for a limited period of time.

This does not mean that security is ignored. Laws may still be created to interfere with this data privacy laws. When national laws and technologies combine, concertedly, to interfere with the right to privacy in the name of national security, public safety, economic well-being, prevention of crime and disorder, the protection of health and morals, and the protection of rights and freedoms of others; then the landscape becomes more complex. One expects this in any modern political system: laws regulating individual rights are sophisticated and up to date, and laws regulating the right of the state to interfere with these rights have to be also carefully crafted, be sophisticated, and up to date.

The EU Data Protection Directive 95/46/EU is the most modern data protection instrument. It ensures that data can flow across the EU and beyond provided that:

- Data must be processed fairly and lawfully.

- They must be collected for explicit and legitimate purposes and used accordingly.

- Data must be relevant and not excessive in relation to the purpose for which they are processed.

- Data must be accurate and where necessary, kept up to date.

- Data controllers are required to provide reasonable measures for data subjects to rectify, erase or block incorrect data about them.

• Data that identifies individuals must not be kept longer than necessary.

The Directive also states that each Member State must provide one or more supervisory authorities to monitor the application of the Directive. Finally the Directive also calls for assurances when data is to be transferred to a jurisdiction outside of the EU to ensure that adequate protections exist. This prevents a situation where a company can collect data in France and then send that data to another country where that data can be used without respecting French laws. Rather, there must be assurances that the data is going to a jurisdiction where there are adequate legal protections.

While the OECD, the CoE and the EU together cover many countries with their guidelines, conventions, and directives, there are still many countries out there without data privacy laws. There are new initiatives emerging to deal with this situation. One initiative is coming from the privacy subgroup of the Asia-Pacific Economic Cooperation (APEC) economies. They have been developing a set of principles that developing economies in the region can adopt to at least develop baseline protections for personal information.

This domain is not devoid of its own complexities and political differences. There are significant divides between the European model and models implemented elsewhere around the world. For instance, the U.S. refuses to implement a privacy law that regulates the conduct of the private sector. There is some concern that the U.S. will use the APEC principles as a global standard rather than what they were intended for, which is a set of baseline principles. This situation prevents the emergence of a global standard based on comprehensive and strong regulation. Some industry officials have also been forthright about their concerns about data protection law. In September 2007 Google called for a global privacy standard but rejected the comprehensive European model and instead called for the weaker APEC principles (much to APEC's surprise!) to be implemented around the world, even in Europe.

This does not reflect a lack of consensus on the need for policy, but rather it shows that a debate can and must be had on the virtues of each regulatory system. Such a debate is occurring already and it is proving to be rich and interesting. Yet, as ever, the internet governance policy process ignores this entire domain because it probably continues to believe that privacy is an insurmountable regulatory domain despite the fact that we've been moving forward for nearly half a century.

Restating the case for privacy

Privacy is a rich and complex area. There are no clear answers to any of the problems it poses. I think this is possibly true of all interesting policy domains.

Yet the internet governance process continues to neglect privacy. The lack of deliberation over privacy while the over-emphasis upon a simplistic view of security is making fools of us all. Privacy is a human right while it is also a consumer interest. How many policy areas can say the same for themselves? And yet the silence continues.

Even though I am sometimes uncertain, sometimes shaken by the challenges in defending privacy, I can not understand why it is not to be at least discussed alongside all of the other pressing policy issues today. This debate is happening elsewhere and the results are fascinating. Limiting debate on this issue limits our policy choices and we will, as we have seen elsewhere, be forced to reckon with our poor decisions at some point in the future.