

Privacy and or as Freedom

Gus Hosein

Every one who works on a specific issue area tends to believe that what he or she works on is core to humanity's future and/or sense of dignity. Environmentalists argue that the future of our global commons is at stake. Those who struggle against the arms trade contend that we can not be a civil world united in peace so long as we continue to make trade in the artefacts of destruction. Gun lobby groups contend that the possession of firearms is a key constitutional right, in some countries, or key to survival, in others. Anti-abortionists are struggling for the lives of the unborn and the morality of the future. Those who focus on development and aid believe that they are helping to heal the inequalities of the world. Through participation in political processes these people, regardless of differing political persuasions and methods, they all endeavour for change.

Privacy advocates are no different, for the most part. You will rarely find privacy advocates protesting outside of buildings or summit locations, though. They do not often warn of armageddon, although warnings of distopias of Orwellian proportions are hardly different. Privacy advocates also contend that there are legal, sociological, and historical foundations to privacy. Most importantly, privacy advocates are well aware that they are in a struggle for the hearts and minds of the general public.

Yet privacy never has the same primacy in public discourse as those other issue areas. When I'm asked 'What do you do for a living?', I describe myself as a privacy-advocate. People then look at me, confused.¹ This probably never happens with anti-abortionists or environmentalists. All the while, free speech advocates are given even higher regard because they seem to be calling for the right of the others to advocate their points.

This relegation to the back of the queue of ‘popular causes for which we must advocate’ is inappropriate. As a right, privacy provides an inherent valuable service to society. As a subject of study, understanding privacy complements our understanding of politics. Privacy and freedom are tightly interlinked, and opening up this relationship opens our eyes to political trends.

Privacy and Freedom

One of the best definitions of privacy that I have ever heard was in fact an indirect definition. In response to the proposed ID-card policy in the United Kingdom, Lord Philips of Sudbury said that while there are many logical reasons to oppose the policy, most prominent in his mind was that it just ‘felt wrong’.

I instinctively and quite deeply reject [the proposed policy]. I can’t quite find the language to rationalise the depth of my feeling about this. (Mistaken Identity Public Conference, LSE, May 19, 2004)

Such an impulse is perhaps the most helpful delineation between when an incursion into the private life of an individual is reasonable and when it is not. As Philips indicates, we often encouch our arguments behind more ‘rational’ language but I would like to emphasise that it first starts with a core belief. Everything else is a cover for this gut instinct.

There are many other ways of defining privacy. In an early form, as we moved towards modern democratic systems of governance, privacy was considered as a protection from invasion.

According to William Pitt in 1763,

The poorest man may in his cottage bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storms may enter; the rain

may enter - but the King of England cannot enter; all his forces dare not cross the threshold of the ruined tenement.

This is part of the thinking that leads to the notion that ‘every man’s home is his castle’. Shortly thereafter, in 1765 Lord Camden, a noted judge, commented that the police had over-reached their authority by searching someone’s home in order to seize papers, saying that

We can safely say there is no law in this country to justify the [police] in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have.

From their time to the 20th century, privacy was embedded in leading constitutional documents, from the French Rights of Man to the American Bill of Rights.

Privacy re-emerged as a key issue of modern times in the late 1800s. Building on definitions and the work of other legal minds of their time, Louis Brandeis and Samuel Warren famously wrote in 1890 that privacy was the ‘right to be let alone’. This seminal article, published in the Harvard Law Review, was a reaction to technological and market developments of the time. Warren, a wealthy member of ‘high society’ had his family’s privacy intruded upon by the tabloid media. The article warned of the growing media frenzy and the threats posed by cameras, or what they refer to as “recent inventions and business methods call attention to the next step which must be taken for the protection of the person”. (Samuel Warran and Louis Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193 (1890))

With the advent of modern computing, concerns increased. With the threat of increased ‘data processing’ and the storage of personal information on ‘data bases’, we sought a more developed

definition of the constitution of privacy. Responding to this threat, in the late 1960s Alan Westin defined informational self-determination. Privacy, he said, is

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. (Alan F. Westin, *Privacy and Freedom*, New York: Atheneum, 1967)

That is, individuals must be allowed to choose what information is made available about themselves, and under which circumstances. This is tightly bound with the notion of human dignity. According to Robert Ellis Smith, privacy is

the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves. (Robert Ellis Smith, *Ben Franklin's Website*, *Privacy Journal*, 2000)

Similarly, Rhoda Howard and Jack Donnelly argue that, as enshrined in the Universal Declaration of Human Rights,

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. (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.

While other definitions are abound, most contemporary definitions draw links between self-determination, autonomy, dignity, surveillance, power, and increasingly, technology.

In an ‘Information Society’, where almost all attributes of an individual can be known, all interactions mapped, and all intentions assumed based on records, our ‘instincts’ have led us to worry. Since the advent of the modern computer, or even as the possibilities of computers entered our minds, and since we saw what we have been capable of when our guardians were given too much control over our personal information and our lives, we have endeavoured as a society to protect privacy. Modern privacy law, after all, emerges from these lessons, struggles, and developments.

The legal definitions, however, come after the ‘feeling’ and ‘instinct’ of privacy. The point to understanding privacy as a core feeling, something inexplicable, however, is that it is tightly intertwined with our sense of right and wrong, our moralities. Even beyond morality, however, where we can forever debate the relativist nature of such norms and morals, there is something about human dignity. When we peer into the life of any individual to a large degree we are peering into an area that we know is wrong.

In a civilized society we limit these gazes because we understand that there is something undignified about knowing so much about an individual. Privacy is the maintenance of dignity that is at the core of human rights. Privacy protects individual autonomy and human agency. Knowing everything about someone reduces that person to a set of known facts, controllable and manipulatable. As long as a zone of autonomy exists around each and every individual, the opportunities for abuse and oppression are lessened. Knowing everything about the activities of all peoples greatly enhances the powers of a ruler. And in a deliberative and open society, privacy

provides a core pre-condition to participation, a most basic civil liberty. Knowing the actions and intentions of your political opponents reduces their ability to oppose your rule and arguments.

Privacy is thus a fundamental component to freedom. As Westin noted at what many felt to be the dawn of the 'information age',

no society with a reputation for providing liberty in its own time failed to provide limits on the surveillance power of authorities. In this sense, American society in the 1970's faces the task of keeping this tradition meaningful when technological change promises to give public and private authorities the physical power to do what a combination of physical and socio-legal restraints had denied to them as part of our basic social system.

Privacy protection is intertwined with liberty. In modern society we need to protect privacy even more so than previously, as technology and modernity influence our conduct. Yet everywhere, privacy rights are burdened.

Privacy as a Threat

Through benign or malignant intentions, indirect or directed attacks, exogenous or forces from within, privacy is under constant threat. As it is a core principle of autonomy and human dignity, and as its reduction enables control, manipulation, oppression, and increased power, this should come as no surprise.

Although it is often claimed that privacy rights around the world changed in September 2001, they were threatened long before. Looking at the 1990's alone, we can see significant changes in law. Although laws on data protection were introduced by a number of countries throughout the 1990's, as well as laws on freedom of information, encroachments were abound. In France silly regulations

restricting the use of technologies to secure communications continued unabated despite technological revolutions. In the US laws were passed to allow for interception of communications regardless of technological innovation. In the United Kingdom any number of policies emerged, ranging from closed-circuit television cameras that now pollute the citiscapes to policies that give any arm of government significant access to your personal life. Similar policies were implemented elsewhere.

The threats to privacy, at their most intellectual foundations, arise from a number of sources, including communitarians, classical feminists, and those seeking well-functioning markets. Finally, there is a school of thought that contends that privacy is not as important as other more valuable 'civil liberties' such as free expression.²

Communitarian Reduction

The communitarians argue that while privacy is a noble value, there are other noble values that we must consider. Amitai Etzioni, a leading proponent of the reduction of privacy in the public sphere argues that we need to renegotiate our privacy rights, for the common good.

Although we cherish privacy in a free society, we also value other goods. (...) To begin a new dialogue about privacy, I [ask] if you would like to know whether the person entrusted with your child care is a convicted child molester. I further ask: Would you want to know whether the staff of a nursing home in which your mother now lives has criminal records that include abusing the elderly? Should the FBI be in a position to crack the encryption messages employed by terrorists before they use them to orchestrate the next Oklahoma City bombing?

Addressing such concerns raises the question of if and when we are justified in implementing measures that diminish privacy in the service of the common good.

(Etzioni, Amitai: *The Limits of Privacy*. New York: Basic Books, 1999.)

Etzioni and the communitarians contend that we do not have an absolute right to privacy. In fact, privacy must be balanced with other rights. According to Etzioni, there is a set of criteria for this balancing act.

1. The purpose for invading privacy must be for a known threat to the common good. E.g. we don't need to demand full medical records to make sure someone wasn't lying about being too sick to go to work.
2. Privacy can be invaded once we have exhausted alternative means of countering danger. Can we instead find out that the person was playing soccer/football with his friends by asking friends?
3. When privacy is to be invaded, it must be minimally intrusive. Only get the part of the medical record that says that he visited the doctor on the day that he claimed to be sick, rather than the full record containing all records of his treatment since birth.
4. Once privacy is invaded, measures must be taken to minimize and treat undesirable side effects. Try to only get his medical record, and not the listing of all people who attended the doctor that day, or do not ask any questions about the type of doctor (was it a sexually-transmitted disease clinic?).

The communitarians, however, fail to recognize two key factors. First, the mere threat of this information being made available, particularly health information, has a chilling effect on its collection in the first place. That is, even under the most stringent balancing tests, if I know that my health information may be disclosed if I do not show up at work one day, I may be less likely to

disclose this information to my doctor in the first place. This has a dangerous effect on the relationship between my doctor and I, and an even more disastrous effect on healthcare generally. If I don't disclose information to my doctor, this will lead to misdiagnoses or worse yet, a lack of treatment.

Second, the communitarians see power in a most benign way. To them, all initiatives to invade privacy start with reasonable acts and minimal purposes. Early cases of intercepting communications in the United States involved society's struggle against drug dealers and alcohol bootleggers. The reasons quickly grow. Access to information relating to who you've called, emailed, and servers you have connected to in the United Kingdom began first to be limited to the police, but subsequent uses increased dramatically. Fingerprinting was once a measure to identify criminals; now it is used to permit people to work or enter borders. What starts small always ends with an avalanche of personal information. Power, once created, rarely regulates itself into a smaller force.

Feminist Critique

The classical feminists contend that privacy is merely a right that is abused by men. The right of privacy, they argue, is based on Anglo-American common law, providing that a husband is master of his household; and as such the State nor anyone else may enter to intervene. As a result, man could subject his wife to beatings so long as he is within his home; and the feminist critique goes on to say that the right of privacy is used to enforce and preserve such authority relations between man and wife. As Reva Siegel argues:

It seems just as likely that legal elites devised the story linking ‘privacy’ and ‘domestic harmony’ to wife beating (...). This right of privacy is a right of men ‘to be let alone’ to oppress women one at a time.

Privacy, therefore, is used to protect men and the home, not women.

This view is supported through historical precedence. In 1852 in the state of North Carolina, the courts held wives incompetent to testify against husbands in all cases of assault and battery, except where permanent injury or great bodily harm is inflicted. The final Court decision stated that:

We know that a slap on the cheek, let it be as light as it may, indeed any touching of the person of another in a rude or angry manner – is in law an assault and battery. In the nature of things it cannot apply to persons in the marriage state, it would break down the great principle of mutual confidence and dependence; throw open the bedroom to the gaze of the public; and spread discord and misery, contention, and strife; where peace and concord ought to reign. -- (North Carolina) *State v. Hussey*, 44 N.C. (Busb.) 123, 126-27 (1852))

More recent discussion on feminism and privacy, however, contends that privacy no longer is used against women like it once was. Women (and more accurately, victims generally) may now be shielded in rape cases so that their names are not disclosed to the public. Women who were previously subjected to spousal abuse may now seek a zone of autonomy through de-listing their telephone numbers and concealing their contact details as they try to start new lives. And even the controversial issue of abortion in the US is sustained by privacy rights.

Economic Argument

Informational self-determination, the ability to control information about yourself and how it is used, can be used in dishonest ways. In his famous ‘economic analysis of the dissemination and withholding of information’, Richard Posner contends that such information control by individuals leads to misrepresentation.

It is no answer that (...) individuals have the “right to be let alone”. Very few people want to be let alone. They want to manipulate the world around them by selective disclosure of facts about themselves. (The Right to Privacy, in Georgia Law Review, Volume 12, 393-422, 1978, p.400)

At some point, he argues, nondisclosure becomes fraud, and the motive for concealment is to mislead others. He goes on to argue that it is more efficient to have organizational privacy (e.g. trade secrets) over personal privacy.

Even within this economic approach, however, Posner notes that privacy in communications is valuable. The smaller the crowd of people that we are speaking to, the more likely we are to speak privately, with informality and brevity. “Allowing eavesdropping would undermine this valuable economy of communication”. He does note that the more we value the privacy of communications, the more likely that its surveillance will be of value to the police, which is also advantageous.

Posner was not anti-privacy. ‘Ostentatious surveillance’ does pose problems even to Posner. This is a form of surveillance that involves “following someone about everywhere”. Such a form of surveillance is legally problematic when the surveillance exceeds what was reasonably necessary to uncover private information “and became a method of intimidation, embarrassment, or distraction”. In this sense, there are limits to what is reasonable, although Posner does not help anyone in defining what is ‘reasonably necessary’, and his points approach the communitarian perspective

quite quickly. And within the Information Society, ‘ostentatious surveillance’ occurs with every move we make.

It is fair to say that Posner’s view of how society works best is, well, different. The economic view does acknowledge that privacy is a useful thing, particularly for communications and organizations. Posner just believes that in the conduct of business and economic affairs, personal privacy is often used for dishonesty. His weakness is that he heralds ‘economic rationality’ above all, viewing the world as filled with autonomous slaves (12 Ga. L. Rev. 428 (1977-1978) Privacy: Economics and Ethics: A Comment on Posner; Fried, Charles). In doing so, he avoids complexity (12 Ga. L. Rev. 430 (1977-1978) Privacy is Dear at Any Price: A Response to Professor Posne’s Economic Theory; Bloustein, Edward J.), and focusses too much merely on informational self-determination, rather than the larger picture of privacy as a whole. In doing so, he intentionally avoids discussing privacy as a safeguard against political oppression (12 Ga. L. Rev. 437 (1977-1978) Privacy is Dear at Any Price: A Response to Professor Posner’s Economic Theory; Bloustein, Edward J.). Finally, according to Richard Epstein in his response to Posner:

The nineteenth century arguments about the abolition of slavery did not in the slightest depend upon the relationship of slavery to material output. The abolitionist of that or any other era regards it as immaterial that the liberation of the slaves might reduce transaction costs or increase the gross national product. The gut position about slavery was, and is, that it is simply wrong for any person to own another person. (12 Ga. L. Rev. 457 (1977-1978) Privacy, Property Rights, and Misrepresentations; Epstein, Richard A)

His point is that legal theory does not depend on economic analysis. A ‘gut feeling’, and an ‘instinctive reaction’ may again be the point from which we start, and the laws follow afterwards.

Secondary to Other Rights and Balance

Those in the field of human rights and civil liberties may criticise the notion of privacy as a human right, as they do not believe it is a right in itself. They contend that there are more primary rights, such as the right to liberty, property, and to be free from injury.

This returns to the notion of 'balance', where individual privacy must be balanced against the right of society to protect the liberty, property, and lives of others, particularly during this war on terrorism. This notion of balance is corrosive to individual rights, however, and in the face of such utilitarian arguments we fall back either to the economic perspective or the weaknesses of communitarianism.

Others argue that privacy is secondary to other more important human rights and civil liberties. They argue that it should always come second to free speech for example. Journalists and free speech advocates who deal with libel and defamation cases believe that the public's need to know takes priority over the individual's secondary right to privacy. Along this line of reasoning, they and others contend that privacy is not a direct constitutional right, but rather is an interpretation of other rights such as the defense from arbitrary search and seizure, and self-incrimination.

This is an almost reasonable interpretation of constitutional law, at least in the US, but none of these approaches are helpful in understanding what is truly at stake within the Information Society.

Privacy may threaten some world views, and may provide impediments to government authorities or may conflict with the rights of others, or with other rights. But privacy, like other rights, are goods in themselves, and protect human dignity. There are also legal arguments to defend privacy, as I'll describe in the next section, but there are also reasons to defend privacy at the same time as we defend other rights such as freedom of expression.

Privacy as Law and Regulation

Privacy is generally protected in two forms of law. The first is constitutional and international human rights rules and laws, where privacy is protected as a core individual right, thus affecting all of government's other activities. The second form of privacy law focusses on the specifics of information privacy, and the fair treatment of information by both governments and industry. This is what we call data protection law, which I will mention in a more limited manner here.

Privacy as an Individual's and Citizen's Right

One of the earliest constitutional statements on privacy emerged from the French Revolution. The Declaration of the Rights of Man and the Citizen of 1789 declared:

Since property is an inviolable and sacred right, no one shall be deprived thereof except where public necessity, legally determined, shall clearly demand it...

Admittedly, this was not a clear declaration of the right to privacy, but when linked with the idea of 'a man's home is his castle', this placed a limit to the reach of government. And if a man's zone of privacy/property was violated, there *was must* clear reasons for this.

The US Bill of Rights was a bit more clear on this idea of privacy and property. In the Fourth Amendment, the Constitution of the United States says:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Here the violation of an individual's person, home, and effects is given greater protection and more clear grounds to question an intervention (including a 'warrant', under 'probable cause', etc.).

Neither of these rights, however, are a clear articulation of a legal privacy right. In neither of those historic documents does the word 'privacy' actually appear. Privacy does appear in other human rights documents, however. Article 12 of the Universal Declaration of Human Rights states that

No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.

In creating the Universal Declaration of Human Rights, the writers knew that privacy was a foundation to human dignity, but also to political participation, particularly after the atrocities of the 1930s and 1940s. Also, the authors of this document were not just Western legal theorists; countries from around the world collaborated on this document, re-affirming that importance of privacy as a universal right and value. This document, however, is non-binding.

The International Covenant on Civil and Political Rights is slightly more binding upon nations. In Article 17 it states that

1. No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks

This treaty not only calls on states to not arbitrarily interfere in the private life of individuals, but the state also has a positive obligation to implement laws to protect this right. But there are no legally binding mechanisms for individuals to enforce their rights under the covenant.

The European Convention for the Protection of Human Rights and Fundamental Freedoms (short title ECHR) of 1950 created the first binding treaty on human rights. Article 8 of the ECHR establishes within ratified states the right to privacy:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence.

(2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.

Again, not only do states have to abstain from interferences, they have a positive obligation to protect these rights.

Within this very definition in the ECHR we see the strains with which European public policy is currently grappling. The protection of the right to privacy is paramount, a constitutional right protected by the ECHR Article 8(1). If only it were so simple, the regulatory landscape would be clean and clear. Under Article 8(2) national laws may be created to interfere with this right, 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; the landscape becomes, in a word, complex.

The ECHR remains remarkable due to two developments that are privacy enhancing for the most part. First, the European Court on Human Rights has a rich history of reviewing laws and imposing sanctions on countries for failing to protect privacy. In interpreting Article 8(2) the Court has

decided that any initiative to interfere with an individual's right to privacy must be in accordance with law and necessary in a democratic society. 'In accordance with law' means that there must be a law that states the conditions for invasion, but also it must be 'foreseeable' in that an individual should be able to change her actions to avoid such an invasion, i.e. if you don't commit a crime, you will not have your home searched. 'Necessary in a democratic society' means that there must have been a pressing social need and the action must be proportionate to the legitimate aim pursued, i.e. you can't read someone's email if you suspect them of having lied about being sick and took a day off work.

The Court has also expanded the protections of Article 8 beyond government actions to those of private persons, i.e. the private sector, where it appears that the government should have acted to prohibit conduct.

Informational Privacy

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. Data must be kept secure and accurate, and not transferred to countries without adequate protection.

In full, the fair information practices as required within a number of international legal documents such as the EU 1995 Directive, the OECD Guidelines of 1980 and the Council of Europe Convention of 1981. To various extents, these documents require 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.

Meanwhile, tighter regulations tend to apply to the category of 'sensitive data'. In the EU Directive of 1995, this type of information is defined as

data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sexual preference. In principle, such data cannot be processed. Derogation is tolerated under very specific circumstances. These circumstances include the data subject's explicit consent to process sensitive data, the processing of data mandated by employment law, where it may be impossible for the data subject to consent (e.g. blood test to the victim of a road accident), processing of data has been publicly announced by the data subject or processing of data about members by trade unions, political parties or churches. (European Commission. Data Protection in the European Union, available at http://europa.eu.int/comm/internal_market/en/dataprot/guide/guide_en.pdf)

Member states may provide for additional exceptions for reasons of substantial public interest.

Such exceptions are permitted if, among other things, it is necessary on grounds of national security, defence, crime detection, enforcement of criminal law, or to protect data subjects or the rights and freedom of others. (European Commission. Data Protection in the European Union, available at http://europa.eu.int/comm/internal_market/en/dataprot/guide/guide_en.pdf)

These are consistent with the exemptions listed under the ECHR.

Key Threats to Privacy in the Information Society

Now that you have an understanding of privacy as a human right, and privacy as a legal right, you may better appreciate the threats to privacy. It is important to remember that many of the intellectual revolutions in privacy were influenced by technology. Warren and Brandeis were reacting to the use of cameras by the tabloid media. Communications privacy laws arose in response to technological innovation in communications such as the telegraph, radio, and telephone. And data protection and modern privacy law arose in response to the prevalence of database and data processing technologies.

Now we are well beyond those days. Personal information is everywhere, to be collected and used and stored. The difficulties and costs in performing surveillance have decreased dramatically, just in time for all of this information to be in the form of bits and communicated across wires and in the air, for all to see.

There are a number of policy initiatives currently to increase surveillance powers even more so.

Surveillance of Communications

In the old days, communications ‘traffic data’ was information found in your telephone bill: who you called, when, and for how long you spoke. Now, things are different. According to a committee of European privacy commissioners:

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. Although transactional data may in some jurisdictions receive a degree of protection under rules protecting the confidentiality of correspondence, the massive growth in the amount of such data is nevertheless a cause of legitimate concern. (Article 29 Working Party, “Recommendation 3/97: Anonymity on the Internet”, (Brussels: European Commission, 1997).)

As communications media are increasingly interlinked (e.g. using your computer on wireless networks, connecting to the internet over your mobile phone), this information becomes more and more detailed. It is not just about what you read, but now your mobile phone company knows where you were, your wireless LAN provider can point to other people who were in the same area as you, and your internet service provider can pinpoint whatever else you did while you were on-line months ago. All human conduct in the Information Society makes use of electronic systems, and this information is now waiting to be linked together.

Considering all of the discussion above regarding privacy rules and laws, one would think that this information was deemed sensitive. However, privacy laws have been rewritten in order to enable surveillance. Previously, internet service providers, telephone companies and mobile phone companies had to delete this ‘traffic data’ when it was no longer required for business purposes. Since September 11th 2001, a number of countries have introduced laws requiring these communications service providers to keep this information for between 1 and 10 years, just in case one day your internet usage information may be of interest to the police, or other government authorities.

New policies have also been introduced to allow for the interception of communications and for real-time monitoring of traffic data. This is not the same as intercepting your post as it was in the old days. Real-time monitoring of communications involves tracking all of your movements while you are on-line in a way that goes well beyond even Posner's conception of 'ostentatious surveillance'.

These new policies are being implemented to increase surveillance while reducing the constraints upon authorities. The new laws being devised not only guarantee access to this data, but they also increase the purposes for which governments may access this information in the first place.

Previously warrants were only issued for specific serious criminal activity and public oversight was thorough and detailed. Now information that was once considered 'sensitive' can be accessed without probable cause, without a clear articulation of suspicion, and for any crime.

Much of the momentum behind these policies arise from two sources. First, governments argue that they are compelled to act due to the changing technological environment, and the increased risks associated with this environment. Because of technological change, they argue, we must adapt old laws for these new technologies. This is despite the fact that these new technologies tend to amplify and transform government power already. (Escudero-Pascuale, Alberto, and Ian Hosein.

"Questioning Lawful Access to Traffic Data". *Communications of the ACM* 47, no. 3 (2004): 77-82.)

The second source of momentum behind these policies is multilateralism. After a number of failed national policy initiatives dealing with the Internet in the 1990s, governments began to work at the international level to establish an international policy. Through such organizations as the Council of Europe and the Group of 8 Industrialized Economies, governments established international treaties and agreements on surveillance, so as to bring these rules home under the guise of harmonization

and international obligations. (Hosein, Ian. "The Sources of Laws: Policy Dynamics in a Digital and Terrorized World". *The Information Society* 20, no. 3 (2004): 187-99) These international initiatives are fraught with problems, however, including a democratic deficit, and a lack of adequate protections for civil liberties.

The surveillance of communications is not limited to government, however. Private firms are increasingly monitoring our interactions on-line. In the early days of electronic commerce this constituted the monitoring of movements through the use of cookies, in order to create profiles for marketing purposes. New forms of revenue generation have since arisen, with new forms of tracking while on-line. Even the sanctity of communications content is regularly breached, with employers monitoring the conduct of employees as they surf the web and reading emails, to web-mail service providers scanning email contents in order to provide 'improved' advertising.

Surveillance of All Activity

Surveillance in an information society is not limited to communications surveillance. Increasingly we are breaking fundamental rules of data protection by using information collected for one purpose for a number of other purposes. And we are joining these sources of information together in order to surveil with even more authority and power.

Data sharing initiatives are abound. The US Government considered developing The Total Information Awareness programme (TIA), an advanced collection of personal information for mining and analysis. TIA was developed within the Pentagon Information Awareness Office, to:

imagine, develop, apply, integrate, demonstrate and transition information technologies, components, and prototype closed-loop information systems that will counter asymmetric threats by achieving total information awareness useful for preemption, national security

warning, and national security decision making. (Report to Congress regarding the Terrorism Information Awareness Program, May 20, 2003)

After much controversy, this system was abandoned, even while other systems are arising. Now the US is intending to profile air-line passengers under its Secure Flight regime³ that brings together airline and reservation databases with government databases to assess the risk of each traveller and to see whether she should be prevented from travelling.

This sharing of information between industry and government also involves the sharing of information across borders. US laws require that any airline that flies into the US must provide the US Department of Homeland Security with access to this 'passenger name record' information to combat terrorism and enhance airplane security.

This initiative is not limited to the US, however. While it was originally a US idea, when the US required foreign carriers to submit this information to the US Government, a number of other countries decided to adopt similar practices. Already the European Union is moving towards a similar data-sharing agreement between airlines and governments for general law enforcement purposes. Australia has a similar initiative, and Canada is requiring access even to domestic travel habits.

Policy initiatives are emerging that aim to increase the collection of information as well. We have already seen the US start fingerprinting and face-scanning all visitors under the US Visitor & Immigration Status Indication Technology System (US VISIT).⁴

These *biometrics* are taken from the up to 30,000 visitors each day and are then stored in US Government databases for between 75 to 100 years; and are then combined with other information

regarding these visitors and aliens. (Privacy International, The enhanced US border surveillance system: an assessment of the implications of US-VISIT, September 28 2004)

Similar systems are being called for elsewhere. In response to the terrorist attacks on a Russian school, the Russian Government stated its intention to fingerprint all foreigners at borders. Japan is considering a system as well. The United Kingdom is planning a similar system as part of its larger biometric identity card regime. The European Union has announced its intentions to create a similar regime that will also involve the fingerprinting of all EU citizens. The EU is proposing that all EU passports include fingerprints, and that all 450 million EU residents and citizens' fingerprints are then kept in a central database. (Privacy International, PI Advises the European Parliament to Stop Biometric Passports) Finally, the UN is playing an active role in establishing standards in biometric passports; this standard effectively globalises the American practice.

These surveillance initiatives are again not limited to government. More and more companies are requiring the collection of fingerprints from their employees, and are conducting background checks of prospective candidates. One interesting example of corporate surveillance is the controversial private-run profiling system, MATRIX (Multistate Anti-Terrorism Information eXchange). This system combines information from government databases and private-sector companies. According to its promotional material, "When enough seemingly insignificant data is analyzed against billions of data elements, the invisible becomes visible". The system was developed by the Florida-based company Seisint, and was used extensively in the months following the attacks on the World Trade Center and Pentagon. The system identified 120,000 people who showed a statistical likelihood of being terrorists. This 'High-Terrorism Factor' was used to conduct investigations and arrests after the information was submitted to state policy, Immigration and Naturalization Service, FBI, and the Secret Service.

All of these systems and policies outlined above are merely the starting point for more invasive practices. Centralised biometric databases are not as interesting as a listing of all the times someone was verified. For example, a biometric identity card system will generate transactional data whenever someone is scanned as they visit their doctor, pass through a border, and are stopped on the street. The same is true for all of the policies for communications surveillance. The listing of all of these transactions will again provide private and public entities with a great deal of information regarding our daily practices and our private lives.

These are the inevitable challenges of the Information Society. But the outcome need not be disastrous.

Privacy as Freedom

Privacy is often regarded as a less important right. First, it is regarded as secondary to other more important rights, and possibly derivative from them. Second, it is seen as the first impediment to combating crime, terrorism, and other social ills. Here I want to destroy this notion and show how privacy is essential to freedom.

Even within the US where there is no comprehensive data protection law, privacy is left with an awkward constitutional status. As mentioned above, the word 'privacy' does not appear in the US Constitution. However, there are other rights that, when combined, may be interpreted as 'privacy rights'. To provide Americans with a constitutional right to privacy, the US Supreme Court has relied upon combining the right to free speech and the right to assemble peacefully in the First Amendment to the Constitution; with the Fourth amendment that protects against illegal search and seizure; and the Fifth that protects against self-incrimination. Since the 1960s these have been interpreted so as to allow individuals to speak and assemble freely without prior identification, to

protect the privacy of places and people, and to limit the ability of government to compel information disclosure. The Supreme Court argued that privacy is within the ‘shadows’ of the Constitution. (Solove, Daniel, and Marc Rotenberg. *Information Privacy Law*. New York: Aspen, 2003.)

A number of interesting Court decisions followed from this constitutional grounding for privacy, leading perhaps to a foregrounding of privacy, and its emergence from the shadows. Privacy can be seen as the enabler of all these Constitutional rights. In the 1950s, for example, the government of Alabama tried to compel the National Association for the Advancement of Colored People to disclose the list of their members in an attempt to intimidate the membership. The US Supreme Court sided with the NAACP in this case. In *Talley v. California* the Supreme Court upheld the right to distribute written material without identification.

Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws anonymously.

The obnoxious press licensing law of England ... was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers. John Lilburne was whipped, pilloried and fined for refusing to answer questions designed to get evidence to convict him or someone else for the secret distribution of books in England. (US Supreme Court. *Talley v. California*, 362 US 60 (1960).)

The Court argued that the right to speak anonymously is firmly rooted in the history of the country, but also in the roots of political participation.

More recently, in 1995 the Supreme Court argued that anonymity was an enabling component of the marketplace of ideas, and essential to the act of free expression.

The interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment. (US Supreme Court. *McIntyre v. Ohio Elections Commission*. 514 US 334 (1995).)

The most recent Court decision upheld the view of that requiring an individual to gain a permit containing one's name in order to engage in door-to-door advocacy of a political cause was unconstitutional.

Anonymity is a shield from the tyranny of the majority [...] It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation -- and their ideas from suppression -- at the hand of an intolerant society. (US Supreme Court. *Watchtower Bible and Tract Society Of New York, Inc., Et Al., Petitioners v. Village Of Stratton Et Al.* 240 F.3d 553 (2002).)

Drawing from the argument that anonymity is a shield from oppression, privacy emerges from the shadows of other rights. Privacy is not just derivative from these other rights, nor is it secondary. Privacy is core to public participation, and as such is essential to freedom. Without privacy freedom is weakened as individuals are without protection from retaliation. Without privacy, the individual

is reduced to judgement of all-seeing observers, both public and private. Without privacy, people will never be able to organize peaceful assembly in opposition to Government without Government's prior knowledge, and with its increased ability to intimidate.

If a Government had the ability to perfectly observe their Opposition, the consequence would be either that the Opposition would go underground, or it would be the last such Opposition. Anti-abortionists would not be able to protest, environmentalists would not be able to organize, gun lobbyists would be registered and watched, those who lobby against the arms trade would be marked. Privacy is thus essential to an open and participatory democracy.

Privacy in an Open Information Society

It is not enough, however, for me to claim privacy as a constitutional right, as essential to democracy, and to leave it at that hoping that no further incursions will arise. No constitutional right, nor any moral right for that matter, is absolute.

The challenge remains in making sense of what the US Supreme Court was saying when, on the balance of interests, anonymous speech outweighs the public interest in disclosure. When the US Supreme Court ruled that individuals had a constitutional right to privacy, the Court issued the following condition: the individual who claims that his constitutional right to privacy was invaded must have had a *reasonable expectation* of privacy. Similarly, within the European Convention on Human Rights, the right to privacy is balanced against many other considerations, on the following condition developed by the European Court of Human Rights: incursions on privacy must be in accordance with law and necessary in a democratic society. Thus our autonomy, dignity, and freedom are at the mercy of social trends.

The ‘reasonable expectation’ is actually a two-prong test. First, the person must act as though he expected privacy. So he should not post copies of his emails on his website, for example. Second, society must be prepared to recognize that expectation as reasonable. To extend the above example, that individual had a reasonable expectation of privacy not only because he kept his emails private, but also because society deems email privacy to be reasonable.

Similarly, according to the European Court of Human Rights, ‘in accordance with law’ means that there must be a law that states the conditions for invasion, preventing arbitrary interference. While this test is easy, the second test is again more challenging. ‘Necessary in a democratic society’ means that any intervention into the private life of an individual must not be overly broad in application. There must have been a pressing social need, and the action must be *proportionate* to the legitimate aim pursued. For example, the Security Services can’t read someone’s email just because they are suspected of having lied about being sick and taken a day off work.

In both cases, social trends are the barometer of privacy as a fundamental right. I started this essay with the notion of privacy as a ‘gut instinct’, something that, when invaded, makes us ‘feel wrong’. I quickly tried to ground this notion into legalistic terms, as constitutional rights and statutory rights under data protection. This granted privacy a primacy in the domain of human rights and civil liberties, particularly, as I said, it is key to public participation and the functioning of an open and participatory democracy. But now we are back where we began, with privacy being subject to fuzzy concepts like ‘proportionate’ and ‘reasonable’ that are up for human judgement and interpretation.

The constitution of ‘proportionate’ and ‘reasonable’ is unclear. There was a time when we thought that capital and corporal punishment were reasonable and proportionate when the crimes were severe enough or the public wanted vengeance, retribution, and entertainment. Generally, this is no longer the case. But there was also a time when we believed that national databases were

problematic, that mass surveillance of communications was disproportionate and unreasonable. Yet within the Information Society, we see these systems and practices spreading.

The reasons for incursions upon our rights to privacy are many, and put forward by even more people, institutions, and agencies. Technological change is a component to this social shift. We now have the capacities to store millions of fingerprints in a single database to verify travelers to the US. As these visitors grow accustomed to submitting their fingerprints in the US, they are less likely to be offended when their own home governments require their fingerprints for more general purposes. The fear of terrorism is another component. Previously we collected fingerprints of criminals, or collected information on suspects; now society seems less obsessed with due process, and many argue that they are willing to forego liberty in the name of security.

The ‘Information Society’, when combined with the equally silly notion of the ‘War on Terror’ may actually produce a frightening state of affairs. Personal information will be the new currency of access and privilege, traded without our consent, and possibly even without our knowledge. Technology and fear are determining much of what we do, and this must somehow be turned around.

Two news stories within two days are cases in point. On November 9, 2004, the New Zealand Press Association reported a story of an employee who was fired because he refused to give over his fingerprints. His company told the Employment Relations Authority that it needed to use fingerprinting technology to combat false time claims by all employees. The fired employee claimed that:

Your employer used to be able to make demands on your time only when you were at work, but now they can hold biometric information on you 24 hours a day – we are no

longer employees and employers, but slaves and masters. (Man sacked for refusing to give employer his fingerprints, 9 November 2004, <http://www.stuff.co.nz/stuff/0,2106,3090380a11,00.html>)

He was fired for refusing a 'lawful and reasonable request', and this dismissal was in turn endorsed by the Employment Relations Authority. According to the story, the Authority made its decision on the grounds that the national Privacy Commissioner argued that 'finger-scanning technology did not breach privacy principles as it merely stored mathematical data rather than actual prints'. This does not prevent it from infringing upon this man's sense of dignity, however.

The second case involves two press articles on a new security system at London Heathrow Airport. Both describe the testing of an X-ray device that sees through passengers' clothes before they board an airplane. A London Times article (November 07, 2004, Plane passengers shocked by their X-ray scans, Dipesh Gadhur, Transport Correspondent) notes how the graphic nature of the results shocked the passengers. Although very effective at identifying hidden devices on the body, the article quotes two 'subjects' of the test who commented on how shocked, alarmed, embarrassed they were. A CNN Article (Airport X-ray sees through clothes, Tuesday, November 9, 2004 Posted: 10:43 AM EST (1543 GMT)) notes instead the passengers who claim that they don't mind the invasiveness, so long as they are safe in the sky. The article also quotes a spokesperson for the airport, saying that 98 percent of participants gave positive feedback. The diversity in the reporting shows the diversity in social norms. Both articles note, however, that the United States Government has decided against adopting this technology because it was so invasive. So norms may appear different in different countries.

Morality and dignity may be the only forces left to fight against this continuing shift downstream. Many of our understandings of human rights and civil liberties are hinged upon a sense of morality

and dignity. We do not permit torture not only because it is against the law, but because it offends us. We regulate many activities not only because they are illegal, but because we feel that they are wrong, and unnecessary in the type of society within which we choose to live. The initiatives discussed in this chapter introduce new norms to an unsuspecting society, and risk changing our senses of morality and dignity, along with our legal rights.

Changing norms will change our regard for what are proportionate and necessary measures in a democratic society. Once it becomes accepted that all information that is derivative from our interactions in modern society is collected by default in the eventuality that you do wrong to someone or to the State, then there is little ground for people to feel offended by forced collection of DNA of all newborns, or the default fingerprinting of all individuals. After all, the logic goes: ‘unless you have something to hide/fear, this data will never be used against you’.

We should all be working to maintain a sense of liberty and freedom in this era, not working even harder to ensure that every single source of information regarding one’s life is subject to surveillance by default, and indiscriminately so. Five years ago we would never have pursued many of these policies and systems. I now worry most about what will happen five years from now, looking back and looking forward: what will we think is reasonable, proportionate, and necessary in a democratic society when all activities and intentions are recordable, accessible, and required?

So this is why I think it is so important.

Gus Hosein, November 2004

¹ Although this may not be because of my answer.

2 this classification of criticisms is from Solove, Daniel, and Marc Rotenberg: *Information Privacy Law*. New York: Aspen, 2003.

3 This system followed the demise of the Computer Assisted Passenger Prescreening System (I and II).

4 There is currently an exception for Canada and Mexico