BITMUN'14

UNITED NATIONS HUMAN RIGHTS COUNCIL

AGENDA

RIGHT TO PRIVACY

Introduction

We live in an era in which it has become trite and clichéd to declare that our very conceptions of privacy and property are shifting. These fundamental attributes of human society, having remained relatively unchanged despite the scientific, political, and social revolutions of previous millennia, have begun to shift before our very eyes with the advent of information and communication technology that supposedly connects us to each other more than ever before. This is especially true in the age of Facebook, with its purported number of over 900 million active users in May of 2012. In joining such a network, we now have unprecedented, game-changing access to the rest of the global community; if we truly wanted to, we could, in fact, "meet" the vast majority of these users online. In contrast to previous expectations of the number of people an average person might meet in his or her lifetime, this bewildering growth in our current ideas of connectivity and interpersonal relationships has constituted a paradigm shift. To fully appreciate the degree to which such a change has come about, however, let us take a step back and examine the philosophical and social currents that have led to this development.

Privacy

We have a tremendous interest in privacy as human beings, and thinkers of every ilk have worked to set privacy on some sort of secure footing. Is privacy even desirable? Even this rudimentary question does not have a solid answer in theory. The so-called "normative" question, whether or not policy is worth having, takes second place to an even more fundamental question: what is privacy? Legal scholar Ruth Gavison noted that a neutral or descriptive concept of privacy is required to build upon and develop a normative argument for or against it. Gavison defined privacy as how much access a third party has to you, as an individual, through information and attention. Yet now, over 30 years later, the very idea of privacy still remains in question.

A basis for this committee's working definition of privacy can be found in the works of the philosopher Jeff Reiman, who in 1976 stated that privacy is "the condition under which other people are deprived of access to either some information about you or some experience of you." Indeed, while the philosophical conversations regarding the idea of privacy may be interesting in themselves, it is important to remember that the greater purpose of this committee will be to define the policy-based limits and protection of privacy in light of technological advancements.

One important point to address, however, is whether privacy should be given "moral legitimacy as a claim to limit access to information or to control information." After all, if no such value exists in privacy in the first place, there are no grounds for using privacy as an excuse to develop policy on privacy violations. An impetus that crosses the boundary between our two parallel ideas in this topic – privacy and property – is the argument that

privacy can be treated as a form of property. Proponents of this view argue that privacy has therefore, in our world, become a marketable commodity just like security and data. On the other hand, legal scholar Julie Cohen argues that privacy is a fundamental value, like equality or liberty, because privacy is critical for the development of "independence of critical faculty and imperviousness to influence." A critical argument for the value of privacy, Cohen notes, is that "a degree of freedom from scrutiny and categorization by others promotes important non-instrumental values, and serves vital individual and collective ends." Put in another way, privacy is an essential component of developing novel, non-conservative, fresh ideas and trains of thought. In fact, without this introspective space, Cohen hypothesizes that every human being's thoughts and beliefs would be in danger of aligning with the mainstream, depriving society of new developments and advancements, a vision that is depicted in many dystopian science fiction novels and may actually materialize in our world.

Throughout the early 1900s, telephone networks had grown in both size and coverage, covering more and more of the world's surface, mostly in developed nations. As a result, the sheer number of people that could be contacted by the device increased, and consequently, so did the population using the telephone.

In terms of privacy, however, this also meant that information was now leaking across that precious boundary between home and the outside world. The privacy of one's personal space was beginning to open its floodgates, as information was sent anywhere and could often be decoded by a persistent outside observer. In short, an interested and powerful third party, including governments and later influential corporations with much to gain in terms of marketing and profits from information regarding the general public, had access to important and private parts of individuals' lives. It is interesting that phone tapping and more generally wire- tapping, often viewed possibly as the most egregious and outrageous violation of privacy in our present culture, were endowed its capacity by the invention of the telephone. It is both a reassuring note of our society's theoretical fairness and a worrisome one about the potency of the method that wiretapping is very strictly forbidden in most nations across the globe. For most democratic countries, wiretapping must be authorized by the court, which requires proof that it would be practically impossible to gather evidence for criminal activity without use of this technique. Most nations, however, have ways for the government to bypass the entire process. In the U.S., the passing of the 1978 Foreign Intelligence surveillance Act meant that there were two additional routes by which the government could circumvent this requirement: by receiving approval form the secretive United States Foreign Intelligence Surveillance Court and by orders from the Attorney General.

To many, this is a worrisome development, in addition to the fact that the recording of a conversation need not be given express consent in most regions.

Rise of the Internet

Undoubtedly, from the very early days of the development of the Internet, as well as of the growth of computing capacity, the concern of privacy invasion has played a central role in dictating policy considerations. Indeed, this concern is understandable from the fundamentally skewed power structure that results from the growth of computing capacity and networks. As noted by social scientist Helen Nissenbaum, "information technology is considered a major threat to privacy because it enables pervasive surveillance, massive databases, and lightning-speed distribution of information across the globe." In the early days of computers, the amount of computing power and accessibility that a single individual possessed in relation to the capacity of a government or multinational corporation was pitiful at best. The concept of "big data", which nowadays dominates the technological
and academic conversations in computer science, has consequently been a scary one for the layperson. After all, if these enormous organizations could have so much data on each and every one of us, some sort of violation of privacy must surely be present. Moreover, what sort of information the government did and did not possess was also a matter clouded in mystery; the public, when its attention was focused on this issue, was constantly left guessing as to the extent that the government knew about their deepest, most private lives.
Yet even though each individual technological development, including webcams, spyware, and data caching, provided specific instances for the possibility of privacy violations, the picture as a whole quickly became murky as well. With all of the possible ways that the government or other powerful organization or individual can learn the many personal facts that we spread over the Internet, how are we to even begin to try to prevent every such potential threat to our privacy? More importantly, how do we define this encroachment on our privacy when the routes towards the issue are so diverse and numerous? Indeed, even academics have found that the very idea of classifying the threats to privacy posed by information and computer technology to be daunting at best. With all of these technologies, do we define an invasion of privacy as any information leak? Some forms of monitoring may be in order for the supposed necessity of security and prevention of crime and terrorism, but many of the methods present at the government's disposal throughout the late twentieth century would not have been acceptable to the general public.

Implications for Privacy

Given all of these developments, it has also become ever more pressing to ask whether privacy is in fact worth it. Classic economic analysis, of course, yields that the 'proper' balance, or rather the most 'efficient' one, will be brought out by supply and demand. In other words, if people so desire privacy as to either restrict access to the Internet or possibly stem the growth of computer technology, they will do so. The fact that there were very few significant attempts to curb this outburst in technological growth may then signify the fact that very few were and are willing to relinquish their own technological capacity for the return of privacy. On the other hand, there were a number of cases of public resistance to privacy encroachment via technology by various governments, most notably in the United States. In particular, in the wake of the September 11th attacks the passage of the Patriot Act, which allowed the government to spy on computer and Internet usage through network operators without any penalties or court authorizations, sparked a furor in which 371 city and county governments and four state legislatures approved statements advocating for the restriction of the Patriot Act to its less controversial provisions.
Moreover, further actions that were pursued by the White House to gather information about its citizens – namely the Total Information Awareness project, which, as its name suggests, would have vastly expanded the scope of governmental searches in private information – was blocked and defunded by Congress, signifying resistance even at the governmental level against such invasions of privacy. This could also mark a point of distinction between when privacy is necessary and when it is violated: why did Congress quickly pass the contentious Patriot Act but vigorously debunk the Total Information Awareness Project? Perhaps a grey area can be found for the settlement of the issue at this boundary; or perhaps a more creative solution remains to be found, especially in light of the growing influence of social networks in privacy.

The UN in its Universal Declaration of Human Rights put forward one of the original international precedents for privacy rights.
In Article 19, the UN claims, "*Everyone has the right to freedom of opinion ... this right includes freedom to*
hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers."
In light of recent elevations in data flow internationally, however, there have been numerous calls for increased oversight and standardization on the part of the UN by multinational organizations. This may seem counterintuitive; after all, the companies calling for such measures, such as Google, Microsoft, and Proctor and Gamble, are among the companies that are threatening privacy in the first place through data gathering and sheer statistical analysis. Yet these companies are calling for international privacy standards to be decreed from a body such as the UN. New Zealand Privacy Commissioner Marie Shroff states that this desire results from the fact that the standards would "bring

legal certainty. Far from it being some sort of bureaucratic initiative to impose more regulation on business, businesses are recognizing this is a highly volatile environment … and it is hard for them to operate their businesses in this very varied world."

In particular, Google has taken the lead in approaching the UN regarding the issue. In 2007, Google's privacy chief, Peter Fleischer, addressed UNESCO regarding an agreement between international governing bodies and multinational organizations on global privacy standards. Fleischer went as far to claim that if this step were not taken, the Internet would face a "crisis of confidence" on the part of its users. This concern comes mostly from the fact that many underdeveloped nations have little to no legislation regarding the passing and usage of information, especially regarding data protection.

Moreover, many governments and organizations have noted that the counter-terrorism effort has resulted in breaches in individual privacy in the past decade. The United Nations Special Rapporteur on human rights and counterterrorism,

Martin Scheinin, has reported to the UN Human Rights Council that the "expansion of watch lists, border checks, financial data sharing, interception of communications, biometrics and ID registers in recent years" due to counterterrorism paranoia have necessitated a global declaration onprivacy in the technological age. Scheinin added that nations "no longer limit exceptional surveillance schemes to combating terrorism and instead make these surveillance powers available for all purposes." Many counter-terrorism measures have been deemed illegal in various courts worldwide, but a more unified declaration on the part of the UN, especially a body such as UNESCO, has been long coming.

The Rise of Facebook

Since the very beginning of Facebook, privacy concerns have been raised. Facebook has never allowed users to completely remove information once posted about themselves from the site. While certain items, such as wall posts and pictures, may be deleted manually, it must be done one at a time. Deactivation is a method of keeping your content from being seen by others, but all of the information remains stored in Facebook's database. One of the first major outcries against Facebook arose when the company decided to establish the "News Feed," which gave users very little control over what aspect of their activities on Facebook were published for any of their friends and acquaintances to see online. Indeed, a group of Facebook users went as far to create a petition against the company, noting that the "introduction of the News Feed and Mini Feed … call into question the safety and privacy of its more than 9 million users." Facebook relented quickly on the issue and added in a number of controls. However, the default was for the posts to be displayed on the Feed, and many users opted to remain that way. More critically, in May 2007, Facebook added its Platform feature, which allowed third party developers to create applications for the site. All of this would be highly innocuous, of course, except that these developers could access any of the information that users posted online except for contact

details like e-mails and phone numbers. This created a flow of information away from Facebook to outside observers. In addition, the application can access any information about the user's friends and networks, without these people having ever added the application or accepted its use.

Past International Actions

Because the idea of privacy as a matter of changing policy in light of new technological developments is fairly recent, there have not been many significant past actions taken by international bodies. In fact, the current debate seems to stem from whether the privacy and property concerns can even be dealt with at the policy level, especially when the very ideas with which we are dealing have not been defined clearly. However, there do exist a number of instances in which the global community dealt with such problems.
The ones that have come into notice recognize that Privacy is unequivocally recognized as a fundamental human right at both international and regional level. It is enshrined in:

- The Universal Declaration of Human Rights (art 12 and 19)
- The International Covenant on Civil and Political Rights (ICCPR, art. 17)
- The Convention on the Rights of the Child (art. 16)
- The European Convention on Human Rights (art. 8)
- The American Convention on Human Rights (art. 11)

International Privacy Standards

The international community has yet to draft some equivalent of a "UN Convention on Data Protection." Although there is no comprehensive regime at present regulating data collection on an international level, a starting point for the creation of a global scheme can be found in the past attempts of some organizations to articulate privacy standards for their respective member states. In
1980, the Organization for Economic Cooperation and Development (OECD), which is comprised of highly industrialized countries, pushed the agenda on international data protection by issuing the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.
The OECD Guidelines signified the first attempt by an international organization to formalize the right to online privacy beyond the declarations issued by the United Nations. Although the recommendations of the OECD are non-biding, the Guidelines established seven principles: (1) collection limitation principle, (2) data quality principle, (3) purpose specification principle, (4) use limitation principle, (5)
openness principle, (6) individual participation principle, and (7) accountability principle. These principles may serve as the foundation for future international agreements. In addition, the OECD Guidelines identified the need to ensure the free flow of data across

borders, as long as the transmission of data does not violate the aforementioned principles. Two region-based frameworks have built on the principles identified in the OECD Guidelines. These are the 1981 European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and the 2004 Privacy Framework endorsed by the Asia Pacific Economic Cooperation. While regional frameworks are slowly emerging, non-government organizations have kept the agenda alive on the international stage. In 2005, the International Conference of Data Protection and Privacy Commissioners issued the Montreux Declaration, which appealed to the United Nations "to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights."

The notification of Prism

The issue of privacy was brought to the forefront of worldwide news by PRISM, a clandestine mass electronic surveillance data-mining program operated by the United States National Security Agency since 2007.

PRISM was launched from the ashes of the Terrorist Surveillance Program, which was implemented by the Bush Administration after the September 11 attacks. The TSP was widely criticized and was deemed illegal because it lacked warrants granted by the Foreign Intelligence Surveillance Court.

PRISM was authorized by the Foreign Intelligence Surveillance Court, and was enabled by the same Bush Administration under the Protect America Act of 2007 and by the FISA Amendments Act of 2008. The Act "specifically authorizes intelligence agencies to monitor the phone, email, and other communications of U.S. citizens for up to a week without obtaining a warrant" when one of the parties is outside the U.S."

The existence of PRISM was publicly revealed by Edward Snowden, an NSA contractor. The leaked document included 41 PowerPoint Slides, which identified the companies participating in the PRISM program. The slides also explained how the electronic communications data tend to take the cheapest route, as opposed to the most physically direct route. Because most of the Internet's infrastructure is based in the United States, it offered the American intelligence analysts the opportunity to intercept the communications of any foreign targets whose electronic data passed into or through the US territory.

During a House Judiciary hearing on domestic spying on July 17, 2013 John C Inglis, the deputy director of the surveillance agency, told a member of the House judiciary committee that NSA analysts can perform "a second or third hop query", which means that the NSA can look at data not only from a suspected terrorist, but from everyone that suspect communicated with, and then also from everyone those people communicated with, and so on.

Concerns and Ideas about the Developing English Law of Privacy

Few can doubt that the UK Human Rights Act 1998, in incorporating the European Convention on Human Rights (ECHR) and in particular the guarantee of the right to privacy in Article 8 of the Convention into UK domestic law, and also in requiring the judiciary in s. 6 to have regard to the Convention in developing the common law, is having a considerable effect on the developing protection of human privacy in English common law. This was predicted when the Human Rights Bill was going through its various parliamentary phases by many, including the Lord Chancellor, who described the judges "as pen-poised ... to develop a right of privacy." Also predicted was the way the expansion was likely to come about: incrementally and, initially at least, by means of expanding established torts.6 The early judicial decisions that have been handed down since the coming into force in October 2000 of the 1998 Act confirm the above predictions. Arguably, they also display the defects of dealing with new societal problems by putting old torts on the Procrustean bed and stretching them out of shape to meet new requirements.

Those who share this view may ask why the richer experience of other systems, in particular that of Germany, France and the USA, has not been extensively employed to help English judges at this formative stage of a new era. In fact, foreign experience has, if anything, been (mis)used, mainly by those who oppose the creation of a new tort of privacy or some equivalent thereof, to stunt such a development. The motives for such actions may be understandable. But the way foreign law and comparative legal experience has been misrepresented or overlooked to restrict developments in our law cannot be left un-answered.

Chinese Angle of privacy

For Chinese citizens, it is clear that privacy rights enjoy only the flimsiest of legal protections. China's constitution, postal law, labor law and medical law all make passing mention of privacy concerns, but they are vaguely worded and are all anyway subject to the notoriously arbitrary workings of the Chinese legal system. Yet some pundits reckon that, as attitudes toward privacy continue to change, the law will eventually be strengthened.

It is well documented that the Chinese government is committed to monitoring media online and in more traditional channels for information that might harm unification of the country, endanger national security, or subvert government authority.18 In February 1999, the government announced the creation of the State Information Security Appraisal and Identification Management Committee that "will be responsible for protecting government

and commercial confidential files on the Internet, identifying any net user, and defining rights and responsibilities, the move is intended to guard both individual and government users, protect information by monitoring and keep them from being used without proper authorization." In 2004, the Chinese government continued to impose restrictions on news reporting and publishing by censoring publishers and punishing unauthorized publishers. Authorities continuously oppressed the expression of opinions that the Party deemed objectionable.

UN Educational, Scientific and Cultural Organization Proposed Solutions

International Privacy Agreement

In December of 2009, UN Special Rapporteur on human rights and counter terrorism Martin Scheinin urged the UN Human Rights Council “to establish a process that builds on existing principles of data protection to recommend measures for the creation of a global declaration on data protection and data privacy.” To jumpstart this process, Scheinin recommended that the Council settles the interpretation ofArticle 17 of the International Covenant on Civil and Political Rights (ICCPR) by establishing data protection as a necessary attribute of the right to privacy. Although UNESCO generally supports the use of international legal instruments to protect privacy online, its focus lies elsewhere. UNESCO is in a unique position to assert that that a legal agreement affirming the right to data protection is a necessary but not sufficient condition for protecting the right to privacy on the Internet. Distinguishing between technologies that “enhance” privacy and those that “extract” privacy is essential for understanding that technology is not only the problem but also part of the solution for protecting privacy. Some privacy enhancing technologies are more desirable than others. According to Marc Rotenberg, the director of Electronic Privacy Information Center, technologies that ensure anonymous transactions are ideal, followed by technologies that give users control over which data to share and finally technologies that merely obtain consent from the users to make persona data available. The exchange of privacy enhancing technologies among member states is an integral part of an international privacy agreement, which cannot be effective solely as a legal framework grounded in human rights.

.

Questions A Resolution Might Answer

The following questions should act as a guide when drafting a resolution for this topic. It is not to be seen as an exhaustive list but rather a starting point from which to produce a constructive resolution.

- Do current human rights documents adequately address the challenges of the Internet?
- In light of recent developments in information and communication technology, should the international community agree on a new standard for privacy and property rights?
- Should the international community adopt the principles found in the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data? What principles should be added or removed?
- What is the most appropriate framework for addressing privacy and intellectual property rights at the international level?
- Should privacy and property rights be addressed separately or do their common context, i.e., the rise of the Internet, warrant a unified approach?
- How much private personal information should a government be able to know about an individual without breaching their rights to privacy and freedom of expression?
- How can governments ensure that the private information and surveillance they conduct on citizens will not fall into the hands of those who could use if for malicious purposes?
- What national and international provisions, regulations and laws should be enacted both nationally and internationally to protect the fundamental right to privacy?