November 11, 2011

Global Trends to Watch: The Erosion of Privacy and Anonymity and The Need of Transparency of Government Access Requests

A report from workshop 160 written by *Katitza Rodriguez*, International Rights Director, Electronic Frontier Foundation and *Katarzyna Szymielewicz*, Executive Director, Panoptykon Foundation.

A Brief Substantive Summary

General Remarks

This panel discussion at the Internet Governance Forum in Kenya offered a snapshot of existing and proposed regulatory frameworks for Internet privacy. It looked at potential risks, global trends, best and worst practices. Panelists examined the Cybercrime Convention, mutual legal assistance treaties for gathering and exchanging information among countries, and the need for transparency in government requests for access to personal data.

At a time when individuals regularly turn to search engines, social networks and other Internet intermediaries to find information online, blog their most private thoughts, share personal data with friends, store sensitive information and share their location through mobile devices via GPS tracking, digital privacy is of paramount importance. Yet research by social scientists has found that few Internet users fully understand how much information they are revealing about themselves and the potential impact this disclosure can have.

Moreover, the ongoing move towards cloud computing means that more and more of our information will be stored online. Millions of people are trusting web-based email services such as Google Gmail to store years worth of private correspondence. Cloud services such as Dropbox or Google Docs store your most private documents. At the same time, the cloud is changing the economics and dynamics of surveillance. The mere flow and storage of traffic data can reveal our online routines; social networks, interests and/or believes. As panelists noted, this information is not adequately protected against misuse or abuse by both corporate entities and governments.

As consumers have embraced cloud computing and mobile technologies, law enforcement agencies have followed. Presenters on this panel noted that governments are seeking broader powers to surveil their own citizens. India RIM was forced to provide intercept capabilities to their Blackberry services. The Iranian government hacked into the Dutch certificate authority Diginotar in order to obtain the credentials necessary to intercept the communications of 300,000 Iranian Gmail sessions. Panelist Christopher Soghoian, a research fellow at Indiana University, noted that cloud computing has made surveillance and the seizure of personal documents much easier and less expansive for U.S. law enforcement. "Google charges $25 to hand over your inbox," says Soghoian who added that the wireless carrier Sprint has 100 employees working full time on surveillance requests. "Yahoo! charges $20 plus the cost of a stamp. Facebook and Microsoft don't even bother charging because they say it's too difficult to get compensated for this."

Presenters on the panel observed that existing laws and treaties do not respond to various privacy risks that arise in digital environment. The Budapest Cybercrime Convention is a decade old, while the European Data Protection Directive and the US Electronic Communications Privacy Act date back to 1980s, predating the modern Internet ecosystem.

Profiling and Behavioral Advertising

Information about users' behavior on-line is often utilized for profiling and targeting purposes. This is not only beyond users' control but also frequently without their awareness. The entire online behavioral advertising ecosystem is based on uncontrolled data processing, which operates smoothly without the need to obtain users' informed consent.

One particular topic that surfaced in this context was the promise of privacy enhancing technologies and the way these technologies conflict with the business models of companies that provide services for free via ads. Soghoian pointed out that it is very difficult to deploy privacy protective policies at companies with ad-supported services. If data stored in Google docs or on Amazon's servers was encrypted, those companies will not be able to monetize the data. "They are analyzing the content of your e-mail to show you ads, and there's not really a privacy preserving way for them to target those ads to you without seeing your data," says Soghoian. "When you give your data to a third party, you lose your control over it and the government can come in whenever it likes, with a valid court order, but they are relatively easy to obtain, and get your data."

Vint Cerf, the father of the Internet who is now the vice president and chief Internet evangelist for Google noted during the panel that Google encrypts access to its services, - such as HTTPS access to its search engines. But Cerf acknowledged that implementing encryption with cloud-based systems is difficult, especially if all the crypto must happen in the browser. "We couldn't run our system if everything in it were encrypted because then we wouldn't know which ads to show you," said Cerf. "So this is a system that was designed around a particular business model."

Cerf says the biggest problem is that cryptography is not very convenient or easy to use. He said companies should work hard to make it simpler and give users more tools to limit what happens to their information. Cerf said Google has designed its system to control personal data.

“At Google, anyway, we don't share any of the information that's in the system with any third parties except under the legal constraints that we're required to abide by,” Cerf. “It's true that we use a lot of information to generate, select and display ads, but we don't share that information with third parties. Some people misunderstand the way the system works. The information stays in the environment.”

A person participating in the discussion noted that Google Analytics on his web site allows him to see user’s personal data such as what key words were searched to get to that site and what browser is being used. But participants agreed that Google is taking firm steps to help preserve privacy by promoting SSL by default. Participants noted that most users do not have an effective legal regime that would protect their privacy in this context. Only some of the leading Internet companies offer their users the possibility to opt-out from cookie-based behavioral targeting. It was noted that European Commission is currently considering a revision of its legal framework regarding e-commerce and online privacy.

Access to Data Stored in the Cloud by Law Enforcement Agencies

Governmental access to data stored in the cloud is particularly worrying given the globalization of web based services and the fact that data is often stored in a different country than the user’s country of origin. If the data is stored in a country with doubtful human rights record or very lax regulation on the access to data for public security reasons, a number of privacy risks will arise.

Cerf insisted that Google only responds to valid requests that are accompanied by court orders or subpoenas. However, it was noted that even international corporations will struggle while confronted with a perfectly valid subpoena issued by the authority representing authoritarian or totalitarian regime.

“As far as governments go it's pretty clear that if the information is available and public and the government feels the need to protect the citizens that they are going to take advantage of whatever they can find in public,” said Cerf. “So we have little choice; if things are shared in that way, governments are going to go after and use that information.”

Participants discussed the unique surveillance capabilities available to the US government, due to the fact that so many widely used cloud computing and communications services are located in the US. Although European countries may have strong laws that protect the data of their citizens, the US government and its powers issued under the Patriot Act and FISA have a long reach – thus putting companies in a very difficult position, where they are in conflict between the laws of the US and other countries. As European, Asian and African governments consider placing their own citizens' data in the cloud, they will have to evaluate the cost savings against the legitimate desire to keep such data safe from foreign political surveillance.

Soghoian noted that Google's use of SSL encryption by default for Google's Gmail service helps to both protect against computer crime and enhance privacy. But he notes that Facebook and Twitter and Microsoft and Yahoo! have not followed Google's lead and some governments are also unhappy with SSL by default. Soghoian noted that Google was the target of a sophisticated man-in-the-middle attack performed in August by the Iranian government in which 300,000 Iranian users' e-mail communications were intercepted to get around Google's encryption.

If CoE, law enforcement agencies and governments were really concerned about protecting against cybercrime, Soghoian argued, they should push for default SSL, timely security updates and OS hard disk encryption. "So if we do care about cybersecurity and cybercrime, we would be seeing governments pushing for real security instead of just expanding their powers," said Soghoian.

Mandatory Data Retention

Another issue that was given substantial attention during the panel and open discussion is mandatory data retention. It was noted that government agencies throughout the world are pushing for laws that force online third party providers to collect and store more personal information that they need for the purposes of their business. Moreover, data retention's legal obligations to log users' Internet use are usually paired with provisions that allow the government to obtain those records, ultimately expanding governments' ability to surveil their citizens.

Citizens groups and civil society organizations find these controversial laws invasive and overbroad. Some countries' courts and tribunals have struck down data retention laws unconstitutional. This is the case with mandatory data retention regime existing in the EU, which forces all Internet Service Providers to store traffic data for the period up to 2 years so that it can be easily accessed by law enforcement entities. It was noted that Data Retention Directive is currently under review.

Panelist Katarzyna, director of the Panoptykon Foundation, noted that her home country of Poland has one of the worst data retention law in Europe with more than 1,000,400 requests for information per year and many cases of abuse. She noted that privacy activists in the EU are discussing how to fight data profiling and whether user consent should be needed to place cookies. Szymielewicz observed that the EU is pushing data retention proposals that go beyond the current requirements for telecommunications companies and Internet service providers to any entity that provides an online service.

"Data stored by telecommunication companies says a lot about your routines, a lot about your social network, a lot about where you go, what is your location," says

Szymielewicz. “So law enforcement can not only trace you back, but can also predict your future behavior.

Security vs. Privacy

Another significant theme of the discussion was an alleged conflict between security and privacy. It was suggested that these two values can be reconciled if sound security policy is pursued. Neither privacy nor general freedom must be the price for increase in public security. At the same time it was noted with concern that some governments justify their notorious attempts to pierce the veil of anonymity and waive the protection of personal data through by pointing to a need to protect national security and engage in lawful investigations.

The Cybercrime Treaty

In recent years the CoE has prioritized ratification of the Cybercrime Convention by non-European countries, and has provided extensive technical assistance to countries that are implementing its provisions in their national law. Even for countries that have not chosen to ratify it, the Convention has become a “guideline” for those interested in developing national legislation against the perceived increased threats of cybercrime.

EFF remains concerned about the potential impact of the Convention, and overbroad national implementations of it, on citizens’ fundamental rights. We have several concerns.

The Treaty provides detail on the types and character of surveillance powers it grants law enforcement agencies. While it mentions the need for privacy protections in a general sense, it fails to encode specific privacy protections necessary to limit the new powers it grants. As a model, then, the treaty is more likely (and has proven more likely) to encourage overbroad surveillance and less likely to ensure adequate privacy protection.

The flaws inherent in the Convention itself are exacerbated by the fact that it was drafted over ten years ago and much has changed since then. The Convention was premised on the notion that ‘traffic data’ (data generated by computers as a by-product of online interactions) is ‘less sensitive’, and so should be more readily accessible to law enforcement. But today’s ‘traffic data’ can include such sensitive information as your otherwise anonymous online identity or your social network of interactions. Mobile companies and our Internet services providers are now recording our whereabouts at every moment, and we are leaving far more detailed footprints that reveal sensitive information of our daily lives. Sensitive data of this nature warrants stronger protection, not an all-access pass.

Panelist Alexander Seger, the head of Economic Crime Division at the Council of Europe, told the gathering that cybercrime is a greater threat to privacy than governments and that the European Court of Human Rights has ruled that governments have an obligation to protect the privacy of citizens against criminal intrusion. Seger believes that references to human rights language in Article 15 of the Convention promotes human rights and the rule of law and allows the treaty to comply with the European Convention of Human Rights and other agreements. He said that the Convention offers safeguards to prevent over-criminalization by supporting the principle that the legal measures are proportional to the offense and by requiring judges to authorize more invasive measures. “It clearly says that interception should be limited to serious offenses, not just to – not be applied to any offense,” said Seger. “Service providers are not asked under the Budapest Convention to preemptively retain data. It’s data expedited preservation. It’s for specific specified traffic or content data, but it’s specific.”

Panel moderator Katitza Rodriguez noted in response to these comments that, the convention is specific on new powers, but vague on protections. Rodriguez was especially concerned that the Convention provides itemizes specific new powers while fails to encode human rights protections with equal specificity. This lack of specific allows countries to implement provisions that can criminalize legal efforts, such as security research activities. Also, while the Treaty does state in general terms that human rights must be respected, it does not clearly set out specific legal standards countries should use to ensure the extensive powers it grants law enforcement are not abused. This is particularly an issue in non-European countries with weak civil liberties. “There are many countries -- and just my country, I am from Peru, from Latin America – we have an ex President, currently in jail, for massive illegal interception of communications.” In many countries law enforcement agencies may not need increased surveillance powers and their judicial system might lack independence.

Seger pointed out that the Convention helps countries around the world establish proper codes of criminal conduct. “We can engage in a dialogue, and that's what we are trying to do in order to help countries take measures against cybercrime, but also improve human rights and the rule of law in any country.”

But panelist Amr Gharbeia, a technology and freedom program officer from the Egyptian Initiative for Personal Rights, countered that in transitional countries like Egypt, ensuring privacy requires that policy makers address questions about rule of law, transparency, national security definitions, and investigative procedures that treat the Internet as a special domain. This is particularly a potential issue where ‘cybercrime’ is already defined very broadly. Gharbeia noted that, in Egypt, “[i]t's actually illegal for you to use any encrypted transmission. So basically everyone who is logging on the Facebook or Twitter account (…) are actually violating the law in Egypt.”

Gharbeia added that in Egypt, developing privacy safeguards that respect the rule of law would require the reinvention of enforcement agencies. He says transparency is also very difficult and companies are required to keep logs for indefinite periods and then hand them over without any clear process. “Trojan horses like Finfisher, by the U.K. based company Gamma, and other systems that live in the center of the network have been found out," said Gharbia. "The only way to find out what the surveillance operations are going on in a security apparatus is if you actually break that. There is no transparency."

Conclusion and Further Comments

The architecture and development of the Internet have caused individuals to lose control over the collection, use and transfer of their personal data online. The fundamental value exchange underlying the Internet economy is that services are provided free of charge in return for pervasive use of individuals' information. This business model remains opaque to many users, who willingly or unwillingly share massive amounts of personal online data with a myriad of parties.

Users should not be alone in their struggle to maintain privacy in digital environment. Sound legal regulation is needed to ensure that fundamental rights of the users are respected. Users should be offered real choices whether to share their data with corporate entities and trade certain services for their privacy. This choice should not be limited to a formal right of consent. The notion of "informed consent" has eroded in the digital environment because of lack of education and awareness of how popular services work. There are also too few viable alternatives for equivalent services that do not require that users provide personal data.

"If you are paying a company for a service, then maybe they will deploy some more privacy enhancing technologies," observed Soghoian. "But when the company is monetizing your data, to provide you with a free and useful service, it's going to be really difficult for them to justify not saving any data by default or deleting IP addresses the minute they come in the door. Those are going to be tough decisions to get past the marketing team and other teams within the company."

Ensuring transparency and education should be the very first step in empowering users in online environment. The next step is to make fundamental principles of data protection – such as data minimization, proportionality and accountability of data processors – internationally binding. One way to work towards this ambitious goal is through the revision of the Convention 108 under the auspices of the Council of Europe. A second important forum for creating new standards can be offered by the EU through a pending revision of the Data Protection Directive that can reshape the whole data protection framework. Another possibility, which should be explored in parallel (never as an alternative) is putting further pressure on international corporations to adopt binding corporate rules with regard to privacy.

Binding privacy standards should also be enforceable against national states. While existing international conventions do contain sound principles with regard to the right to privacy, such principles are notoriously violated by both authoritarian and democratic states under the label of national security. Gharbeia pointed out that in 2006, according to Amnesty U.K., Microsoft handed over the details of the Hotmail account belonging to anti-nuclear activist Mordechai Vanunu's before a court order had been obtained by alluding that he was being investigated for espionage.

The challenge of mandatory data retention and the use of commercial data stored in the cloud by law enforcement agencies is increasingly relevant across the globe. One of the most striking examples of this tendency is a US law that allows for political surveillance of foreigners' data stored by US-based companies (FISA).

There is clearly an urgent need to adopt international standards for data protection in vertical relationships such as the citizens vs. state authorities. In order to do so, we need to consider the following questions:

- What limitations should apply to the scope of data being collected by various types of commercial entities, Internet access providers, search engines, on-line shops, social networks or web mail services?
- Should there be a legal obligation to store any data generated for commercial purposes and if so, for how long and for what purposes?
- Finally, what should be the conditions for law enforcements agencies to obtain access to personal data, regardless of whether it is stored for commercial or public security purposes?

Data protection should be seen in a broader context. The principles we adopt today will become more and more relevant in the future. They must be robust and adapt to the development of new web-based services, such as Internet of things, the smart grid or increasingly popular geolocation services. Policy makers have an obligation to protect basic human rights and develop strategies that work.

Workshop 160: Global Trends to Watch: The Erosion of Privacy and Anonymity and The Need of Transparency of Government Access Requests

Speakers:

- Vinton G. Cerf, vice president and chief Internet evangelist for Google, USA.
- Amr Gharbeia, Egyptian blogger, technology and freedom program officer from the Egyptian Initiative for Personal Rights, EGYPT.
- Alexander Seger, Head of Economic Crime Division of the Council of Europe, EUROPE.
- Christopher Soghoian, Ph.D. Candidate in the School of Informatics and Computing at Indiana University, USA.
- Katarzyna Szymielewicz, human rights lawyer and activist. Co-founder and executive director of the Panoptykon Foundation – a Polish NGO member of European Digital Rights, EUROPE.

Moderator:

- Katitza Rodriguez, Electronic Frontier Foundation's international rights director, PERU, USA.

Remote Moderator:

- Joana Varon, Researcher on Development and Intellectual Property at the Centre for Technology and Society (CTS/FGV) from Fundação Getúlio Vargas (FGV) School of Law in Rio de Janeiro.

Organizers:

- **Electronic Frontier Foundation (EFF)**: From the Internet to the iPod, technologies are transforming our society and empowering us as speakers, citizens, creators, and consumers. When our freedoms in the networked world come under attack, the Electronic Frontier Foundation (EFF) is the first line of defense. EFF broke new ground when it was founded in 1990 — well before the Internet was on most people's radar — and continues to confront cutting-edge issues defending free speech, privacy, innovation, and consumer rights today. From the beginning, EFF has championed the public interest in every critical battle affecting digital rights. EFF fights for freedom primarily in the courts, bringing and defending lawsuits even when that means taking on the US government or large corporations. By mobilizing more than 61,000 concerned citizens through our Action Center, EFF beats back bad legislation. In addition to advising policymakers, EFF educates the press and public.

- **Panoptykon Foundation**: Its mission is to protect human rights, in particular the right to privacy, in the clash with modern technology used for surveillance purposes. We want to analyze the risks associated with the operation of modern surveillance systems, monitor the actions of both public and private entities in this and intervene when human rights or democratic values are threatened. We are not opposed to the use of modern technology. However, what we do care about is the preparation of legal solutions that will strike a balance between competing values, such as security and freedom. We do believe that aspirations to increase public security or broadly conceived efficiency should not be pursued at the cost of the right to privacy and individual freedom. Our aim is to provoke social discussion on the reasons, signs and consequences of this phenomenon.