SURVEILLANCE AND COMMUNICATIONS INTERCEPTIONS- ABRIDGED

Presentation by Arthur Gwagwa, Senior Research Fellow, Strathmore University with contributions from Tomaso Falchetta (Privacy International).

I will speak on trends at UN for a as well as at regional and states levels, new forms of surveillance by police officers and intelligence services such as social media intelligence and offer recommendations.

1. A SHIFT AT THE UN POST-SNOWDEN REVELATIONS

ALTHOUGH the UN's role to monitor states laws and practices on surveillance and communications interceptions following the public outcry in response to the Snowden revelations, there are growing concerns about the right to privacy in the era of new surveillance laws and practices. There is:

- Technological advancements that facilitate soft forms of surveillance and policy responses have been slow.
- Increasing incidents of terrorism, especially in Europe, over the past few years, which have provided justification for intrusive laws and practices.
- Blurring of lines between surveillance by states and that which carried out by companies, such as social media companies. Since most of these companies are like empires in terms of their influence, they can exert influence on governments.

On a positive note, these challenges are encouraging the tech community to work with the policy communities in an effort to operationalize human rights concerns in technology development, such as the work that is being done by Access Now.

AT the UN For a level, two significant developments are worth mentioning since the 2014 OHCHR Report:

- In addition to a number of resolutions that have been passed, the establishment of the UN Special Rapporteur on the right to privacy at the end of 2015 filled a significant gap in the international human rights protection system.
- While the right to privacy remained prominent at the UN in 2016 (as it did in 2015 and in 2014), a shift in focus can nevertheless be detected: from a focus on the practices of government surveillance to the responsibilities of companies to respect the right to privacy. Please see the report of the UN Special Rapporteur on freedom of expression and the language contained in the 2016 UN General Assembly resolution on the right to privacy in the digital age which, while maintaining the language on state surveillance contained in the previous text (adopted in 2014),also builds upon it by adding significant provisions to address the role of companies.

- It is important that going forwards, both the U.N and other parties working on surveillance and privacy concerns continue building their work on the foundation of the 2016 resolution, by addressing concerns emanating both from the states and companies, but also by trying to understand the dynamics of such relationships in different thematic and geographical contexts.

- While research by Gary King, Jennifer Pan, and Molly Roberts underscores the role of states based on their theory of collective action, their views fall short. Citizen Lab has since been realized that states and companies have a shared responsibility.

- McKinnon's Networked Authoritarianism which is the foundation of the work that Ranking Digital Rights examines this synergy between states and companies.
- According to Citizen Lab research findings, corporations are still under the pressure of the state. For example, the Chinese government downloads responsibility for censorship on to the private sector. So power and efforts to control are being pushed down in a distributed way. What we see in data produced by Citizen Lab is evidence of how this system works. It's not practical for the government to directly control every aspect of censorship, they need the participation of the private sector. Pressuring companies to follow "self-discipline" is how the government can be effective.
- Also see the work of Perry Link on what he calls the Anaconda in the Chandelier, which offers some insights on censorship in China and the environment it creates and Rmack who uses the metaphor of likening China's system of information control to a complex industrial project like a hydro-electric dam. This is an apt way to describe what Citizen Lab observed.

2. THREATS POSED BY AN ERA OF NEW LAWS AND TECHNOLOGIES

2.1. Laws and practices on surveillance

While the striking down of the Safe Harbour Data sharing agreement after the Snowden revelations offered some hope, regretfully, however, many governments have been adopting laws or proposing legislation that increase their intrusive powers of surveillance or that seek to legalize post facto the privacy invasive practices of their security services in ways that fall short of applicable international human rights standards. NGOs have been challenging powers conferred by such legislation in both national and European Courts, for example, the successful challenge to the UK's rushed Data Retention and Investigatory Powers Act (DRIPA) of 2014. Let's look at some of the laws:

China

China introduced new anti-terrorism legislation in December 2015. While the new law does not go as far as requesting companies to hand over encryption keys, it does require companies hand over technical information and help with decryption.

United Kingdom

After the challenge to DRIPA, the UK passed the Investigatory Powers Act (IPA), nicknamed by privacy experts as the "Snoopers Charter," because it authorizes the Government Communications Headquarters (GCHQ) to engage in bulk interception, acquisition, and equipment interference of 'overseas-related' communications and communications systems, comprising of communications "sent or received by individuals who are outside the British Islands."

Germany

Germany adopted the Communications Intelligence Gathering Act. The act authorizes the Federal Intelligence Service (BND) to gather and process communications of foreign nationals abroad. Some of the world's largest internet exchange points (IXPs) are situated in Germany, thus making the country a central hub for significant portions of the world's internet traffic.

France

Two weeks after the November 2015 terrorist attacks in Paris, during which 130 people were killed, France adopted the International Electronic Communications Law. The law officially recognizes the powers of the French Directorate General for External Security (DGSE) to intercept, collect, and monitor communications "sent or received abroad."

2.2. Laws and practices on data retention

While the striking down of the EC Data Retention Regulations 2009 by the CJEU on the basis of necessity and proportionality offered hope, there are still concerns on privacy and cybercrime issues caused by blanket retention/mass surveillance of data, especially data gathering capabilities that are not authorized on the basis of a judicial warrant.

- The EU's General Data Protection Regulation, adopted in 2017, offers a good data protection framework, but also leaves a lot of room for interpretation about the scope of protection offered to data subjects. Other initiatives, such as the current revision of the EU ePrivacy Directive, could help developing the data protection principles that should underpin a digitized society.

Data retention in Europe

The Tele 2-Watson case found for the first time that imposition of obligation on companies is a violation of the right to privacy. However, there has been a **lack of implementation by EU member states of the Tele 2/Watson case recommendations.** Privacy International reviewed legislation in the EU and found that all laws are not in compliance with the ruling. There is a risk that human rights experts and others are going one way and states the other way leading to an ever increasing gap. This raises issues of rule of law, for instance if the EU countries do not respect decisions, and this goes beyond human rights violations but rule of law.

2.3. New Forms of Surveillance

Introduction: Human Rights, Big Data and Technology

Big Data analytic and information tools are also used for predictive policing which may lead to discrimination. Is it time to consider whether fundamental human rights concepts and approaches need to be adapted to meet the rapidly evolving technological landscape.

New forms of surveillance by police officers and intelligence services

- **Social Media Intelligence**

Social media intelligence (SOCMINT) refers to the techniques and technologies that allow companies or governments to monitor social media networking sites (SNSs), such as Facebook or Twitter. Social media intelligence may include tools to collect, retain, and analyse a vast range of social media data and interpret that data into trends and analysis.

How is SOCMINT misused by governments?

The UK Chief Surveillance Commissioner **commented** in 2015 that "Just because this material is out in the open, does not render it fair game".

Privacy International recommends a detailed study by the SR on this topic.

- **IMSI catchers and biometric technology**

Such technologies can be used to identify cases, for example, the case of London police using facial recognition technology in the Nottinghill Carnival protests. Such surveillance in public spaces has implications on the right to peaceful assembly, protests and privacy.

3. Recommendations

There are two main routes to the protection of rights online, namely, the technological and the legal. The UN should continue working with both in order to devise policy responses that bridge the two. Here, I will present a few examples of technological routes that have been proposed in order to protect privacy, freedom of expression and a broad range of other rights online.

3.1. Technological routes

- Bulk Collection of Signal Intelligence: Technical Options. Committee on Responding to Section 5(d) of Presidential Policy Directive 28: The Feasibility of Software to Provide Alternatives to Bulk Signals Intelligence Collection.
- Better algorithm design instead of content controls.
- Encouraging companies to enable secure communication in their networks to protect against unlawful interception, such as the use of https protocol including the use of encryption and other privacy protection tools. A good example is the work being done by the Open Technology Fund and also the Privacy Enhancing Technologies Symposium (PETS).
- Explore filtering, meta tags and relocation technologies to protect individual privacy in the right to be forgotten cases while protecting the public's right to know which also constitute part of the right to freedom of expression. See the case of A.T. v. Globe24H.com, the Supreme Court of Canada ruled against Google by asserting global jurisdiction over the internet and the ruling in ***Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*** (2014) conflicts with the Canadian ruling.

Legal and policy routes

- Address thematic dissonance at the UN For a, for example, reconciling the 2016 Human Rights Council resolution on the right to privacy in the digital age which notes that that profiling of individuals may lead to discrimination and he Security Council resolution on counter-terrorism, calling for profiling of all air travelers and widespread collection and sharing of personal data, as well as introducing biometric technologies on a mass scale.
- The post-Snowden era and "legalization" of the surveillance market. Case in point is the analysis by the National Endowment for Democracy under their series "Networked Authoritarianism".
- Encouraging corporate responsibility, for example, the work being done by Ranking Digital Rights.
- Monitoring inter-regional inter-jurisdictional issues such as the potential conflict been the CJEU Safe Harbour ruling and the pending case of ***Microsoft Corp. v. United States***.

- On data retention, a good case in point is the 2016 Germany case in which a data protection authority in Germany prohibited Facebook from collecting and storing the data of WhatsApp users in the country. For good measure, the authority also ordered Facebook to delete all data already forwarded by the app. Also, see the panel discussion of Joss Wright, Ross Anderson, and others with the UK's Parliamentary Science and Technology Committee regarding the UK's Investigatory Powers Bill available here: http://parliamentlive.tv/Event/Index/34da6c14-73c4-45c0-bc56-c8596fd14117/.
- In 2017, the Canadian Supreme court made important rulings on privacy by upholding citizens' Charter rights against unreasonable search and seizure by recognizing that text messages, "in some cases," deserve privacy protections. In 2014, in **R V Spencer** it also ruled that the request for an IP address infringed the Charter's guarantee against unreasonable search and seizure.
- On balancing security and liberty, see: S. Landau, Testimony, Hearing on "The Encryption Tightrope: Balancing Americans' Security and Privacy", Judiciary Committee, United States House of Representatives, March 1, 2016. https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy/