SURVEILLANCE AND COMMUNICATIONS INTERCEPTIONS- ABRIDGED

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

Topics to be addressed:

Trends at UN for a as well as at regional and states levels and new forms of surveillance by police officers and intelligence services such as social media intelligence.

1. UN FORA LEVEL

2013: Over emphasis on states in the post Snowden revelations.

Concerns about the right to privacy in new surveillance laws and practices: Soon after the Snowden revelations and public outcry, the UN's role to monitor increased. They put surveillance under spotlight. The UN particularly the Human Rights Council, the UPR and the UNGA have addressed this and also the independent bodies such as the Human Rights Committee and Special Procedures have increasingly addressed both freedom of expression and privacy in the period leading to the first High Commissioner Report in 2014, for example, see reports by Frank La Rue, former SR on the right to freedom of opinion and expression.

This led to the first OHCHR Report in 2014 which raised deep concerns about the implications of digital surveillance practices by governments, and their damaging impact on human rights, including the right to privacy. The report recommended effective and accessible judicial, legislative or administrative remedies for violations of privacy through digital surveillance and also the establishment of strong legal protections to ensure that such violations do not happen in the first place.

Developments since 2014 OHCHR Report.

After 2014, the UN has continued to pay significantly increased attention to modern forms of communications surveillance and their effects on the right to privacy and other human rights.

- In its 2015 resolution on the right to privacy in the digital age, the Human Rights Council expressed deep concerns at the negative impact that surveillance may have on the exercise and enjoyment of human rights, most notably the right to privacy.
- By establishing the UN Special Rapporteur on the right to privacy at the end of 2015, the Council filled a significant gap in the international human rights protection system.

- The Universal Periodic Review in 2015 witnessed increased attention on issues of privacy in the digital age: some governments made recommendations related to modern communications surveillance law during the reviews
- These recommendations constitute an important sign that the right to privacy is finally receiving due attention within the UPR framework.

2016: A Shift In Focus: New Developments on the Right to Privacy at the UN?

- 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.

- Two significant examples of this new focus are the analysis by the UN Special Rapporteur on freedom of expression and the language contained in the UN General Assembly resolution on the right to privacy in the digital age.

UN General Assembly resolution on the right to privacy

- In December 2016, the UN General Assembly adopted its third resolution on the right to privacy in the digital age. The resolution maintains the language on state surveillance contained in the previous text (adopted in 2014) but it builds upon it by adding significant provisions to address the role of companies

2018: OHCHR Expert workshop & the need to find an equilibrium.

The need to strike a balance is backed by research that reflects on surveillance practices, which is why this panel is focusing on surveillance and not states surveillance as in the earlier years.

The Snowden revelations which mostly fingered the U.S Government, for example, see research by Landau and Perry King, might explain why there was an obsession on states. Also subsequent research by Gary King, Jennifer Pan, and Molly Roberts underscores the role of states but as Citizen Lab show, their theory of collective action falls short.

Current research makes a case for a shared responsibility between states and companies. This includes:

- McKinnon's Networked Authoritarianism which demonstrates the way the live streaming industry is being regulated in China is a good example of the wider arguments she makes on intermediary liability in China. I also refer to Ranking Digital Rights Reports.
- Corporations are still under the pressure of the state. 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.
- Perry Link on what he calls the Anaconda in the Chandelier, which offers some insights on censorship in China and the environment it creates
- In this blog Rmack also has references this 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.
- Also, in my research across Sub-Saharan Africa, we have countries were Telcos and ISPs are government-owned. Rules relating to intermediary liability change. Such countries, mostly include former communist countries, include Angola.
- Also, David Kaye, in his remarks during an interview with Al Jazeera, albeit on internet shutdowns, acknowledges that the limitations that companies may have in pushing back.

Need to address thematic dissonance at the UN Fora

- Right to privacy at the UN in 2017 – In his blog, Don't let your left hand know what your right hand is doing, Falchetta notes with concern how a 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 clawed back a progressive 2016 Human Rights Council resolution on the right to privacy in the digital age, noting that profiling of individuals may lead to discrimination.

2. STATES AND REGIONAL TRENDS

Important Inter-regional developments.

- Regionally and inter-regionally, while the CJEU struck down the Safe Harbour Data sharing agreement after the Snowden revelations, in the U.S., the pending case of ***Microsoft Corp. v. United States*** might claw back that decision leading to conflicting jurisdictions.

- ***Right to be forgotten:*** This concept raises a tension between individual privacy and FOE: In the case of A.T. v. Globe24H.com, the Supreme Court of Canada ruled against Google by asserting global jurisdiction over the internet but also see the ruling in ***Google Spain***

SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (2014) conflicts with the Canadian ruling.

- 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".

Trends on surveillance legislation

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. The state of new legislation particularly in Europe and around the world, for example, Kenya, Colombia and China have passed new surveillance laws thereby putting into law the secret practices of intelligence services. Such laws, some of which have been passed in response to increasing terrorism incidents, have not been in compliance with human rights according to the United Nations 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.

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."

Trends on Data Retention

This has been a problematic area.

- CJEU's striking down of the EC Data Retention Regulations 2009 as unconstitutional, largely due to issues of necessity and proportionality.
- Privacy and cybercrime issues caused by blanket retention/mass surveillance of data
- Data gathering capabilities to be authorized on the basis of a judicial warrant, rather than gathered a priori with judicial warrants being necessary only to access the data.

  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/
- The EU's General Data Protection Regulation, adopted earlier this year, 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

Tele 2-Watson Benchmark

This case found for the first time that imposition of obligation on companies is a violation of the right to privacy.

The 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, including in countries such as Colombia.

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.

Emerging good practice. 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.
- Other researchers suggest better algorithm design instead of content controls.
- I will present more on technical routes during the workshop on Information Controls on Wednesday at 2pm.

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.

The use of 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.