07

PRIVACY

ANDREW PUDDEPHATT, GLOBAL PARTNERS DIGITAL

INTRODUCTION

The purpose of this webinar is to discuss the meaning of privacy in a cybersecurity and human rights frame, exploring how the notion of privacy and its realisation is changed by the Internet, technically, commercially and normatively. We will identify the range of factors shaping the way that privacy is being affected online and the roles and responsibilities of different stakeholders.

THE WHAT – WHAT IS THE TOPIC ABOUT?

Privacy has different meanings in different contexts and societies. At its heart is the idea of the security and integrity of a human being and their control of their immediate environment and what is known or can be known about them.

Exact definitions of privacy are elusive – national and international courts have refused to provide clear definitions of privacy. At a general level privacy is understood to be protection from "arbitrary or unlawful interference with his privacy, family, home or correspondence, … [and] unlawful attacks on his honour and reputation." Thus protection of reputation (from defamation) is linked to privacy which creates tensions between freedom of expression rights and privacy rights. Anonymity and encryption, sometimes referred to as rights by activists, should be more properly regarded as enablers of rights – both of privacy and free expression.

It should be noted that privacy is not the same as data protection. Data protection policy has rules designed to address the systematic collection of data about individuals and the policies applying to all personally identifying data held by designated 'data controllers'. Privacy, however, is more fluid concept applying to information about which a person may have a reasonable expectation of privacy.

Throughout history the understanding of privacy has changed depending upon societal and technical developments. While the notion of personal integrity and dignity lies at the heart of privacy as it does of all human rights, it has a different meaning in a communal village to that of a modern city. Two big factors affecting the way we understand privacy are the emergence of generalised private property (single households) and communications technology. For example the modern understanding and debate about privacy grew from debate about publishing photographs of people in newspapers at the end of the nineteenth century. There is therefore no exact boundary to the definition of privacy, and a dramatic technological change like the Internet will inevitably re-shape understandings of privacy. This may help explain the contrast between what people say about privacy and the internet and how they behave.

THE WHY – WHY IS THIS TOPIC IMPORTANT FROM A HUMAN RIGHTS PERSPECTIVE?

Technically the internet enables the collection of new types of personal information; facilitates (and economically demands) the collection and location of personal information; creates new capacities for government and private actors to access and analyse personal information; creates new opportunities for commercial use of personal data and sets new challenges for regulation given the transnational nature of the internet.

In addition new internet services redefine the privacy environment dramatically - cloud computing (raises questions of security, data breaches and ownership); search engines (systematically tracking and monitoring our behaviour); social networks (depend on a company led exchange and analysis of data provided by users); the mobile internet ties internet use to geo-located devices; and the Internet of Things connecting all potential objects which together convey a complete picture of our lives.

And governments are increasingly relying on digital platforms to provide services through use of data with designated e-identities that allow services, banking, voting, health monitoring etc. The sheer volumes of data available privately and publically make it difficult to conceive that governments won't seek to access it.

Moreover governments have become increasingly concerned about security issues online – for both legitimate and illegitimate reasons. All governments are attempting to access information online to the limit of their technical ability, raising serious concerns about:

- Scope of surveillance (who are the targets and how big is the net)
- Legal framework of surveillance
- Use of mass metadata searches excluded from legal accountability
- Weakness of oversight
- Absence of legislative competence
- The provision of many internet services based on a business model based on advertising.

We trade or cede our privacy in exchange for free services. Such service models either directly depend upon exposing private information (Facebook), or they intrude on privacy to create efficiencies (e.g. tools that optimise searches based on tracking user preferences). Generally there is little real public pressure or incentives to challenge this model and informed consent to data use for users online is complicated by range of different applications, complexity of terms of use, and apparent public indifference.

So the key question is: how to protect privacy and individual liberties while enabling the free flows of personal data and maintaining security of personal data. This will depend upon strong security both technically – encryption – and normatively – with appropriate legal rules governing access to and use of personal information.

THE WHO – WHO ARE THE MAIN PLAYERS?

There are two areas to focus on -

- The implications of developments in private sector and where the technologies and markets are leading.
- The use of personal data by governments – not just security surveillance but wider recasting of citizen/government relationship digitally – tax, health, etc.

At the heart of the notion of privacy lies sense of personal integrity and dignity whatever the social context. At the core of this is sense of ownership and control, i.e. consent to use of information (basis of data protection system) and what can be known. Current business models require us to hand over ownership of our data to companies in exchange for benefits -use of that data is loosely regulated if at all. How do we control this?

Companies should practice greater transparency about data management practices, provide accessible and reasonable terms of service, explore shift of business model to one where there is greater user control of data with the ability for users to own data and grant permissions for use and encourage higher standards of encryption and anonymity, as both are enablers of privacy rights and publish details about government requests for user data.

Governments should commit to ensuring user security and privacy as a policy goal, commit to freedom of expression (aware of the need to balance both rights), understand cybersecurity as embracing users interests, be transparent about the rationale and scope of surveillance or other measures violating privacy and ensure that rules governing surveillance and privacy violations are grounded in law, consistent with international principles and subject to supervision by independent courts and finally regulate effectively e.g. by having technical skills on regulatory bodies.

Lastly civil society has an important role to represent user rights and consumer interests, to bring concerns from excluded and marginalised groups, to provide innovative ideas and policy options; to champion a human rights and public interest approach to privacy policy.

THE WHERE – WHERE IS THIS TOPIC BEING ADDRESSED?

Ten years ago, the International Law Commission concluded that “no homogenous hierarchical meta-system is realistically available” within the international legal order to resolve detailed differences among the separate spheres, that this would have to be left to the realm of practice. This means little prospect of a global privacy policy – so how can it be ‘practiced’?

Among the important venues for policy are:

- **Policy forums** - International Conference of Data Protection and Privacy Commissioners discussions, Internet Governance Forum
- **UN normative standards setting** such as the UNGA (resolutions on privacy),
- Recommendations such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
- **UN Special procedures** e.g. UN Human Rights Commissioner (recent report on privacy); new Special Rapporteur

- **Technical bodies** – e.g. Internet Engineering Task Force (IETF) - work on increased encryption standards, RFC 6973, RFC 6772, RFC 6280
- **Regional courts** – ECHR generic privacy cases and **national courts** – Yahoo, Louis Feraud judgements.