About the session:
In the context of a seemingly increasing number of large data breaches in recent years (OPM, Target, Anthem, etc), the objective of this session was to understand whether organisations dealing with personal data (companies, governments) are investing enough resources to protect and secure users’ data, and if not, why. One of the key cross-cutting considerations was to assess the cost of such data breaches and whether this cost, or negative externality, is a sufficient incentive to improve organisations’ behaviors in protecting user data.

Moderator & organiser: Nicolas Seidler, Senior Policy Advisor, Internet Society
Speakers:
• Bruce Schneier, CTO Resilient Systems Inc., international security expert, cryptographer, security & privacy expert, and author.
• Priya Kumar, Research Analyst, Ranking Digital Rights
• Michael Nelson, Public Policy, CloudFlare, teacher at Georgetown University
• Drew Mitnick, Policy Counsel, Access Now

Session notes: Karen Rose, Senior Director, Strategy & Analysis, Internet Society
Session report: Nicolas Seidler, Senior Policy Advisor, Internet Society

> Summary of discussions <

Are we seeing a greater number of data breaches as of late?
• While it may seem that we are reaching a record high of large scale data breaches, panelists felt that 2015 is more the year of “the story about the breach” than necessarily a reflection of increasing numbers.
• The scale of the breaches might be bigger in recent years however.
• Exposure of top Executives through these breaches may be an effective way to trigger corporate changes for greater data security.

Are organizations collecting more information than necessary?
• One issue that was raised is that companies may be collecting more information than they actually need, because collection and storage is cheap, and they hope to find use for this data down the road. Doing so, they are exposing themselves and users’ data at risk of breaches.
• As every company is becoming a digital company, the risk of storing data is extending to companies that are not pure ICT companies, but also traditional industries dealing with
digital data (e.g. banks, retail, airlines, insurances, etc). These organizations may not have the same “security culture” as pure ICT companies.

- The panel couldn’t identify companies that are visibly taking the lead in dialing back in terms of the data collection and storage. This may indicate that more conservative data collection practices isn’t an important market differentiator.

**Transparency on data collection and security**

- Transparency of companies around data breaches is essential for the market to lead to better outcomes in terms of user data protection. Rankings, insurances rates and media exposure can help users be more informed in order to switch between services depending on their data security practices.
- The question is not only what was breached, but what information are companies collecting that makes them a tempting target. Many consumers are not aware what data they have on them in the first place, and few organizations are transparent on data they collect, and how they protect it.
- Some panelists also raised that the “notice and consent regime” (by which people agree to a particular service’s terms of services) is generally not an effective competition-based system, because people can’t realistically opt out of an e-mail address, or a credit card, etc.

**Public administrations**

- Beyond companies, question was raised whether governments are aware of the risks they are taking when they collect data.
- The case of the US Office of Personnel Management data hack was mentioned, and it seems there is low evidence that lessons have been learned towards better protections.
- It was also mentioned that often with government services, there is no notice and consent (e.g. signing up for a driver’s license).

**Should there be different levels of responsibility for different levels of data?**

- A few panelists made the point that this is already the case in the offline world, e.g. for health data.
- Some classes of professionals also carry greater responsibility depending on the sensitive nature of information they deal with: priests, lawyers, doctors, etc.
- Some panelists raised there should be similar levels of due diligence rules in the security space as we have in the financial disclosure space, but that it may be challenging to achieve. There is a lot of outsourcing and data can be handled by many companies down the line.

**Internalizing the negative externalities of a data breach**

- The fallout of data breaches was characterized throughout the discussion as a negative externality (much like pollution can be a negative externality on the environment based on industrial activity), and the question arose on who is actually bearing the costs (in economic terms: internalizing the negative externality).
• Most thought that users, not companies or organizations, are ultimately baring the costs of these breaches.
• Some argued, that the two major ways to get companies/organizations to internalize the externalities are Liability and Regulation, while others made the point that a mix of market dynamics with light regulatory intervention could be effective.
• Example was given of automobile safety, where regulation has played a role along ranking system and consumer reports that influence consumers' purchasing decisions and can push the industry to adapt.

Other challenges
• Challenge for companies: government data retention laws that ask companies to keep data longer than they would for businesses purposes.
• Need to broaden the protections to “user information”-any piece of information that can be connected to a user (and not limiting to so-called “personal information”, that might be narrowly defined)
• Better security with third parties? An argument was made that 3rd party contractors (e.g. cloud services) that manage data are being more closely scrutinized on their practices. There is a trend towards companies outsourcing their IT functions because the companies themselves will not be able to keep up with cutting edge data security practices.
• As long as the information age is based on collecting and monetizing data, we cannot dissociate these business models from the risk of getting more and more surveillance.

Conclusions/outcomes
• If market-based pressure from data breaches is to be effective in generating better data security practices by organizations, it needs to be based on transparency and consumer awareness. Users can’t make decisions and influence company practices based on information they don’t know about.
• All agreed that transparency, competition, innovation and some regulation may be needed to generate better data protection practices from company and administrations.