Introduction by President ad interim Philippe Gillet and Arjen Lenstra, Chairman
The Chairman welcomed the participants and introduced the President.
The President noted with pleasure the large number of participants. He noted that today’s topic for discussion was not purely technical, while EPFL is a technical institution. But, given the development and importance of technology, it is important that technologists also discuss policy issues.
In particular, recent revelations regarding government surveillance have shaken out confidence in the freedom and openness of the Internet. So it is time to start a debate and to find solutions that will allow us create the truly free and open Internet that we all cherish.

Caspar Bowden, “FISA, PRISM, and Data Protection”
Cloud Computing allows you to scale your computer power easily and is a major development, but users have to be shown that it is safe and secure. But this is not the case in the present legal environment, in particular with respect to US law.
Numerous specific US laws and court judgements authorize widespread surveillance, in particular for international telecommunications, which can be intercepted without court warrants. The laws allow surveillance of activities such as cloud computing even if they are not alleged to be criminal nor related to national security. Such surveillance would be illegal under the European Convention on Human Rights.
This situation can be addressed by raising awareness of the situation, and by building a European cloud.

Nikolaus Forgó, “Privacy and European Law”
Currently debated issues are not really new, they go back to the Internet business model, in which apparently free services are in reality funded by turning user-provided information into a product that can be sold. Many Internet promoters are pushing the idea that privacy is dead and should no longer be assumed. Indeed, if people agree to waive privacy, there is no problem. But there has to be informed consent, which is typically not the case for contracts of adhesion formed by clicking on a web site. Typical waiver-of-privacy clauses are extremely broad. In addition, consent is not requested regarding the architecture, which is determined by technical bodies; side effects of the architecture may be difficult to understand by non-specialists.
In Europe, data protection laws are very stringent, including control by independent data protection authorities (who however tend to be underfunded). Personal data can only be processed if allowed by law or if the person consents. However, many important questions remain open because courts have not yet ruled on certain issues. Issues related to intelligence services are not covered by EU directives or regulations.
A new directive and regulation are being considered, but are unlikely to result in any major changes compared to the current situation.
Axel Arnbak, “The #NSAFILES and the question (most) law scholars don't ask: can law make a difference?”

Concerns regarding lack of privacy of cloud computing were initially dismissed as scare mongering by US providers. Recent revelations have shown that we are moving towards a regime of total surveillance. US law does not restrict surveillance of foreign persons, on the contrary, it explicitly facilitates total surveillance, and the surveillance is not subject to meaningful court review. Cloud computing facilitates the surveillance, as does the concentration of most Internet markets (including for security certificates). Intelligence agencies collect and analyse commercial data and political information as well as data related to national security. They also share such data with each other. Such agencies are politically powerful and employ large numbers of very skilled people.

Political leaders in Europe have tended to deny that there is an issue. It is unlikely that US laws will be modified to protect privacy of non-US persons. Reform of Internet governance or of the architecture also appears unlikely or would not be effective. Overall reform of European laws is not likely to be effective, but some specific new provisions could help, such as increasing user awareness, whistleblower protection, and increased penalties for violations of European law. Application of international human rights law is difficult because spying is a common practice and there is no enforcement jurisdiction. However, a case could be brought under the European Convention on Human Rights. But it is not clear what the practical effects of a ruling would be regarding surveillance by non-European agencies. Leaking and whistle blowing might be more effective, and is, to some extent, protected under the European Convention on Human Rights.

Bruce Schneier

The issue of privacy on the Internet goes well beyond government surveillance. A great deal of data is provided on the Internet and can be captured and collated for various reasons, including commercial. Indeed, data is natural by product of the information society and the increasing use of computers and data networks. In particular social networking sites. Data is increasingly stored and increasingly searchable. Most data might well migrate to cloud computing for cost reasons.

Usage of data depends on national laws, but, in the US, there is little protection of data. And intelligence agencies are largely exempt from privacy laws. Intelligence agencies are merely doing their jobs, which is to collect as much data as possible.

New players are building closed platforms so as to maintain control of the applications and users. So users are losing control both of the data and of the applications, which may be in their interest (lower cost, higher value added services). Information will be stored permanently.

There is a convergence of commercial and government interests. People have an expectation of privacy, meaning control of their information. But this expectation is no longer valid and privacy policies have to be stated explicitly. As technology evolves and becomes more widely implemented, there will be even less control of data, thus less privacy. But privacy is a fundamental human need: it is a trade off between power and liberty. Transparency and accountability are required.

We can shape the use of technology, through laws and rules. Technology alone is not the solution because most people cannot use sophisticated technologies.
Richard Hill, “Internet Freedom, Snowden, and Dubai”

Various proposals for treaty provisions to increase international cooperation to improve cybersecurity and to combat spam were opposed by various countries (in particular the United States) during the ITU’s 2012 World Conference on International Telecommunications (WCIT-12) in Dubai, primarily on the ground that such provisions could be invoked by non-democratic states to impose censorship and restrict freedom of expression. Such arguments seem strange today, in light of the recent revelations regarding US and other countries’ pervasive surveillance of electronic communications. Be that as it may, a large block of developed countries did not sign the treaty approved in Dubai. This situation creates uncertainty regarding cooperation with respect to security issues and can lead to a continuation of unilateral, and extraterritorial, assertions of national powers, including surveillance and cyberwarfare. Yet there are continued calls for cooperation, in particular at the bilateral level. It is suggested that international cooperation would be a more appropriate way forward, and that it should be based on specific principles that are based on universally recognized human rights.

Bill Binney, “Democracy and Surveillance Technology”

There is insufficient Congressional oversight of current US surveillance programs, which threaten democracy and violate the US Constitution. These programs were established without properly informing Congress. The judicial oversight is ineffective. Data are used by law enforcement agencies (and not just in the US) to construct cases allowing them to obtain warrants. There is now resistance in Congress to these surveillance programs and it is possible that they will be curtailed. A more effective program, which would also protect privacy, would limit surveillance to contacts who are within two degrees of separation of a known suspect (linked to a person linked to a suspect); the current system generates too much data and is ineffective.

Jacob Appelbaum

It is important to make the facts public, so that an informed discussion can take place. But those who know the facts cannot reveal them because it would be illegal to do so and it might result in going to prison. Cryptography is a tool that can help to protect privacy. Surveillance should be strictly limited and there must be an appropriate legal framework. At present, data retention in the US is too long, and analysis of metadata is not restricted. This can be used to create social graphs. Communication systems should be designed to prevent this sort of surveillance. Policy has to be allied with technology to protect privacy.