Next-Generation Internet Consultation

Main conclusions from the web-workshop with experts on privacy and personal data spaces

Friday 9th December 2016

Introduction

The European Commission launched the initiative "Next Generation Internet" aiming at innovating at the speed of the Internet. As part of the supporting consultation process this on-line workshop focused on Privacy and Personal Data spaces. Well recognised experts with different background participated (see list at the end) and discussed the following points:

- Vision
- Research and Legislation
- Key research and business challenges
- Possible building blocks

Vision

The internet will be THE digital environment in which we live and will potentially know everything about us. If cost of privacy is perceived as negligible then market interest will prevail.

The debate around the evolution of the internet should be at the political level to find alternative paths for Europe. There is not enough attention to privacy in the public debate today.

Europe should be faithful to the decentralised design of the original internet. Failing to do that will hamper trust in the Internet development.

IOT and Big Data create new and unknown power balance between providers and users that needs to be framed by European values e.g. privacy protection, decentralisation, collaboration, and transparency.

Research and Legislation

There is a misalignment between the interest of users and adopters (SMEs and Start-ups) and the policy/legislation notably the forthcoming General Data Protection Regulation (GDPR) mainly in timescale to comply with the law.

There is a tension between innovation and legislation that can be a limiting factor for instance some aspects of GDPR are not clear enough to allow safe investment in R&D&I.

If requirements come from the regulation, then companies will just do a minimum effort to fulfil them; if protecting privacy becomes a key business differentiator, then this will drive investments, developments and services and products.

The legislation seems to be centred more on the end-service, but not that much on the hardware, software, firmware on which it builds upon or on the supporting/associated third party services: hence it may become difficult for the end service to integrate any privacy and to trust them.

Key research and business challenges

Privacy might not be a top priority: users/consumers demonstrate they are keen to give away many personal data through large aggregators in exchange of free services. The challenge is how to move towards redistribution and decentralisation of trust.

There is the perception that GDPR will make release of personal data among providers more difficult than today and/or more expensive because of liability and reputation; in addition the barriers created by the legislation will be too high for new (SME/start-ups) entrants while the legislation will not significantly change existing market players' behaviour.

IOT is seen both as an opportunity but also a major privacy issue for instance through proliferation of hardware of unknown origin.

Possible building blocks

There is a much needed effort to be done on cryptographic advances and that, in many cases, can be used to support other key building blocks.

Transparency: end-users should be aware of the level of privacy they get in accessing a given service for instance: through certification marks easily understandable; open source software checked by trusted parties (such as hackers or NGOs) to form a decentralised trust; this could also be extended to open/certified firmware and hardware design.

Ease of use: the barrier for privacy should be minimised in terms of ease of use.

Decentralisation technologies are key but should not increase the number of actors which ultimately is harmful to trust.

Cost: there should be an understanding of what is the cost of giving away personal data as a negative incentive just like for the CO2 emissions although privacy is a very subjective matter.

Business Model drive: any successful alternative model to "GAFA" (Google, Apple, Facebook, and Amazon — the 4 most powerful American technology companies) will have to integrate socio-economic values as opposed to a plain share of personal data model where Europe cannot compete.

H2020 grants: enshrining in all H2020 projects the principle of personal data's attribute release inside the grant in order to ease personal data exchange among parties (including commercial parties and cross-border) similarly to what was done for the open research data pilot.

There should be bridges between basic and applied research in the funding system encouraging creativity, flexibility within short revision cycle.

Disclaimer:

The views expressed in this publication are those of the authors and do not necessarily reflect the official European Commission's view on the subject.

NAME	COMPANY
Florian Kerschbaum	University Waterloo, security/encryption researcher
Carmela Troncoso	IMDEA, privacy researcher
Linus Nordberg	TOR project , Programmer
Hannah Short	CERN, user perspective
Niels van Dijk	SURFnet bv, Technical product manager Trust & Identity
Christos Kanellopoulos	GRNET, Software Engineer - Systems Architect