Keynote

Ivan Szekely, PRICON conference, 14 May 2018

Privacy challenges of our time

I am honored to be here and to deliver a brief keynote and an introductory presentation to the participants of the PRICON conference at the Institute of Economics in Zagreb.

1.

Privacy is facing serious challenges in these times.
Some say: "Privacy is dead, get over it", according to the infamous quotation from Facebook founder Mark Zuckerberg. In a more critical wording of Pete Cashmore, "Privacy is dead, and social media holds the smoking gun". You can of course reply: *Your* privacy may be dead, but not mine – but in this debate there is no equality of arms; and it is almost impossible for an individual to oversee and understand what happens with the information about her private life, what conclusions are drawn from this information, and what are the consequences of analyzing and using this information. (It is telling that those who say that privacy is dead have the necessary power to protect their own privacy...)

The reasons are manifold. Data-driven economies, national security concerns, the monetization of personal data – but a crucial factor behind all this is the rapid development and the possibilities of information and communication technologies: computers, networks, information gathering and analyzing tools.
A few decade earlier theoreticians discussed the concept of the Social Construction of Technology – today some politicians and businessmen seem to believe in the „Technological construction of society", including the limits of privacy. Naturally, privacy is a broader concept than data protection but it increasingly depends on how personal data are handled.

2.

Others say: People are not interested in privacy any more.
This is simply not true: even the digital natives are interested in their privacy, but in a different way, according to the changing social relationships. Numerous surveys and other researches – including PRICON – have shown the high level of concern about privacy in society. It is true that there exists a certain privacy paradox: people say they are concerned but do not act accordingly. – Why? Do they lie or mislead even themselves? No, it is the setting (the complicated procedures, the non-transparent systems, the offered benefits) that prevents them from acting accordingly.

But even if it were true that people are not interested in privacy, society would not be entitled to disregard its members' privacy. Similarly, one could not say that people are not interested in their health: they eat junk food, live an unhealthy life – so why should we bother with health safety regulations, instead of selling cheaper and more profitable products?

3.

Privacy is a right, privacy is a demand, privacy is a value. It is a constitutive public good, it is a core element of a constitutional democracy, a western type rule-of law society. It would be a mistake to think that, for example, FOI (or access to public information) is a collective right, a collective demand and a collective value, while privacy serves only individuals: No, privacy itself is a public matter in society.

Again others say that privacy is a Western concept that does not work in the cultural East, nor in the globalized networked societies. On the contrary: people in the Eastern hemisphere do have a demand for, and a value of, privacy (sometimes less of codified rights); they can even enjoy virtual privacy in the most crowded circumstances, due to their psychological capacities and traditional techniques. And even the seemingly uninterested young generations, the digital natives, have developed their protective techniques, different from the older ones, as the contexts and boundaries of privacy are changing rapidly in today's networked societies.

In Edward Snowden's words: if you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say. Snowden's revelations showed that not only criminals are under constant surveillance but virtually everybody. And the recent Facebook and Cambridge Analytica scandal revealed that not only targeted pizza advertisements are at stake but the influencing of the behavior and actions of masses of people. This shows that privacy has a much broader connotation than many would think: it includes personal integrity, self-determination, aspects and preconditions of autonomy, freedom of expression, and lastly freedom.

4.

But how could Facebook and Cambridge Analytica (which represent only the tip of the iceberg) get this far in the unlawful and unethical use of personal data of hundreds of millions of people? In my opinion, it had three main factors:

(1) predictive data analysis
(2) psychological/emotional influence
(3) real time targeting

– all of them have been possible by the use of new ICT.

Naturally it is not only the information superpowers, the NSAs, the Facebooks, the Googles on the one side, and the individuals on the other side: there exist a range of those who process and use personal data for different purposes, big and small, public and private data controllers, intermediaries, including ourselves. Their understanding and use of new ICT determine their capabilities, even if we don't understand what is happening with our data.

Sometimes the use of our personal data by others is directly advantageous for us, sometimes it is disadvantageous but necessary, and sometimes we pay a disproportionate price for immediate benefits, because we cannot oversee the consequences (and we are living in a Present Continuous Tense anyway). And there are such data intensive applications without which we were simply not able to conduct our daily business or communicate with others. In order to understand the opinion, attitudes and behavior of the data subject, of ourselves, conducting researches like PRICON is inevitable.

5.

And there are other important players in this landscape:

First, those who design, develop and operate the IT systems – in short, the IT professionals. As Lawrence Lessig stated: "Code is law." To make it simple: no matter what the law reads, business in general is conducted the way as the IT systems are coded. It is an exaggeration, but it would be a mistake to think that all code-makers are square-minded and blindly follow their masters' interests and values: research showed (one conducted by myself a few years ago) that they have a more complex view and attitudes in this field. Some of them develop PETs and tools, or reveal secret backdoors in confidential communication etc.

Second, there are still "traditional" lawmakers, too: they also need to understand new and future ICT, otherwise laws and regulations would become but "fig leafs" on the unethical operation of IT systems.

Third, researchers, research institutions, scholars, theoreticians are also important players, needless to say in this environment. But it would also be a mistake to think that all researchers are of a high ethical standard (as opposed to certain business or political entities), see the transferring of research data for direct political purposes in the Facebook case. Researchers may also be tempted to sell their research findings to privacy-invasive companies, in exchange of getting access to "Big Data", and even the ethically sound researchers – like us – cannot guarantee what their research findings will be used for.

Fourth, also important is the civil sector whose representatives try to get individuals understand what happens with their personal data, and represent their rights, raise their awareness, and influence legislation and regulation.

6.

So the landscape is complex.

However, there exists a less visible, much less researched, but important player: the Data Protection Authorities (DPAs) who are entrusted with the task of supervising all this; their role will be even more important after May 25 in Europe, and indirectly, in the global flow of personal data as well.

In the following I would like to direct your attention to the importance of whether DPAs have relevant expertise in ICT, especially whether they understand future and emerging technologies in the field of data protection and information privacy. I will now present the main findings of a recent research conducted jointly by Prof. Charles Raab of the Univ. of Edinburgh, and myself.