Protecting privacy also means preserving democracy

September 1 2014, by Alexandra Walther

Credit: © Alain Herzog

What impact does the proliferation of new mobile technologies have? How does the sharing of personal data over the Internet threaten our society? Interview with Professor Jean-Pierre Hubaux, a specialist in communication networks and privacy protection, a major field of IT security.

Jean-Pierre Hubaux as a professor at the EPFL's School of Computer and Communication Sciences. During the last decade, Jean-Pierre Hubaux and his team at the Laboratory for Computer Communications and Applications have focused their research efforts on privacy protection, in particular for mobile communication networks (and notably geolocation) and personal data (with genomic data as an

application example).

What type of personal data should we try to protect?

Nowadays, administrative, medical or legal data are mostly kept in digital form. And a plethora of personal data is now publically accessible, whether voluntarily or otherwise, over the Internet. The exposure of such records to the digital world poses fresh challenges as quickly as the Internet grows. At the same time, the propagation of new technologies such as smartphones and tablets threatens our privacy.

How have mobile technologies changed the situation with regards to privacy protection?

Cell phone companies must locate a subscriber's cell phone in order to channel communications via network antennas. However, locating our cell phone not only reveals our physical location, it also reveals when we are there, how long and even with whom. So far, this personal data is relatively well protected within the current legal framework. In addition, users pay a subscription to cell phone companies. Cell phone companies therefore generate a profit under a traditional business model of fee-based services. However, this is not the case for service providers such as Google, Facebook Mobile or Foursquare. How do these companies make money? They do so precisely by collecting and analyzing the personal data of users.

Free services therefore pay for themselves with our data…

That's right. What you do not pay in monetary terms, you pay by some other means, and often without your knowledge. Service providers obtain geolocation data: i.e. where you are, when, how long and with

whom. They can then cross-reference this data with the content of your e-mail messages and your electronic agenda or with the type of searches that you enter into their search engines. If you are also registered on a social network such as Facebook or Google+, then they've hit the jackpot. In other words, what you do not pay for with money, you pay for with your personal data. In the best-case scenario, this data is only used to send you targeted advertising based on your interests, gender, age, income level as well as the interests of your friends and colleagues…

Which other risks need to be considered?

A pessimistic, but plausible, scenario is that your personal data in digital form will be used for surveillance purposes, since governments can demand access to your data. Governments also already conduct surveillance on a massive scale, as revealed recently in NSA-related scandals. Targeted surveillance (sometimes performed secretly) is of course needed, notably to fight organized crime, but mass surveillance is unacceptable. Additional risks include harassment (e.g., blackmail) and identity theft.

To make matters worse, the legal framework lags behind service providers, which are generally U.S. companies based on a new business model whose profitability can only be achieved through the exploitation of personal data. In addition, mobile technologies are evolving at a breathtaking pace, which makes it even more difficult for legislation to keep up with our day-to-day reality.

But let me be clear on this: the Internet and associated services are a fantastic invention! Let's just say that often the most wonderful innovations have side effects, such as the larger carbon footprint caused in part by the increasing use of hydrocarbons or the rising number of cases of senile dementia caused by medical advances and resulting gains

in life expectancy.

But who would even want to take advantage of access to our personal data?

Well, your employer may want to know whether you have had job interviews with the competition. Your insurance company may decide to accept or refuse you as a policyholder on the basis of your absenteeism from work. Your bank may decide to reject a loan application on the basis of an assessment of how likely you are to remain healthy. Just consider the fact that for $100, a private company will analyze a sample of someone's saliva for simple DNA sequencing. For $5,000, that same company will provide a complete analysis of a person's genome. What transits over the Internet are not only your genetic data, and therefore any abnormalities (i.e. physical and mental defects caused by your genes), but rather a portion of your entire family's genome, revealed in a probabilistic fashion since you all share the same genetic makeup.

What would happen if privacy were to disappear?

Well, it would be the end of truth as we know it, the end of mutual trust and the end of democracy!

Imagine a world in which you could no longer trust your own doctor for fear that your medical records could fall into the wrong hands. Would you lie to your doctor to protect yourself? Under what circumstances and to whom would you lie in order to protect your personal data from being divulged at any time? It would be the end of truth because people would begin to lie methodically, which in turn would undermine mutual trust. If medical confidentiality can be eroded in this manner, imagine what would happen to confidentiality in electronic voting systems. In a democracy, the people are sovereign and must be able to vote as they see

fit without fear of reprisals.

In your opinion therefore, unfettered access to personal data is nothing less than a threat to democracy?

Absolutely. If voting secrecy is no longer guaranteed, will voters be subject to undue pressures as a result of their political affinities? Will they be forced to vote in a way that goes against their own personal convictions? All dictatorships violate the privacy of their citizens. All democracies have laws aimed at protecting privacy, which is paramount to preserving democracy.

What solutions do you propose?

Follow the money trail and the strategy will appear! According to game theory, a mathematical discipline borrowed from economics, it is possible to calculate the degree of motivation to perform certain acts. In other words, we can assess the financial cost of different strategies that the adversary has at its disposal to determine which one offers the best "quality-price ratio". The ultimate aim is to reach a point where none of the adversary's strategies is motivating because the cost exceeds the benefit in each case. In the area of geolocation, we have shown how users of geolocation services are able to preserve their privacy with an acceptable level of service quality. For instance, users can install a software application that hides their tracks, indicating only that they are in Lausanne but not indicating that they are actually in such and such office at the EPFL, for example. We have also quantified location privacy. Generally speaking, our contributions make use of probabilities and statistics (including inference techniques), communication protocols, applied cryptography and machine learning.

How about other disciplines?

It is important to encourage interdisciplinary approaches to address social phenomena associated with information technologies, law, economics, etc. Over the past few years, my laboratory has been working closely with geneticists from CHUV and the EPFL as well as with a start-up company, Sophia Genetics. We have also entered into discussions with telecom operators.

Provided by Ecole Polytechnique Federale de Lausanne

Citation: Protecting privacy also means preserving democracy (2014, September 1) retrieved 25 April 2024 from https://phys.org/news/2014-09-privacy-democracy.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.