A Global Conversation with Laura Brandimarte

DOES GOVERNMENT SURVEILLANCE GIVES TWITTER THE CHILLS?

On the 9th of October 2017, we had the possibility to meet Ms. Laura Brandimarte, Professor and Researcher at the University of Arizona. Professor Brandimarte gave us an interesting speech about the effects of government surveillance and in particular about her recent research on anomalous trends in users' behavior on Twitter after Edward Snowden's revelations made them aware of of the existence of surveillance programs.

The idea of a total, a global, government surveillance of citizens is surely something not new to us, as we can see from Bentham's Panopticon (a particular type of prison designed by Jeremy Bentham in the 18th century, where a single watchman could observe all the inmates without that this latter knew if they were being observed or not) or from the well known George Orwell's book "1984".

First of all, what do we mean by government surveillance?
It is the constant collection of mass data made, in this case, by the American government about US and non-US citizens. This is extremely important for national security because in this way the government can guarantee the safety of its citizens, for example by monitoring potential terrorists or criminal activities. But the use of surveillance devices, like the Stingray, a particular machine used by the US police to monitor potential criminal phone calls, can also be seen as a violation of privacy if it intercepts innocent citizens conversation. Therefore we can say that we all knew about government surveillance but we didn't know how deep and consistently it was until June 6, 2013. That day, Glenn Greenwald published an article on The Guardian about government surveillance programs over the US and not US citizens provided by the anonymous tipster "Citizenfour" (who later revealed himself as Edward Snowden).

In 2007, the NSA (United States National Security Agency) started working on a number of surveillance programs that some companies were forced to accept without getting any kind of benefits: Prism, Happyfoot, Bullrun, Project X. By using Prism, the government could have access to any users' personal information collected by media companies (Microsoft, Google, Facebook). Happyfoot could leak location data and it was usually used to determine if US or non-US citizens were acting suspicious. Bullrun is considered to be the most dangerous of all the surveillance programs, mostly because it could interweave economic transactions and because it could decrypt mobile phone's algorithms without direct physical access to monitored phones through the so-called "back door track". By using Project X, the government had physical access to all communication tools.

How did the public react? And did awareness of Government surveillance programs affect the way people express themselves on Twitter?
According to the Pew Research Center, surveillance programs prompt the 87% of U.S. adults who have heard of the government surveillance programs to change the way they use

technology. Ms. Brandimarte decided, therefore, to study if and how people were influenced by the "revelation" by observing users' behavior on Twitter. In other words, the research tried to discover if users started tweeting in a different way, or if they were at least more inhibited in tweeting. The previous attempts of estimating chilling effects of Government surveillance have been made in 2014 by Marthews & Tucker, which tried to measure the "chilling" effects of Government surveillance on Google searches. To measure this effects, Marthews & Tucker selected a bunch of sensitive words that the government had clearly announced to be monitoring on social media and studied their use before and after Snowden's revelations. This research showed, for the first time, that people were influenced by the latter and limited themselves in searching sensitive words. Furthermore, many other surveys noticed a decrease in the use of sensitive and non-sensitive words.

Prof. Brandimarte's research took a step further from Marthews & Tucker's one one, and for the first time actual data were used, in this case twitter data, to measure the chilling effect of government surveillance. Prof. Brandimarte's team selected almost 400 sensitive words monitored by the DHS, the Department of Homeland Security, and compared them to a list of words relating to food. The team took a sample of 10% of all the tweets published in the US during the year 2013, and divided them into two groups: tweets published before Snowden's Revelation and tweets published after Snowden's Revelation. By doing so, they collected a representative sample that amounts to more than 18 billion tweets. After having gathered this huge amount of data, they searched for the two set of keywords, the non-sensitive words relating to food, and the sensitive ones. Statistical machine learning algorithms and an econometric model were used to check the frequency of use of the two sets of words to verify any interesting anomalies. The final results showed, even in this case, that starting from the 6th week after Snowden's revelation, and especially in "Blue States", users actually changed their online behavior, becoming less willing to use certain sensitive words.

Why was this research useful? Because it showed through actual data how government surveillance can influence our online behavior, with the risk of causing various harmful results. In fact, an excessive surveillance lead by the government is not only a violation of an ethical principle, privacy, but it also has practical economic consequences. The provision of information about economic transactions might harm the whole economy: oversea companies might stop doing business with US companies unless the government agrees to ensure compliance with privacy policies and laws. Moreover, it could dissuade many users from participating to online health communities (owing to the fact that people would stop discussing sensitive issues), and to political organizations.

In conclusion, it is obvious that government surveillance is something essential for national and international security, but at the same time, it is necessary that the fine line between security and citizens' privacy remains clear, and not overstepped.

Raffaele Campione and Regina Cantoni