Tracking the Digital Traces

Felician ALECU, PhD, Lecturer
Department of Economic Informatics and Cybernetics
The Bucharest University of Economic Studies, Romania
E-mail: alecu[at]ase[dot]ro; Web Page: http://alecu.ase.ro

Abstract: These days we are in the middle of a huge scandal about NSA fighting against terrorism by running a massive surveillance program. Mister Eduard Snowden, a former NSA employee, revealed classified documents that clearly show how NSA is targeting the communications of everyone by collecting, storing and filtering the data in various ways.

Keywords: spying; tracking; snowden; mass surveillance; lavabit.

JEL: O33, O38.

Digital Traces

Digital footprints (also known as digital traces) are the marks a user had left by the interactions in a digital environment, like Internet and mobile phones.

These marks are usually reflecting details about the user’s activity in the digital environment – location, IP address, items clicked, elements searched for, visited pages, calls content, text of messages, and so on.
Mass Surveillance Programs

Mr. Snowden clearly indicated that Companies like Google, Facebook, Apple, Microsoft — they all get together with the NSA and provide the NSA with direct access to the backends to all of the systems you use to communicate, to store your data, to put things in the cloud, and even just to send birthday wishes and keep a record of your life.

Felix Dzerzhinsky (NKVD) once said There are no innocent people. There are only such who weren’t examined in the proper way.

Today, according to Mr. Snowden, the situation is pretty much the same:

It’s getting to the point, you don’t have to have done anything wrong. You simply have to eventually fall under suspicion from somebody, even by a wrong call, and then they could use this system to go back in time and scrutinize every decision you’ve ever made, every friend you’ve ever discussed something with, and attack you on that basis, to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer.
Stephen Walt correctly pointed out that Conventional terrorism—even of the sort suffered on 9/11—is not a serious threat to the U.S. economy, the American way of life, or even the personal security of the overwhelming majority of Americans, because al Qaeda and its cousins are neither powerful nor skillful enough to do as much damage as they might like. [...] post-9/11 terrorist plots have been mostly lame and inept, and Americans are at far greater risk from car accidents, bathtub mishaps, and a host of other undramatic dangers than they are from
"jihadi terrorism."

"Innocent“ Internet Users

So, from an economic point of view, it is hard to find reasons to spend a huge amount of money for such a not serious enough threat like terrorism.

**Government pressure - The Lavabit Story**

Despite of these rumours, we have to always keep in mind that the records of our lives are secrets and they should remain like that. Meanwhile, the Lavabit, an encrypted email service believed to have been used by U.S. leaker Edward Snowden, was shut down. *Lavabit’s founders felt Gmail was a great service but that Google was actively violating the privacy of its users by displaying ads related to keywords in their e-mail*, says the Lavabit official website.
The Lavabit messages used asymmetric encryption, which encrypts incoming e-mails before they’re saved on Lavabit’s servers, so these messages could not even be read by Lavabit itself.

The owner of Lavabit, Ladar Levison, posted a message explaining the reasons that stayed behind this extreme decision: *I have been forced to make a difficult decision: to become complicit in crimes against the American people, or walk away from nearly 10 years of hard work by shutting down Lavabit.*

![Lavabit](image)

Lavabit – the service is suspended, image taken from www.lavabit.com

A few days after, Silent Circle, another encrypted communication provider, shuttered its service. *Silent Mail was a good idea at the time, and that time is past*, the company said.
The NSA mass surveillance programs are covering all types of communication – internet traffic, online content, mobile phone calls, credit card records, etc. – so this article will be the first one from a series of papers trying to find the proper options for regular citizens to protect themselves against government (legal or illegal) actions.

Conclusions

As a strictly personal point of view, I can disclose it is quite normal for any user to leave some traces on the Internet. Even if you go through the desert you leave traces BUT in a few hours these traces start to fade, disappear, so after a while no one knows you've been there. Again, it is usual to have left traces on the internet, but the problem with these digital traces is related to the fact they no longer disappear from the system, so when someone has a suspicion, he can build a case by analysing and digging through these historic items - calls, discussions, confident, out context or not. And this is not normal, at all.

References