

Securitisation and technology

Luka Glušac

Plan

Two major issues to be discussed:

- fishery
- cardiac arrhythmia

Harpoon vs. Trawl Bag



Types of surveillance

- Mass or untargeted surveillance
- Profiling
- Randomized surveillance
- Targeted surveillance

Stanford experiment

- Participant A communicated with multiple local neurology groups, a specialty pharmacy, a rare condition management service, and a hotline for a pharmaceutical used solely to treat relapsing multiple sclerosis.
- Participant B spoke at length with cardiologists at a major medical center, talked briefly with a medical laboratory, received calls from a pharmacy, and placed short calls to a home reporting hotline for a medical device used to monitor cardiac arrhythmia.
- Participant C made a number of calls to a firearms store that specializes in the AR semiautomatic rifle platform. They also spoke at length with customer service for a firearm manufacturer that produces an AR line.
- In a span of three weeks, Participant D contacted a home improvement store, locksmiths, a hydroponics dealer, and a head shop.
- Participant E had a long early morning call with her sister. Two days later, she placed a series of calls to the local Planned Parenthood location. She placed brief additional calls two weeks later, and made a final call a month after.

Stanford experiment

- Participant A - a multiple sclerosis sufferer
- Participant B - a heart attack victim
- Participant C - a semiautomatic weapons owner
- Participant D - a home marijuana grower
- Participant E - someone who had an abortion

Joining forces

- The cooperation between the NHRI (The Ombudsman) and the Commissioner for Information of Public Importance and Personal Data Protection on protecting the inviolability of citizens' communications.

The results

- The NHRI insisted on following the case law of the European Court of Human Rights, so the amendments to the Law on the Military Security Agency and Military Intelligence Agency provided that electronic surveillance of telecommunications and information systems for the purpose of collecting retained traffic data, without accessing the content, requires an order of a higher court.
- At the same time, any secret surveillance of correspondence and other communications, including permanent electronic surveillance of the content of telecommunications and information systems, requires an order of the Supreme Court of Cassation. In that way, a solid judicial ex ante system of oversight was created.

Telecommunications companies

- There are four telecommunications companies in Serbia, three of which also provide mobile telephone services.
- They all have a legal duty to keep information about the access to their databases, so-called phone listings for one year and to register any such access.
- According to findings of the Commissioner, of those four, only one company had used database (listing) access control software.
- This software allows them to count the number of external visits to telecommunications databases, that is, by police and security services.

The findings

- Over the course of only one year, one telecommunications company alone had registered more than 4,000 accesses on request and more than 270,000 direct (online) accesses to the company's listings database.
- Of those 4,000 requests to access listings, more than half did not quote any legal grounds or court orders.

14 systemic measures

- The first subset is related to the interception of communications.
- The second subset was aimed at legislative improvements, to allow for better functioning and oversight of the security sector.
- These measures were proposed 12 years ago. Out of these 14 measures, only two were fully implemented.
- Since 2017, nobody is doing a follow-up.

Forging partnerships

- This work was possible due to the partnership between an NHRI and the Data Commissioner.
- What potential partners can you identify in your country when it comes to technology issues?

Thank you!