Can we maintain Human Rights in Our Cyber Empire?

Yvo Desmedt
Univ. of Texas at Dallas
USA

and

University College London
UK

December 11, 2014
1. **THE INDUSTRIAL EMPIRES**

The industrial empires were created based on the industrial revolution.

Marx pointed out that:

> private ownership can be abused. The solution he proposed was to have the government nationalize all private property.

Three different systems emerged:

- **System:** Pure Capitalism  |  Communism  |  Fascism
- **Emphasis:** Private property  |  State property  |  Reduced rights
- **Destroyed by:** Great Depression  |  Soviet collapse  |  WWII

Sole system that survived: **Well regulated capitalism**
2. **What is Privacy?**

Privacy is the right to live a life, within the boundaries of an interacting society, without the need for others to know what one thinks, what one does.

Oxford dictionary:

A state in which one is not observed or disturbed by other people

Privacy has been the key foundation for the US Supreme Court to justify abortion.

Ideal situation of privacy: London before the invention of the telephone.
3. **THREATS FROM GOVERNMENTS**

The Snowden leaks made the press. However, they only confirmed what was already known from, e.g.:

- “The Puzzle Palace”
- The Codebreakers
- The Patriot Act

Some “revelations”:

- People in companies have been bribed
- Eavesdropping capability is huge
- NSA and GCHQ have used malware to attack, e.g., phone
companies

- NSA benefits from Windows error reporting
- we now have state installed malware

For more details: see lecture by Bart Preneel given at Chinacrypt 2014: [http://homes.esat.kuleuven.be/preneel](http://homes.esat.kuleuven.be/preneel)

A more recent revelation:

The NSA has collected technical information on about 70% of mobile phone networks world-wide through an operation called Auroragold, according to The Intercept.

See e.g., Computer Weekly, 5th of December 2014.
4. WHAT DOES NOT MAKE HEADLINES?

- Only 2% (1% in December 2013) of Snowden’s leak got published (newspapers self censored!)
- Your mobile (and smartphone) is as an ankle monitor (but you do not have house arrest!)
- Facebook can turn on microphones and cameras of smartphones/laptops without your permission.
- GM’s OnStar car leaks your location!
- Cameras everywhere: UK breaking a record
- CEOs are switching to the cloud (e.g., e-mail)
- Since Facebook is foreign, no court order is required in the UK to spy on Facebook activities by UK citizens.
Only 1% of Snowden files published - Guardian editor

Mr Rusbridger said the paper had "made very selective judgements" about what to publish.

Only 1% of files leaked by former US intelligence analyst Edward Snowden have been published by the Guardian newspaper, its editor revealed today.
4. What does not make headlines?

- Only 2% (1% in December 2013) of Snowden’s leak got published (newspapers self censored!)
- Your mobile (and smartphone) is as an ankle monitor (but you do not have house arrest!)
- Facebook can turn on microphones and cameras of smartphones/laptops without your permission.
- GM’s OnStar car leaks your location!
- Cameras everywhere: UK breaking a record
- CEOs are switching to the cloud (e.g., e-mail)
- Since Facebook is foreign, no court order is required in the UK to spy on Facebook activities by UK citizens.
Power corrupts: people at NSA (and GCHQ) used their power to:

- intimate nude photo's unrelated to work
- spy on spouses
5. Technology: a solution?

Answer: The Good, The Bad and The Ugly technologies

Most current technologies fall in the category of “ugly”, at least from a privacy viewpoint! Examples:

Search Engines (e.g, Google, knows your interest), smart phones (know where you are), social networks (Facebook knows your friends), Google Docs (know on what you are working), Gmail and Hotmail at work (know a lot about your work)

Some technologies seem to be good. Examples are:

- Encryption (assuming NSA can not break it!)
- Threshold Cryptography: avoiding putting all eggs in one basket, i.e., can deal with hardware trapdoors and untrusted components
• anonymous e-cash

However, these are not widely deployed and software security is only getting worse. Moreover, Neumann (SRI) stated:

NSA has apparently abandoned the EAL-7 very high assurance level evaluations that are part of the Common Criteria.

So, what can we do in the meanwhile:

• Dump your mobile (I did in 2006)
• Buy old laptops without microphones and cameras
• Avoid the cloud (an official policy at University of Texas Dallas)
• For state and company secrets: avoid any electronics (a Russian approach). Also when you visit NSA, no electronics allowed!
What about bad? These are technologies sold to be good, but they are truly bad. Example:

Normal use of internet
Internet using Tor
6. **Reactions to Snowden’s leaks?**

Besides a complain from Merkel, Europe is not blocking export of data.

Moreover: American companies fall under US laws! (see also)
China’s reaction has been very different:

- Cisco equipment is now avoided
- Huawei offered $500,000 for a researcher to start a research group on information security.
- Moreover, for many years there is the Great Firewall of China. Implying China has: its own search engine (Baidu), its own social networks (e.g., Renren), its own twitter (wechat).
After the terrorist attack of September 11, 2001, some have questioned the need of confidentiality and privacy. Since data today is the driving force of our cyber economy, the philosophy smells like Cyber Communism.

In Cyber Capitalism, there should be no private data in governmental hands, i.e., similarly as in Industrial Capitalism! This means that spying should primarily be restricted to cases:

- with court orders,
- when the target is a foreign government (e.g., Merkel), or military

NSA should not be become the Western version of the KGB.
We need to make sure our physical rights extend to the virtual world. We need agreements between friendly countries extending our rights. So, when a German citizen (not a politician!) visits Italy, the German has the same rights against spying as in Germany.

The Rome Treaty is a major problem related to the EU. Indeed, anything related to national security is considered off the table (i.e., handled by each country). Spying on military falls within that category. A German citizen (not a politician!) e-mailing an Italian friend, does not fall under national security!

What if EU and the USA do not agree? Italy should block all exports to foreign countries of data created by minors (so no Facebook, no Twitter) and warn adults of their export activities.
Besides Governmental abuse, we discussed industrial abuse. For example, people are being tricked into giving away their data for free and data is money! If we want cyber capitalism to succeed, we will need regulations. Having Facebook (or any other “app”) be able to turn on a camera without the user’s consent is totally unacceptable.

Conclusion: We need to restore and extend rights. Good technology might help, but making secure implementations is a major challenge.