With every search online, every "like" or "+1" we disclose more and more intimate facts of our lives (our location, our interests, our friends). The online public spaces where we can interact, experiment and innovate, without worrying about government or corporate surveillance and discrimination are getting ever-smaller.

A recent study analysed Facebook "likes" and was able to determine with surprisingly high accuracy a range of personal information that some users may not have made public, including their sexuality, if they're smokers or not, their religion, how they'll vote in the next election and what their level of intelligence is.

Based on our personal information that our devices make available – most of the times without us knowing it – we are being profiled and risk paying more for hotels, flight tickets and other travel expenses.

Identity theft has been the biggest source of complaints to the Federal Trade Commission in the US for the past eleven years. Your identity and your money are consistently at risk with needless data collection and bad security by companies.

Your mobile phone is becoming a cash machine for mobile application developers. In one of several examples, Whatsapp forced customers (barring those using iOS 6) to grant it access to their entire address book and then retained all that information, meaning millions of non-consenting, non Whatsapp user have had their data given up over the years – to the profit of a company they may never even have heard of!

access

EUROPEAN DIGITAL RIGHTS

Google makes more money out of your data every second than an average citizen in some EU countries makes in a month!

Industry is simultaneously lobbying for increased censorship and surveillance to prevent citizens from gaining unauthorised access to copyrighted and lobbying for the right to use our personal data without authorisation!

A recent study showed that profiles used by Google reinforce racial stereotypes. Most EU countries and Members of the European Parliament want to give more flexibility to companies to engage in profiling activities.

Companies frequently give foreign law enforcement authorities access to your data without following agreed legal procedures and respecting safeguards. US lobbying led to Article 42 of the draft Regulation (which aimed to restrict this activity) being deleted in its entirety, even before the Regulation was published.

Our data are increasingly being used for purposes we are not even aware of. A society where people are permanently restricting and self-censoring their online communications because they have no trust is bad for citizens and bad for business.