About Hacking, Tracking and Leaking: Selfies, Data Access & Privacy

Selfie & Privacy

The word '*selfie*' is the most popular word of 2013 according to The Oxford University Press. In The Netherlands, part of the press has picked up this honourable mention.

But online dictionary Dictionary.com assigns to this word a completely opposite meaning: '*privacy*'. And that is for sure no coincidence.

The popularity of the selfie shows how current and attractive the combination of personal data, cloud, mobile, local and social media has meanwhile become. Self-sharing data is fun!

But the fact that privacy is a popular search word also indicates that sharing data is simultaneously seen as a big risk. Almost daily we read about data being hacked, tracked or leaked. While worrying about others sharing data, citizens in The Netherlands appear on average in 1,500 online and offline data files. Not surprising, considering that The Netherlands has a very high percentage of internet users (93% of its population) and places itself number 5 on the worldwide list.

Given this high percentage of internet use amongst the Dutch population, one would expect privacy related issues to get a lot of attention. However, the right to privacy is generally accepted and recognised offline, but once online privacy is seemingly not considered that big an issue anymore by many internet users. This is remarkable, considering that digital data can easily be collected and relocated much faster in Big Data amounts, worldwide, and without any national boundaries. Given the serious risks involved, people, businesses and institutions should be more aware and adopt a more active approach when it comes to the protection of their personal data online.

Data are currency

We have been living in a fast developing information society for about 20 years. Data have not only become the new currency, but also turned out to be an essential economical asset comparable to oil, gas, water, metals and other raw materials. By processing, data can be converted into cash, which makes it very attractive and of invaluable importance.

Nowadays, more and more data are provided and generated online. In the next years to come, we will be linking another 100 billion appliances and other objects to those (personal) data. The Internet will not just become the Internet of Things, but also the Internet of Everything. It is high time to pay serious attention to the word 'data'. This word with only four letters has various qualifications, impacts and stratifications.

Key words

When it is about sharing, giving away and storing data, no one in 2014 can hide behind ignorance. The basic notion should be that personal data are very important. Three questions to be considered before dealing with the new gold are:

a. **Choice:** which data do you share?

b. **Control:** who can use the shared data?

c. **Transparency:** what will be done with the data?

The following provides you with directions how to deal with your data:

1. **Commercially tracked**

   Almost all successful technology businesses, such as Google, Facebook and Twitter are earning billions with your data. Consciously or unconsciously, you have given 'opt-in' permission so that they can combine data and use it for profiling, advertising and resale. If this is associated with free service or functionality, this seems reasonable. But are your data not being used for more than you wish or had expected? In the US, a large-scale investigation on trade in data obtained without permission, used to predict consumer behaviour, is pending. What will be next?

2. **Hacked or leaked because of technical errors**

   Whether or not businesses or governments are using your data with objective justifications, small errors can cause data to leak. Sometimes because software-updates/releases contain errors or have not been implemented correctly (as happened last year at amongst others Facebook, LinkedIn and Google). And sometimes because IT-infrastructure and its IT-personnel insufficiently equipped to distinguish vital data. For example, in the busy month of December 2013, 40 million credit card data together with the safety codes were stolen at a big American grocer, Target. Most businesses and institutions do not know whether someone is logged in on their systems and who that person is, let alone whether they are being hacked at that moment.

3. **Hacked or leaked from within**

The ‘inside job’ within a business or organisation happens much more often than you think. Not just last year at Google, but even at the NSA. But then, you will find ‘moles’ everywhere.

4. **Hacked from the outside**

By the government

‘Mole’ Edward Snowden showed us what we all already suspected: governments are surreptitiously shoulder surfing, authorised with a legal basis, after judicial testing, or unauthorised, as long as they have sufficient budget. The Police Act in the Netherlands provides the government for instance far-reaching powers to collect and store data; as long as ‘one’ thinks it ‘sufficiently relevant’ to investigate, this is legally permitted, without any judicial verification. The Netherlands and many other countries in Europe have at least as much as and sometimes even more powers to access data than other countries. And most European countries have so-called Mutual Legal Assistance Agreements (‘MLAT’) with which exchanging data internationally is made rather easy.

By hackers

But don’t forget amateur or professional hackers: some of them are capable of creating quite some chaos, or earning indecent amounts of money with ‘data hostage’. A typical example of this is wifi-hacking. Free Wifi is fantastic if you know for sure that the person offering that Wifi can be trusted. You do not want to pass on sensitive data to an unknown person, do you? Yet this is exactly what happens at this moment more and more often. People are logging in, for instance at airports or in other public places, on unknown Wifi that has been installed by cyber criminals, in order to intercept and re-use passwords and e-mail traffic. This is what systematically happened to clients of asset managers recently.

5. **Leaked because of curiosity or stupidity**

There is no remedy to rule out stupidity. A file with 40,000 clients that apparently can be accessed, can be copied onto a laptop which is not secured and which laptop is then lost by an employee of the business concerned, in this case Ziggo. Everyone will agree that this may simply not happen, but it does. The data chain had not been regulated and was not protected, whereas such a vital data chain is nowadays almost as important as the food chain or the manufacturing chain of medicine. When recently, for example, an external online security company scattered USB sticks with the bank’s logo at the parking lot of this bank, the greater part of the USB sticks had been put into computers of that bank within an hour, unauthorised.

Forewarned, forearmed

Data leakages, hacking, tracking and other privacy infringements or (un)authorised data access are all elements of daily life. Sometimes desired, but mostly undesired. With awareness, logical thinking and adequate tailored measures, every person, business and institution can judge and choose which data to use when online, and how to check it.

This means observing data as a three-dimensional object, and splitting it into various qualifications, components and user levels.

Commercial exploitation, security, regulation and crime are aspects of a continuous cat-and-mouse game. Human ignorance or error will remain one of the biggest issues, but forewarned is forearmed: let this be the subtitle of every selfie.

Author: Arthur van der Wees, founder and managing director of Arthur's Legal