40 registered logs of my phone in one day

During a random day in January my phone's location is registered 40 times. This is due to the Danish Data Retention Law, which obliges the telecommunication companies to monitor the citizens' location at all times a day on behalf of the government, and in clear violation of EU law.

By Freja Wedenborg

My Friday the 12th of January, 2018, has a relatively early start.

During the night my phone is routinely logging on to a telemast near my home in Copenhagen's North-West neighbourhood, in one hour intervals. But at 08:35 am the entries start changing. At this time my phone is logged-on to a telemast in the outer parts of the neighborhood of Nørrebro, about a kilometer away from my home. At 8:40 it is registered yet another kilometer away. And then it goes silent. The next entry doesn't appear until 9:55, where I seem to be moving a short distance within the same neighborhood. Then there are another two entries in the same area, until the phone is logged on a mast in Copenhagen downtown at 15:15.

This can be gleaned from the information that my phone company has logged about me from that morning, and it is actually a bit intimate for me to share.

You see, I started my morning with a doctors appointment in Nørrebro that day. The logged information gives a quite detailed description of the route my bus was taking towards the area of the doctor's office and during the following hour, when my phone was turned off. From 10:00 I was working from at local café until I had a meeting with a contact at 15:30 in Copenhagen downtown. The registration from our meeting places my phone 350 meters from our meeting point.

In total, my phone's location has been registered 40 times that day, starting at 1 am and ending five minutes before midnight. On other days the logs have up to 60 location registrations. During Friday the 12th, the logs also show that I have received nine incoming SMS', one phone call and one voicemail, and that I have sent six sms' and made one outgoing call. The time, duration and number of all these interactions are registered too, with the exception of one call received from an unlisted number.

This is the scope of data surveillance that all Danish citizens are exposed to everyday, and to which the authorities can gain access.

The Data Retention Law

The story of the Danish Data Retention Law is a fascinating tale of how illegal mass surveillance can be implemented in the laws of a democratic nation.

Since 2007, the Danish telecommunication companies have been obliged to register their customers' digital movements and to store records of it for a year, so that authorities can gain access to the information with a warrant.

This practice was introduced in the Data Retention Law of September 2007. The law is an implementation of the EU's Data Retention Directive from 2006.

The EU directive originally compelled countries to log their citizens' telecommunication and internet traffic, but left it to the individual member states to decide which methods to use and how much data to collect.

The Danish implementation, however, exceeded the requirements of the directive in several respects, making it the most comprehensive data retention law of all the EU member states.

Most controversial was the so-called session logging, which meant that the telecommunication companies tracked and stored information of the citizens' use of internet, such as where they logged-on from, what websites they visited, and for how long they stayed online.

A comprehensive mass surveillance, which led to widespread protests from citizens' groups.

Ruled out twice

In 2014 those protests received support from a ruling of the European Court of Justice, which declared the data retention directive invalid due to its "wide-ranging and particularly serious interference with the fundamental rights to respect for private life and to the protection of personal data".[1]

Subsequently, the Danish government withdrew the practice of session logging, not because of the Court of Justice ruling, but because the vast amounts of data had proven useless to the police.

But, like most other EU countries, Denmark continued the parts of the Data Retention Law that came from the original directive, despite the ECJ ruling declaring it invalid.

In December 2016 a second ruling from the European Court of Justice deemed the data retention illegal. The ruling opens up for targeted data retention to be allowed for the purpose of fighting serious crime, as long as the retention is limited to what is deemed strictly necessary. But firstly, it clearly states that "EU law precludes national legislation that prescribes general and indiscriminate retention of data."[2]

In other words, the Danish mass retention of data from all citizens with a phone or internet access is in conflict with the EU law.

---

[1] Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others, 8 April 2014

[2] Judgment in Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others, 21 December 2016

Data retention continues

Sweden, where the case that led to the EU courts' second ruling was started, immediately reacted by suspending their data retention laws. But Denmark didn't follow suit.

Despite the two very clear rulings, data retention continues to this day in the same scope as in 2014, and the latest official statements indicate that the government has no intention of changing this soon. A review from Statewatch in December last year shows that most EU countries are similarly trying to maintain as much surveillance as possible.

In Denmark, this includes information about which phone numbers your number is calling and texting (sms and mms), when that is happening, and which telemasts the phone is logging on to when it happens.

Official statements from the government indicate that it has no intention of changing these rules in the near future. But when they do, preliminary plans have shown a intention to move from logging information about people's interactions via calls and text messages, and towards more detailed logging of their location via telemasts.

This may seem less intrusive, but surveillance experts warns that it will mean an almost complete registration of where the citizens are at any given time of the day.

To fully comprehend the scope of this mass surveillance, we must understand how telemast logging works.

Already today, telecommunication companies are compelled to log the connection of their customers' phones to one of the more than 18.000 telemasts in Denmark. These companies handle this practice differently, but a mapping exercise carried out by the Danish internet activist Christian Panton shows that the biggest company, TDC, logs the position of their three million customers between 50 and 100 times per day.

In the cities, this data places a phone within a few hundred meters of the logged mast, while in the countryside the distances are slightly bigger. This information gives an almost complete picture of each of the companies' customers location at all times during a given day.

As my example showed in the introduction, this information can be both personally and professionally sensitive.

Imagine for example that the contact I was meeting in the afternoon was a source planning to breach his duty of confidentiality and leak sensitive information to me. And imagine that I would later use this information for a story. In a subsequent investigation it would be quite easy for the authorities to use the location logs to pinpoint which employee from the workplace in question I had been meeting with before the disclosure.

A democratic problem

The Danish data retention is extensive. But it is just one part of the widespread digital mass surveillance of the citizens that the Western authorities have launched since 2001.

Many of the surveillance measures have been introduced in the wake of terror attacks, thus creating a conflict between the terror laws and our democratic rights.

In 2013, former NSA-contractor Edward Snowden's disclosures showed us how the world's intelligence services systematically surveille the phone and online activities of millions of citizens across the planet, including through programs that give these authorities almost unlimited access to the information we exchange via third party services like Facebook, Google and Skype.

Since then, many citizens have become increasingly aware of how to protect their right to digital privacy by using secure communication services or encrypting their phones and computers. But in many countries, also in Europe, authorities have responded with attempts to criminalize the usage of these tools.

We live in a time where state authorities are getting more and more power to to monitor their citizens.

At the same time, journalists and citizens are experiencing increased restrictions on their capacity to monitor how the authorities are using their power. For example, public oversight over the activity of intelligence services is being restricted, while the legislative process is being moved to channels without FOI-access, and whistleblowers are facing increased persecution.

This is a serious democratic problem, which challenges our constitutional right to privacy and information.

But it also changes our working conditions as journalists and media workers with an obligation to protect our sources.

What to do

So how can we act on this situation?

In Denmark a number of different steps have been taken.

In early 2018 a group of internet activists and privacy NGOs are planning to sue the government for continuing the data retention against EU law.

Meanwhile, the Danish Union of Journalists have taken a two legged approach to the issue.

On one hand the union is working to avert legislative attacks on the right to privacy and to ensure journalists' continued opportunity to provide their sources protection.

On the other hand the union is training their members in digital self-defense based on the understanding that knowing how to protect yourself, your sources, and your equipment from digital attacks is instrumental for journalists today.

The union has also worked to ensure that future colleagues are now being taught a basic level of digital self-defense at the Danish School of Media and Journalism.

There are many ways to approach this new reality.

But one thing is certain; Digital surveillance and the attacks on our right to privacy and confidentiality is something that we have to deal with, as citizens as well as media workers.

Freja Wedenborg *is a Danish journalist and author of the book 'Cryptoguide for journalists'. She is Brussels based and currently works in the European Parliament. Freja teaches digital self-defense for journalists at the Danish School of Media and Journalism and is also a board member of the Danish Union of Journalists.*