Testimony for PEGA hearing on spyware and fundamental rights

Ot van Daalen*

27 October 2022

Dear members of the PEGA Committee,

Thank you for inviting me today to the hearings on "The impact of Spyware on Fundamental Rights" and "The impact of Spyware on Democracy and Electoral Processes".

I am an assistant professor of privacy and security law at the Institute for Information Law at the University of Amsterdam. Last year, I published a report for the Dutch Ministry of Foreign Affairs on the export of cybersurveillance technologies under the new Dual Use Regulation. This month, I finished a PhD on the human rights obligations of governments relating to information security.[1] Today, I want to focus on one aspect of this research, namely the human rights obligations of states with regard to the regulation of vulnerabilities in software and hardware.

Vulnerabilities are a prerequisite of spyware

First, what does the regulation of vulnerabilities have to do with spyware? Well, in order for spyware to be installed and operated on a device, you would need *access* to, and *control over* this device. But isn't a device protected against this? Of course. However, these defenses sometimes do not provide a fully effective shield – they are, in short, vulnerable.

Gaining control over a device requires exploitation of one or more vulnerabilities in a system's defense. Vulnerabilities are, in other words, a prerequisite of spyware.

* Assistant professor in privacy and security law at the Institute for Information Law of the University of Amsterdam, o.l.vandaalen@uva.nl

[1] O.L. van Daalen, *Making and Breaking with Science and Conscience: The human rights-compatibility of information security governance in the context of quantum computing and encryption*, Amsterdam: 2022.

Without vulnerabilities, spyware would be next to impossible to covertly install and operate.

So the first take-away of my contribution is that the regulation of spyware is intimately connected to the discovery, sharing and exploitation of vulnerabilities.

Vulnerabilities will always be there and will always be found

Now, if you would want to curtail the use of spyware, one regulatory response could be to *strengthen the defense* of digital systems. Currently, much attention of EU policymaking is devoted to this aspect – see for example the NIS2 Directive and the proposal for the Cyber Resilience Act.

Still, even if organisations would shore up their defenses significantly, vulnerabilities will remain. It's next to impossible to develop systems without vulnerabilities in the current digital ecosystem, and even if some organisations succeed in doing so, it isn't realistic to expect all organisations to do this.

Another regulatory response then would be to limit the *research* into vulnerabilities. If you don't find them, they cannot be exploited, would be the underlying thinking. Unfortunately, and perhaps uninentionally, there is some of that in EU policy as well: under current EU rules, such as the Cybercrime Directive and the Copyright Directive, information security researchers may face civil and criminal liability when doing research into vulnerabilities and sharing their results.

There's a problem with that too. Vulnerabilities are discovered regardless of such prohibitions – think of criminals running ransomware schemes, intelligence agencies running hacking operations and academics doing it for scientific acclaim. And again, research into information security can be useful, because if you don't find vulnerabilities, you cannot fix them.

But currently, vulnerabilities do not have to be disclosed

This leads to a surprising situation in the EU. Currently, if you are a security researcher, and you find a vulnerability in, for example, an online camera, you're not obliged to share your findings – this research might even be illegal in the EU. You could choose, however, to sell the knowledge of this vulnerability to a broker, who will pay you good money for it. This might be legally dubious, but the chances of being caught are small.

As a result, there are currently numerous individuals and private companies whose

business model it is to find vulnerabilities and sell them to others, sometimes for millions of Euros per vulnerability. Many of these vulnerabilities will not be used to strengthen systems but, instead, to attack them. And some of these vulnerabilities may end up facilitating spyware.

The question is whether EU governments have an obligation to change this. I conclude they do.

EU must regulate the handling of vulnerabilities

For this conclusion, I firstly analysed information security-related case law on Article 8 of the Convention and Articles 7 and 8 of the Charter.

From this case law, it becomes clear that states have an obligation to minimise the risk of unlawful access to private information and systems. The consideration of the European Court of Human Rights in *I v. Finland* (2008), which was about unauthorised access to medical data, is particularly relevant: the Court considered that states have an obligation *to exclude any possibility of unauthorised access*.[2] Similarly, the EU Court of Justice has read into Articles 7 and 8 of the Charter an obligation to prevent unauthorised access to private information in the context of data retention case law.[3]

Now, this does not mean there is no room for balancing interests, for example between the right to confidential communications and the prevention of crime. This has been confirmed for example in *K.U. v. Finland* (2008).[4] Here, the Court concluded that it is the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context.

[2] ECHR 17 July 2008, Application no. 20511/03 (*I v. Finland*), par. 38; see also ECHR 25 February 1997, Application no. 22009/93 (*Z v. Finland*).

[3] In *Digital Rights Ireland*, for example, the Court considered the required security measures insufficient, in particular because they permit providers to take into account economic considerations when determining the level of security they apply; CJEU 8 April 2014, Cases C-293/12 and C-594/12 (*Digital Rights Ireland and others*), par. 67. And in *Tele 2* it considered that, given "the quantity of retained data, the sensitivity of that data and the risk of unlawful access to it, the providers of electronic communications services must, in order to ensure the full integrity and confidentiality of that data, guarantee a particularly high level of protection and security by means of appropriate technical and organisational measures"; CJEU 21 December 2016, Cases C-203/15 and C-698/15 (*Tele2 Sverige and Watson and Others*), par. 122.

[4] The Court considered that although "freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others"; ECHR 2 December 2008, Application no. 2872/02 (*K.U. V. Finland*), par. 49.

This brings me to my second take-away: if states have an obligation to reduce the risk of unlawful access, and vulnerabilities increase the risk of unlawful access, then governments have an obligation to ensure that knowledge of vulnerabilities is used to strengthen information security in the public interest.

The next question is, how this can be achieved.

By introducing a duty to disclose information security research

For answering this question, I analysed the obligations of states with regard to the right to freedom of expression (under the Convention and the Charter) and the right to science (as protected in the International Covenant on Economic, Social and Cultural Rights and the Charter). This led me to conclude two things.

Firstly, the EU should clarify that information security researchers have a right to research vulnerabilities and share the results thereof. They should not face the risk of criminal and civil liability, if certain conditions are met.

And this is the second conclusion, most relevant to this committee: states should introduce a duty to disclose the findings of vulnerability research. This has two benefits. Firstly, it ensures that information security measures can be strengthened. Second, it puts an end to the current situation where researchers can keep vulnerabilities secret and sell them to private brokers.

There should be some boundaries to this duty to disclose. Firstly, when you're disclosing vulnerabilities, you should do so in way which reduces the risk that others can exploit it. This means, generally, that the involved parties should be granted an opportunity to fix the hole before disclosure. Second, if you've found vulnerabilities which only affect your own systems, it would not be necessary to disclose them to allow others to fix them. Third, if you've found vulnerabilities in things such as ransomware, which for example allows you to assist victims in decrypting their files, it would not make sense to disclose these either.

Finally, there is the question to what extent states can retain vulnerabilities for a limited time to exploit them, only afterwards informing the organisations which can fix the hole. This is the most relevant to this committee, and it is also the most complicated.

The German Constitutional Court has already considered this question, concluding that the fundamental right to confidentiality and integrity of IT systems does not require authorities to notify "any IT security vulnerabilities immediately and in all

circumstances."[5] According to the Court, delaying notification must, however, be based on a legal framework that resolves the conflict between the different interests involved.

Whether this conclusion is warranted under the Convention and the Charter requires further research. My initial assessment is that the German Court gives too much leeway to states in this regard: on balance, the public interest favours immediate disclosure, and the burden rests on governments to demonstrate otherwise. This, given the poor state of information security, will be difficult to accomplish.

One important distinction is probably between a vulnerability leading to a class break — a weakness in many systems at once — and a vulnerability in one particular server, for example as a result of a wrong configuration. If only one particular server is affected, this is far less problematic than if many systems are affected.

This leads me to my final conclusion: spyware is intended to work on every device. And as the research of this committee demonstrates, its use is often highly problematic and in some cases illegal. This means that the retention and sharing of vulnerabilities for this purpose should be severely restricted, if not completely banned.

* * *

Relevant sources

BVerfG 8 June 2021 (*IT-Sicherheitslücken*).

CJEU 21 December 2016, Cases C-203/15 and C-698/15 (*Tele2 Sverige and Watson and Others*).

CJEU 8 April 2014, Cases C-293/12 and C-594/12 (*Digital Rights Ireland and others*).

ECHR 17 July 2008, Application no. 20511/03 (*I v. Finland*).

ECHR 25 February 1997, Application no. 22009/93 (*Z v. Finland*).

ECHR 2 December 2008, Application no. 2872/02 (*K.U. V. Finland*).

[5] BVerfG 8 June 2021 (*IT-Sicherheitslücken*), par. 43-44.