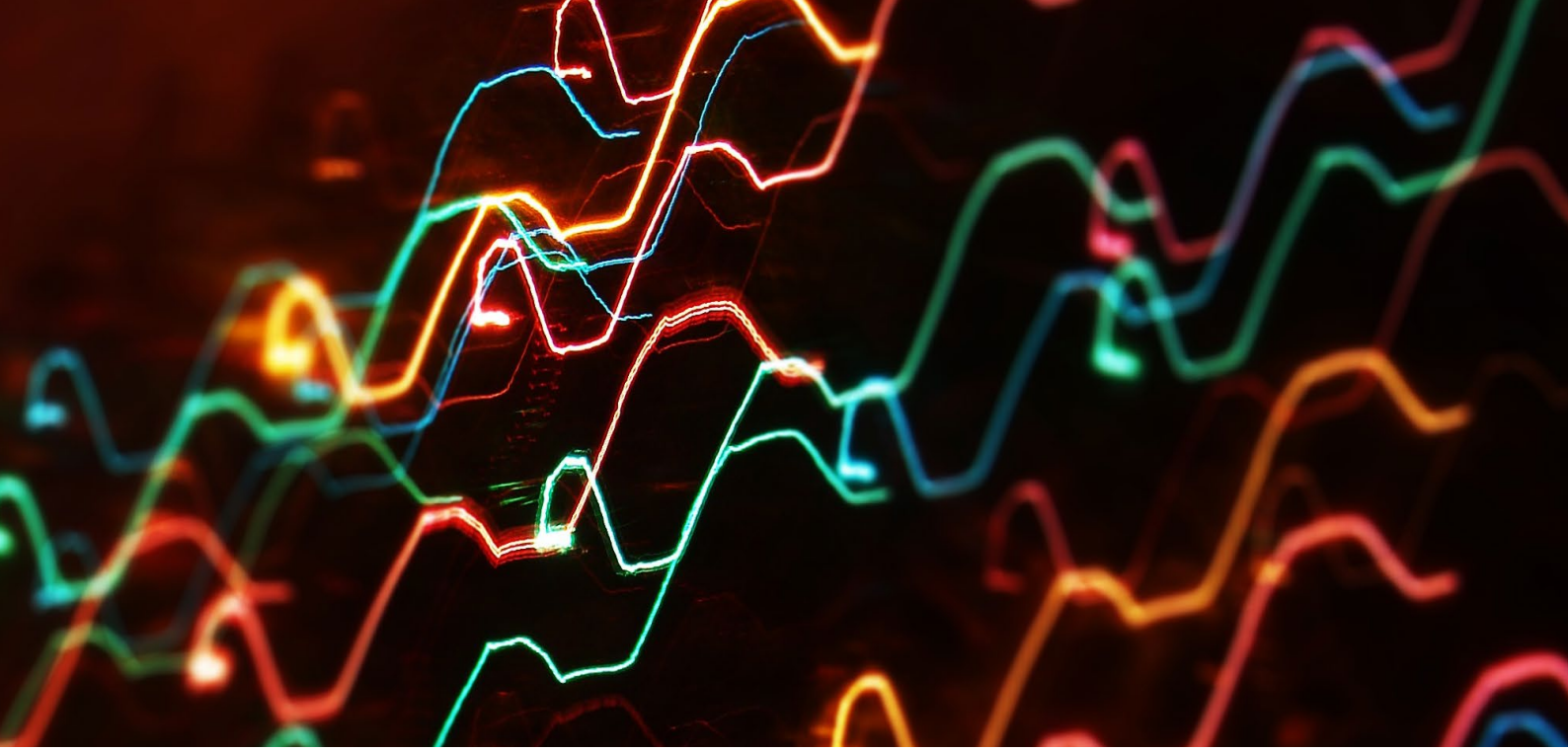

Sheetal Kumar

How can digital rights defenders respond to the rising use of government hacking as the Internet of Things grows?

Future-Proofing
our Digital Rights

DFF Digital Freedom Fund

Sheetal Kumar

How can digital rights defenders respond to the rising use of government hacking as the Internet of Things grows?

The growth in connected devices

In June, the global telecommunications company, Ericsson, doubled its estimate of the number of 'things' (or devices) expected to be connected to the internet by 2023: **it now expects 30 billion connected devices in just five years time.** This will seem like an abstract number to anyone who doesn't follow the "internet of things" or "IoT" industry - but what it means for us in reality is that we will be surrounded by more and more things which collect, receive, and transmit data about our daily lives, including personal and sensitive data about our locations, our habits, our political views and even our sexual preferences.

From a privacy perspective, this greater number of connected devices is a challenge because such devices introduce new points of vulnerability for attack or hacking and resulting breaches of personal data. Each and every one

of these "things" – from cars to coffee machines – becomes a possible target or victim of hacking, which the European Parliament LIBE committee refers to simply as "accessing a suspect's computer or phone remotely through the Internet without the person's knowledge or consent". But hacking techniques are not, of course, the sole purview of lone (cyber) criminals. **Hacking is being used by a range of government actors (the military, security services and law enforcement) , for various reasons from investigating extremist groups and child exploitation rings, to gaining an upper hand in espionage operations.** These measures have purportedly been adopted in response to the phenomenon of "going dark", which is the term used to describe the scenario where certain types of data become unavailable because they are encrypted. Yet, hacking is not only a highly intrusive technique that is very difficult to use in a narrow, targeted way, it also relies on certain practices like the hoarding of software vulnerabilities. Practices like these weaken everyone's security because it means that information of such vulnerabilities can be more easily leaked to the public.

> The greater use of hacking by governments will pose a grave threat to privacy and security.

Governments legitimise their hacking in two main ways: by legalising broad hacking powers and/or by using existing criminal legislation which provides general powers permitting the interception of communications (like wiretap legislation, for example). **The largely unevenly regulated but greater use of hacking by governments in an environment of increased connectivity will pose a grave threat to privacy and security.**

So what are the concrete and practical steps that digital rights defenders can take to protect privacy, considering this future challenge?

What digital defenders can do

First, digital rights defenders should consider the opportunities to resist the legalisation of broad hacking powers. This is what recently happened in Austria, where draft legislation which would have increased hacking powers, including for law enforcement, was withdrawn on the basis that it represented an excessive intrusion on the right to privacy. Public action in countries which have

gone on to legalise hacking powers, such as Germany (where activists and politicians alike have sent constitutional complaints to the government over its use of malware in criminal investigations), and the UK (where a successful legal claim against the Investigatory Powers Act challenged rules requiring companies to store users' data so the state could access it), have shown examples of how this can be done.

Hacking also leads to the collection of evidence in a way that makes it easy to tamper with or manipulate, meaning it can violate due process or fair trial rights. These rights can be used by digital rights defenders to challenge evidence obtained by hacking. Digital rights defenders can also push for the establishment of vulnerability disclosure processes, to increase transparency and reduce the likelihood of governments hoarding vulnerabilities.

> Hacking also leads to the collection of evidence in a way that makes it easy to tamper with or manipulate

Second, digital rights defenders should support efforts at the global level to develop norms that do not tolerate government hacking except in the most limited of circumstances. The expectation is that a new UN Group of Governmental Experts (GGE) will reconvene to discuss and develop norms around state behaviour in cyberspace. Although it's not clear yet what the new GGE will discuss, a commitment like the one suggested in Microsoft's Digital Geneva Peace Initiative to limit the use of state-sponsored hacking would be an important step forward, and would help digital rights defenders to shape relevant national legislation as well as to hold their governments to account in the future.

Finally, in order to support these efforts it would be helpful for civil society groups to work together to document cases and instances of government agency hacking and, where possible, the legal frameworks that are used to support hacking. This would help provide a solid evidence-base for resisting overly broad frameworks and advocate for limitations on government hacking.

This short piece cannot do justice to the scale and complexity of the challenges that IoT raises and the distinct challenge of a rise in government hacking within that context. However, as has been outlined above, there are some

steps that we should take to reduce the risk of violations of privacy arising from this challenge. In the main, greater coordination is needed - greater coordination among and within civil society groups who work to protect and defend the right to privacy, particularly at the global level. For example, digital rights defenders could coordinate around global norm processes (the GGE and the Global Commission on the Stability of Cyberspace, for example) and push for the development of cyber norms that limit government hacking.

In the first half of 2018, the cybersecurity firm Kaspersky Lab detected three times more malware attacks on smart devices compared to 2017. If this is a sign of things to come, we must make sure that our governments are abiding by their obligations and protecting our privacy and security, not undermining it. **If we start now, firstly by ensuring that appropriate legal frameworks exist at the national level and, secondly, by engaging with global norm processes to push for commitments from governments to limit state hacking, while also thinking creatively about how to engage with other stakeholder communities, we should be better prepared by 2023 to deal with the privacy and security challenges we face as we move towards the inevitability of having more and more connected things in our lives.**

Sheetal Kumar, Programme Lead, Global Partners Digital

Sheetal leads strategic oversight for a global cybersecurity and cybercrime project, which supports civil society coordination to protect and promote human rights in internet policy processes.

When algorithms decide your rights

Future-Proofing our Digital Rights

About the Digital Freedom Fund

The **Digital Freedom Fund** supports strategic litigation to advance digital rights in Europe. With a view to enabling people to exercise their human rights in digital and networked spaces, **DFF** provides financial support for strategic cases, seeks to catalyse collaboration between digital rights activists, and supports capacity building of digital rights litigators. **DFF** also helps connect litigators with pro bono support for their litigation projects. To read more about DFF's work, visit: **www.digitalfreedomfund.org.**

The **Future-Proofing Our Digital Rights** project was made possible thanks to the support of the Foundation for Democracy and Media and the Renewable Freedom Foundation. **DFF** receives organisational support from Open Society Foundations, Luminate and Adessium Foundation.

Democracy & Media Foundation **Stichting Democratie & Media**

Renewable Freedom Foundation

DFF Digital Freedom Fund

E-mail:
info@digitalfreedomfund.org

Postal address
Digital Freedom Fund
P.O. Box 58052
1040 HB Amsterdam
The Netherlands