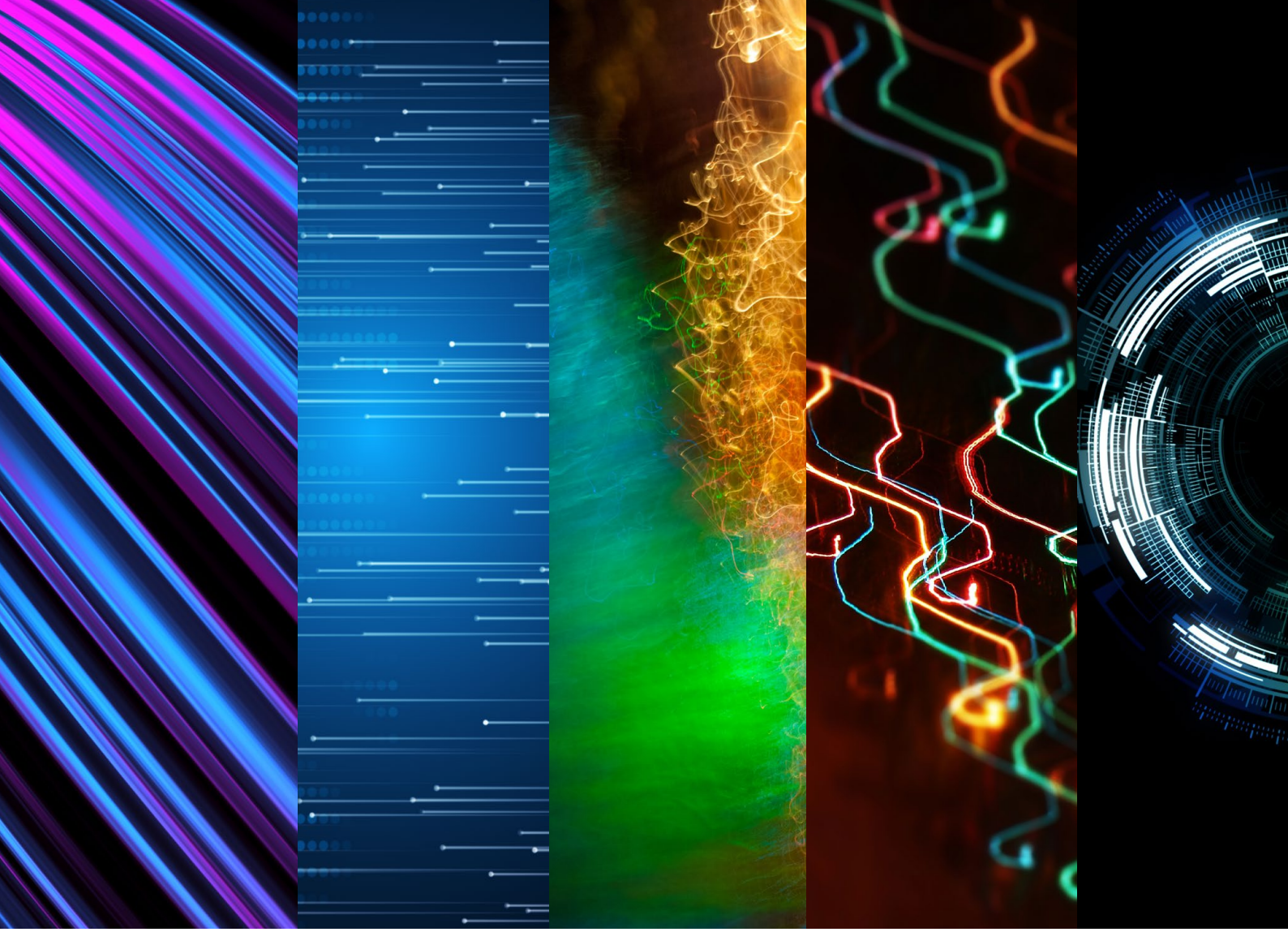


Future-Proofing our Digital Rights

DFF Digital Freedom Fund

Future-Proofing our Digital Rights

Digital Freedom Fund

When algorithms decide your rights

Author: Iris Lapinski

Towards a better protection of children's personal data collected by connected toys and devices

Authors: Ingrida Milkaite & Eva Lievens

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

Author: Sheetal Kumar

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

Author: Steve Song

Creating an inclusive digital future - urgent action needed

Author: Stacie Walsh

Iris Lapinski

When algorithms decide your rights

Future-Proofing
our Digital Rights

DFF Digital Freedom Fund

Iris Lapinski

When algorithms decide your rights

November 2039.
Brent, London, England

Sarah woke up. Her head was aching. A drink too much the night before. She looked at the alarm clock. It was 9.00am. She listened if she could hear noises in the house, but it was silent. She was relieved. Her two children, Selena and Brandon, had already woken up, made themselves breakfast and had gone to school.

Then she remembered her appointment and rushed out of bed: 9:30am at her local Citizens Advice Bureau. To get from Chalkhill Estate to the High Road she would need to run and have some luck to catch the bus on time.

In the bus on the way to her appointment, she felt like this journey had been in the making for a long time. Four years ago, her sister Chantell, who had cerebral palsy and heavily relied on support, had her home care visits dramatically cut from 56 to 32 hours a week. A new algorithm had reassessed the amount of care her sister would be given. Her sister had pleaded with the assessor, explaining how that simply wasn't enough support, but neither the assessor nor her sister seemed to quite understand how the decision was reached by the computer to reduce the amount of care. Her sister's health situation hadn't improved, but an invisible change had occurred that created this new result. When the assessor entered the information about her health status, daily rou-

tines and needs for support into the computer, it ran through an algorithm that Brent council had recently approved, determining how many hours of help she would receive.

And then there was her younger brother Jordan who had been arrested and charged with burglary and petty theft for grabbing an unlocked bike and a scooter with his mate. When Jordan was booked into prison, a computer program spat out a score predicting the likelihood of him committing a future crime. Yes, Jordan had had issues before and a criminal record for misdemeanours committed when he was a juvenile. But how could he be classified at a high risk of re-offending? He had told her that so many other seasoned criminals with multiple convictions of armed robbery had been classified as low risk. But then those guys were white and Jordan was black...

So now it was her turn. Yes she was not the perfect mum, she was the first to admit that herself. She was struggling, not just because of her learning disability which made it hard to stay in a job, but also because she tried to help her sister after home visits were cut.

Unfortunately, her energy to support Selena and Brandon was often nil and they regularly missed school. So a few weeks ago a woman from the council had come by her house and had told her that her family was classified as high-risk and was being placed in a special programme of families being at risk of child sexual abuse and gang exploitation. She had been horrified to hear this and needed help. Her neighbour Sue had told her that Citizens Advice had launched a new service: AAS – the algorithm advice service.

Fred, the young Citizens Advisor, was a student training as a data scientist. He would help her to analyse which data points had triggered her high-risk classification and what rights she had to contest some of the data used by the council and the conclusions drawn.

The future in the story told above has not happened yet to one individual as far as I know. However, if you look at how algorithms get used by public authorities in the US today in **judging re-offending risk** or in **re-assessing disability benefits** you can see that algorithms there already have a direct impact on the realisation of human rights.

In the UK most public sector programmes like **the one run by Brent council and IBM to identify children and families at risk** are still in pilot stage today, but their potential impact on human rights is equally strong.

Artificial intelligence (AI) and machine learning (ML) have been around as a niche in the field of computer science for years without much public attention. However, in recent years, there has been exponential growth of practical use cases in government sectors like health, education and criminal justice that have triggered a lot of public debate on the risks and unintended consequences of it.

When you look at historical patterns of how societies have managed the change and challenges created by new technologies, I would argue there are three overlapping phases:

1. The ethics and convention phase;

2. The standards and regulation phase; and

3. The campaigns and appeal phase.

1. The ethics and convention phase

Since 2016 a lot of activity has taken place in this phase for AI and ML. In spring 2016, the Obama White House's Office of Science and Technology kicked off its '**Preparing for the Future of Artificial Intelligence**' initiative which held four public workshops including the first **AI Now Symposium** called "The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term" which has been followed by **annual events and reports** since.

In September 2016, the **Partnership on AI** launched with Amazon, Facebook, Google, DeepMind, Microsoft, and IBM as its founding members, and Apple joining in early 2017. By today, the partnership has grown beyond industry ac-

tors to include NGOs like Amnesty International and media organisations like the New York Times, as well as widening its reach geographically to China with Baidu becoming a member in October 2018.

In June 2017, the UK House of Lords established a **Select Committee on Artificial Intelligence** that published its **recommendations** in spring 2018. A lot of this activity during 2016 and 2017 raised the ethical implications and unintended consequences of different uses of algorithms, especially those used by the public sector and attempted to agree on shared overall ethical principles. For example, these five principles were identified in the Lords' report:

– Artificial intelligence should be developed for the common good and benefit of humanity;

– Artificial intelligence should operate on principles of intelligibility and fairness;

– Artificial intelligence should not be used to diminish the data rights or privacy of individuals, families or communities;

– All citizens have the right to be educated to enable them to flourish mentally, emotionally and economically alongside artificial intelligence;

– The autonomous power to hurt, destroy or deceive human beings should never be vested in artificial intelligence.

Also as part of this overall global debate, John C. Havens of Institute of Electrical and Electronics Engineers (IEEE) pointed out in **this article** that values and ethical principles lead design and development decisions in AI.

2. The standards and regulation phase

In my view, in 2018 the focus started to shift towards more work being done on translating these ethical principles into specific institutions, codes or toolkits. One of the key Lords' recommendations was the creation of an AI Code that should build in much more detail on the ethical principles set out. The **Partnership of AI working groups** kicked off in summer 2018 **aiming to create practical toolkits**. In October 2018, AI Now published its Algorithmic **Accountability Policy Toolkit** providing resources and explanations for both legal

and policy advocates. I believe that the next few years will be dominated by activity in this phase – both voluntarily led by tech industry players, as well as law-makers and government agencies to create standards, procedures and regulations around acceptable use of AI. I think this will consist of initiatives building on top of existing regulations like the **EU General Data Protection Regulation (GDPR)**, as well as initiatives looking to create new mechanisms of (self) control.

3. The campaigns and appeal phase

As every human rights activist knows, it's the third phase of change that then makes human rights real and applicable to the individual. This is when in the future organisations like **Citizen's Advice** in the UK offer support and legal assistance to appeal (no, the AAS does not exist yet, but I believe it would be a logical development to meet the needs of citizens in the future) and organisations like the **Digital Freedom Fund** can support strategic litigation to help create a body of case law in this new emerging field. Especially for algorithms used by the government and public sector it will be crucial for the realisation of human rights that they can be challenged through due process, that they are open and accountable – rather than private and proprietary – and that the government allows citizens to access impartial advice when they face problems with algorithms.

I don't believe that a lot of activity in this third phase will take place in the next few years, but someone, somewhere will need to start it. Especially in the US, where most algorithms have been deployed by state actors so far, it would be interesting to explore litigation against obscure use cases directly impacting human rights. With the **Human Rights Act currently under threat** in the UK it might be harder to start litigation there despite its success in the past. It will be interesting to see which country will be the host of human rights battles against algorithms in the future.

About Iris Lapinski

Iris Lapinski is founder and CEO of Apps for Good, a technology education non-profit aiming to grow the next generation of problem solvers. Since 2010 Apps for Good has reached over 140,000 young people primarily in the UK, Portugal and the US with courses on apps, Internet of Things and machine learning.

When algorithms decide your rights

Future-Proofing our Digital Rights

Ingrida Milkaite & Eva Lievens

Towards a better protection of children's personal data collected by connected toys and devices

Future-Proofing
our Digital Rights

DFF Digital Freedom Fund

Ingrida Milkaite & Eva Lievens

Towards a better protection of children's personal data collected by connected toys and devices

A snapshot of children's digital lives

Internet connected devices and applications are increasingly present in individuals' lives and homes. These trends inevitably also affect children. From a young age, they use smart devices that are created for them, such as internet connected smart toys, enabling play and learning. They are also affected by devices that are not directly targeted at them but are nevertheless "around" in their daily reality, such as smart home assistants that record and process everything that is said in a home, including children's conversations.

Interactive toys, such as the "Hello Barbie" and "My Friend Cayla" dolls engage in conversation with children, record children's voices, store them through the services of different companies and may also transfer recorded data to advertising, analytics or other companies. Cuddly toys or baby clothing contain medical sensors that monitor children's body temperature, heart rate and

blood oxygen saturation levels which may be consequently sent to a parent or doctor's app. Finally, cute connected robots now share features which include voice recognition, remote video control, gesture-based interactions and facial tracking of children. **Given the fast-paced evolution of technology, unwavering advances in machine learning and big data analytics, and the ongoing digitisation of childhood, it can only be expected that such connected or smart toys and devices will continue to be developed and marketed in the coming years.**

It can only be expected that such connected or smart toys and devices will continue to be developed and marketed in the coming years.

Consequences?

Yet, in an environment where so much information can be collected through interaction with devices, children cease to be mere "players" or "consumers". They become "data subjects" that disclose information or "personal data" about themselves, both consciously and unconsciously. Today, children's personal information is collected and processed in unprecedented quantities, a phenomenon that scholars have denoted the "datafication" and "quantification" of children's everyday lives from a very early age. This phenomenon is facilitated by the increasing adoption of digital devices, the embracing of apps and platforms for a variety of purposes and the vast possibilities to use, analyse and infer information about users, and, as such, becoming a standard practice that is here to stay.

Of course, personal data might be collected and processed to attain valid or beneficial objectives, think about improving a child's health situation. Concerns, however, relate to the collection and combination of children's (sensitive) personal information enabling the creation of child-user profiles. These profiles can then be used for many different purposes, such as, for instance, behavioural advertising which is so sophisticated that it affects people's, and especially children's, choices without them realising it. Moreover, constructing highly detailed personal profiles of children from a very young age onwards

could also lead to potentially discriminatory practices in the future, such as excluding children with certain profiles from particular types of education or refusing to grant specific health insurance policies based on sensitive medical data that a cute cuddly lion once collected and stored.

In the same vein, the use of artificial intelligence technology which processes children's personal information, such as their product preferences, ambitions, likes and dislikes, which is a feature already integrated in the "Hello Barbie" doll, has sparked difficult questions concerning the never-seen-before emotional bonds between children and objects. Finally, the security of such connected toys and the collected data is an increasing concern in many parts of the world. In Germany, for instance, children's smart watches tracking their location (which were hacked in Belgium and the Netherlands) and the "My Friend Cayla" doll were banned because of security risks. The doll was discovered to be hackable, enabling strangers to talk to children through the doll. In the United States, the Federal Bureau of Investigation (FBI) has warned parents about the potential security risks concerning children's interaction with internet connected toys that are equipped with sensors, cameras, microphones, data storage, voice recognition technologies and GPS trackers.

Playing by the rules? Legal requirements for data processing through connected toys and devices in Europe

A recent recommendation by the Council of Europe on Guidelines to respect, protect and fulfil the rights of the child in the digital environment expects Member States, with regard to connected or smart devices, including those incorporated in toys and clothes, to take particular care that data protection principles, rules and rights are respected when such products are directed principally at children or are likely to be regularly used by or in physical proximity to children.

In the European Union (EU), the General Data Protection Regulation, or the GDPR, which became applicable in May 2018, explicitly acknowledges, for the first time in the context of EU data protection law, that children's personal data merits specific protection since children may be less conscious of the risks, consequences and safeguards, and their rights in relation to the processing of personal data.

On the one hand, the GDPR affords certain rights to data subjects, children included, such as the right to be provided with transparent information about

data collection, processing and storage in clear and plain language, the right to object, or to request erasure of their data. On the other hand, the GDPR requires data controllers (any natural or legal person which determines the purposes and means of the processing of personal data (article 4(7) GDPR), to adhere to certain data protection principles. These principles include, for instance, lawfulness, fairness and transparency of processing, data minimisation, purpose limitation, privacy by design and privacy by default, and ensuring the integrity, confidentiality and security of data. In the context of the Internet of Toys (IoT) devices, these requirements mean that the toys shall process children's personal information fairly, only collect the necessary data for the toy, and protect its security. According to the GDPR, "profiling" and other forms of automated decision making that produces legal effects concerning a person or similarly significantly affects a person cannot concern children (see, for example, recital 71 GDPR). In its recent guidelines on profiling, the Article 29 Working Party confirms that there is no absolute prohibition on the profiling of children in the GDPR, but that organisations should, in general, refrain from profiling them for marketing purposes. This should be taken into account by Internet of Toys providers.

In short, just like general toy safety is regulated, as expected by society (for instance the Toy Safety Directive 2009/48/EC which requires particularly high standards concerning the physical, mechanical, chemical, electrical, hygiene and radioactivity risks), there is a lot of potential in the GDPR to ensure that the child's right to data protection is ensured. The proof of the pudding, however, will be in the uptake and enforcement of those rules.

> There is a lot of potential in the GDPR to ensure that the child's right to data protection is ensured.

Ways forward

The new data protection framework in the EU presents opportunities for a consistent application of important data protection principles to ensure children's rights to privacy and data protection. The implementation of these principles may also lead to a much needed "de-responsibilisation" of children and parents. Data processing is often so opaque that it is not realistic to expect

parents, let alone children, to understand the lengthy and complex privacy policies as we know them. **Under the GDPR, it is up to the controllers to ensure that their data processing practices are designed from their inception with the respect for children's right to data protection in mind.** This will require a change in current thinking, a much more future-oriented thinking about values and fundamental principles that should not only be integrated into design processes from the very beginning, but that should also be evaluated and assessed at regular intervals.

> Data processing is often so opaque that it is not realistic to expect parents, let alone children, to understand the lengthy and complex privacy policies as we know them.

National Data Protection Authorities (DPAs) and the European Data Protection Board, established by the GDPR, are the key actors in terms of the actual enforcement of the obligations that the full chain of IoT providers, such as designers and manufacturers of toys, software and app developers and the platforms where the collected data is stored, have with regard to children and their parents. In the coming decade, the extent to which data processing practices through connected toys and devices will actually afford children the specific protection that they merit will not only be determined by those actors in the chain but will crucially depend on guidance and actions by DPAs.

Finally, governmental and non-governmental organisations, as well as schools and child rights advocates should continue to work on awareness-raising with regard to both the benefits and the risks that internet connected toys present, as well as the obligations of data controllers in this context. Participation of children in the connected society as empowered digital citizens starts in early childhood, and all actors that are involved should do the utmost to ensure that this ambitious goal in achieved, here, now and in the future.

About Ingrida Milkaite

Ingrida Milkaite is a doctoral student in the research group Law & Technology at Ghent University in Belgium. She is working on the research project “A children’s rights perspective on privacy and data protection in the digital age: a critical and forward-looking analysis of the General Data Protection Regulation and its implementation with respect to children and youth”. This project monitors the implementation of the GDPR in relation to children(‘s rights) until 2021.Ingrida takes part in the activities of the Human Rights Centre at Ghent University, is a member of the European Communication Research and Education Association (ECREA) and a contributor to the Strasbourg Observers blog.

When algorithms decide your rights

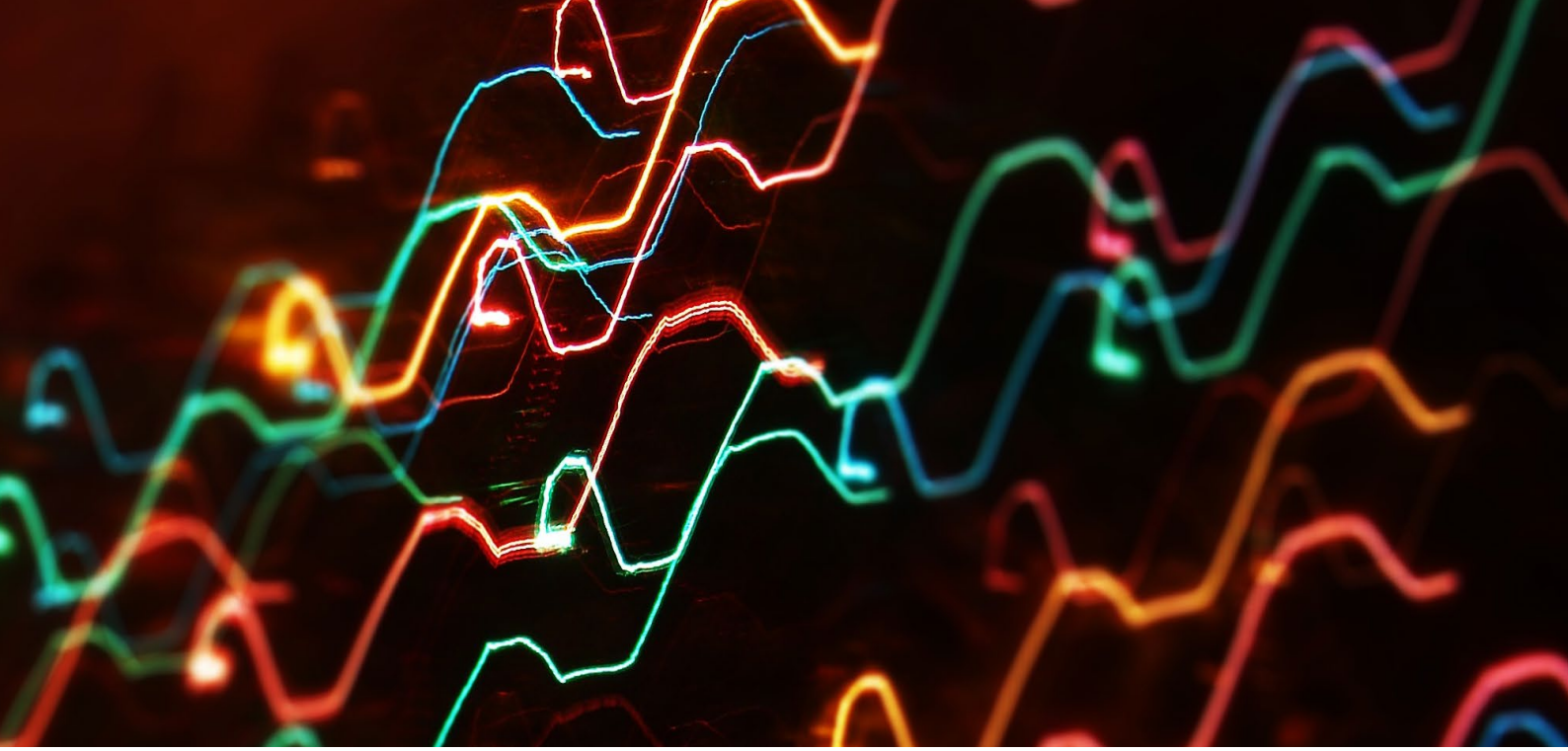
Future-Proofing our Digital Rights

About Eva Lievens

Eva Lievens is an Assistant Professor of Law & Technology at Ghent University and a member of the Human Rights Centre and the Crime, Criminology & Criminal Policy Consortium. A recurrent focus in her research relates to human and children's rights in the digital environment. She is a member of the Flemish Media Regulator's Chamber for impartiality and the protection of minors, the associate editor of the International Encyclopaedia of Laws – Media Law and a contributor to the European Audiovisual Observatory IRIS newsletter for Belgium.

When algorithms decide your rights

Future-Proofing our Digital Rights



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.

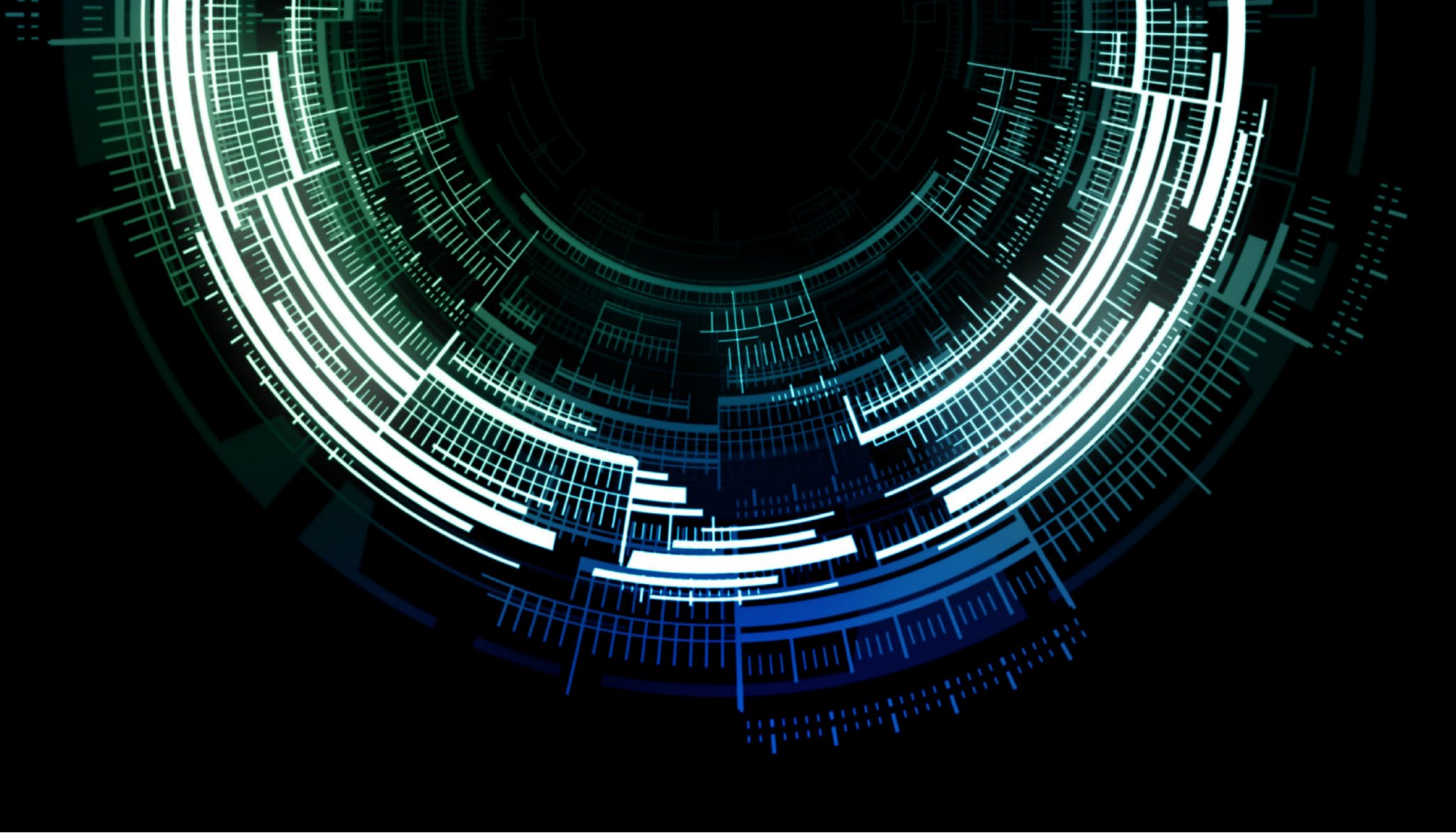
In the first half of 2018, the cybersecurity firm Kaspersky Lab detected three times more malware attacks on smart devices compared to 2017. If this is a sign of things to come, we must make sure that our governments are abiding by their obligations and protecting our privacy and security, not undermining 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



Steve Song

Internet Drift: How the Internet is Likely to Splinter and Fracture

Future-Proofing
our Digital Rights

DFF Digital Freedom Fund

Steve Song

Internet Drift: How the Internet is Likely to Splinter and Fracture

The idea of a "splinternet" or "Balkanization" of the internet is not new, although the exact manner by which this is becoming a reality is evolving. Early discussions on the topic focused around cultural or policy differences and extraterritoriality that could result in a **fractioned internet**. For example, China's Great Firewall is implementation of a national policy which creates an "intranet" connected to the greater Internet.

However, there is another shift in internet infrastructure that is less talked of and even more fundamental to its functioning – the physical backbone of fibre optic cables crossing oceans and international borders that enables the relatively seamless experience of the Internet regardless of location. Increasingly investment and ultimately ownership and control of the cables used to transport information across the world is moving away from telecommunications operators. One example is the increased investment in and ownership of trans-oceanic cables by application and service providers, or platforms, such as **Google, Facebook, and Microsoft**. Another is the strategic investment in undersea cables by nation states as part of a geo-political cyber strategy.

Internet Giants and Undersea Cables

Historically, undersea cables were either publicly owned or owned and operated by telecommunications network operators (telcos) which had little to do with content or application delivery, unlike digital platforms like Google, Facebook and others that are now beginning to expand their private networks. The demand for global, high-speed, low-latency services has driven the development of local data centres which can serve a platform's content instantly almost anywhere in the world. Keeping these local data centres up-to-date consumes six to seven times more **undersea traffic** than the rest of the public internet combined.

Not surprisingly, platforms have begun to invest in the Internet's long-distance transport layer, such as undersea cable capacity, in order to serve these networks of data centres – also largely owned and operated by the platforms themselves. In contrast, what is called "last mile" of content delivery (moving content from the data centre to the end user) is still largely owned and operated by telcos. What began as investment in data capacity on existing cables rapidly became investment in the undersea cables themselves, many of which are now either partly or wholly-owned by content platform companies. The implications of this are sobering.

An undersea cable owned by a platform such as Google, Facebook or Microsoft becomes a private network connecting their data centres. As such, these cables are not governed according to the rules that have governed the Internet and its network operators to date, those of common carriage and neutrality. The telco industry, having a long history dating back to the telegraph, has had a fairly standard regulatory structure with a strict delineation between content providers (e.g. a phone company or Google) and the non-discriminatory network infrastructure which carries communications. Companies like Google are keen to avoid regulation and, as a result, have **publicly stated** that they will not resell capacity on their cables because they would then effectively operating as a telco and be subject to the oversight of telecommunications regulation.

However, this would not prevent platforms from engaging in capacity swaps with other platforms that own capacity with the result that a significant percentage of international internet traffic will not be subject to any regulatory framework. It may also result in a closed club of undersea capacity that is only accessible to other data platforms with similar investments.

Worse, because platforms account for so much international traffic, their decision to invest in their own undersea cables is likely to have a significant negative impact on investment and growth of undersea cables not owned by platform companies.

This is likely to have the effect of consolidating the dominance of a few large platform companies that can offer performance through their private networks that eclipse the public internet. Net neutrality regulations will not have any power to influence this shift.

> What began as investment in data capacity on existing cables rapidly became investment in the undersea cables themselves, many of which are now either partly or wholly-owned by content platform companies. The implications of this are sobering.

State Dominance of Infrastructure

Nation states, most notably China, are pursuing strategies that are not dissimilar to the Silicon Valley platforms. China is investing a significant amount of resources to build a geographically strategic infrastructure making it possible for internet data to flow around the world entirely on fibre optic infrastructure owned by China. The **SAIL cable** linking Africa with South America, the **PEACE cable** linking Asia to Africa, as well as a possible **Trans-Pacific initiative** linking China directly to South America are all examples of this. Growth in China's outward expansion and investment in communications infrastructure development geographically overlaps with many of the initiatives in its **Belt and Road Strategy**, which seeks to strengthen China's economic ties with 71 countries (accounting for over half the world's population) through investment in roads and waterways – and the building of Internet infrastructure mirrors these areas of investment.

The focus of development of this infrastructure may be between governments or regions that share governance structures and ideologies – particularly authoritarian regimes. This may reduce people's access to information, association and participation in online forums. New communication technologies in this vein may further infringe on digital rights such as privacy and freedom of expression by **embedding surveillance** or even censorship capabilities in the

infrastructure that would be in the hands of governments. At a higher level, these expansive policies and strategies are already impacting **democracy and national sovereignty.**

Conclusion

For consumers, this shift to a less public internet – whether by big tech giants or nation states – would limit enforcement of digital rights. What can digital rights defenders do? Digital rights defenders should engage with standards development organisations – such as IETF, regional standards bodies, or even join a member state's delegation at the ITU – and other open internet governance processes to support an open internet model. They should also engage directly with governments to build a mutual support for and understanding of the benefits of an open internet, and the internal costs of adopting more restrictive technologies and building redundant infrastructure. Particular attention should be paid to landing stations and the terms on which undersea cables are granted landing rights.

Rights defenders should also build awareness and understanding of the impact of both privatisation and splintering of the internet so that they may urge their governments and policymakers to take appropriate steps. One such approach might be to consider the use of anti-trust laws to break up media conglomerates, particularly those found to be in violation of local laws or deemed "outside" regulation due to their strategically built ecosystem. Likewise, national regulatory bodies or other organisations may be able to use litigation based on existing laws such as competition, consumer rights, and data protection to pressure platforms to act in a manner that supports a free and open Internet and robust marketplace.

Rights defenders should also build awareness and understanding of the impact of both privatisation and splintering of the internet so that they may urge their governments and policymakers to take appropriate steps.

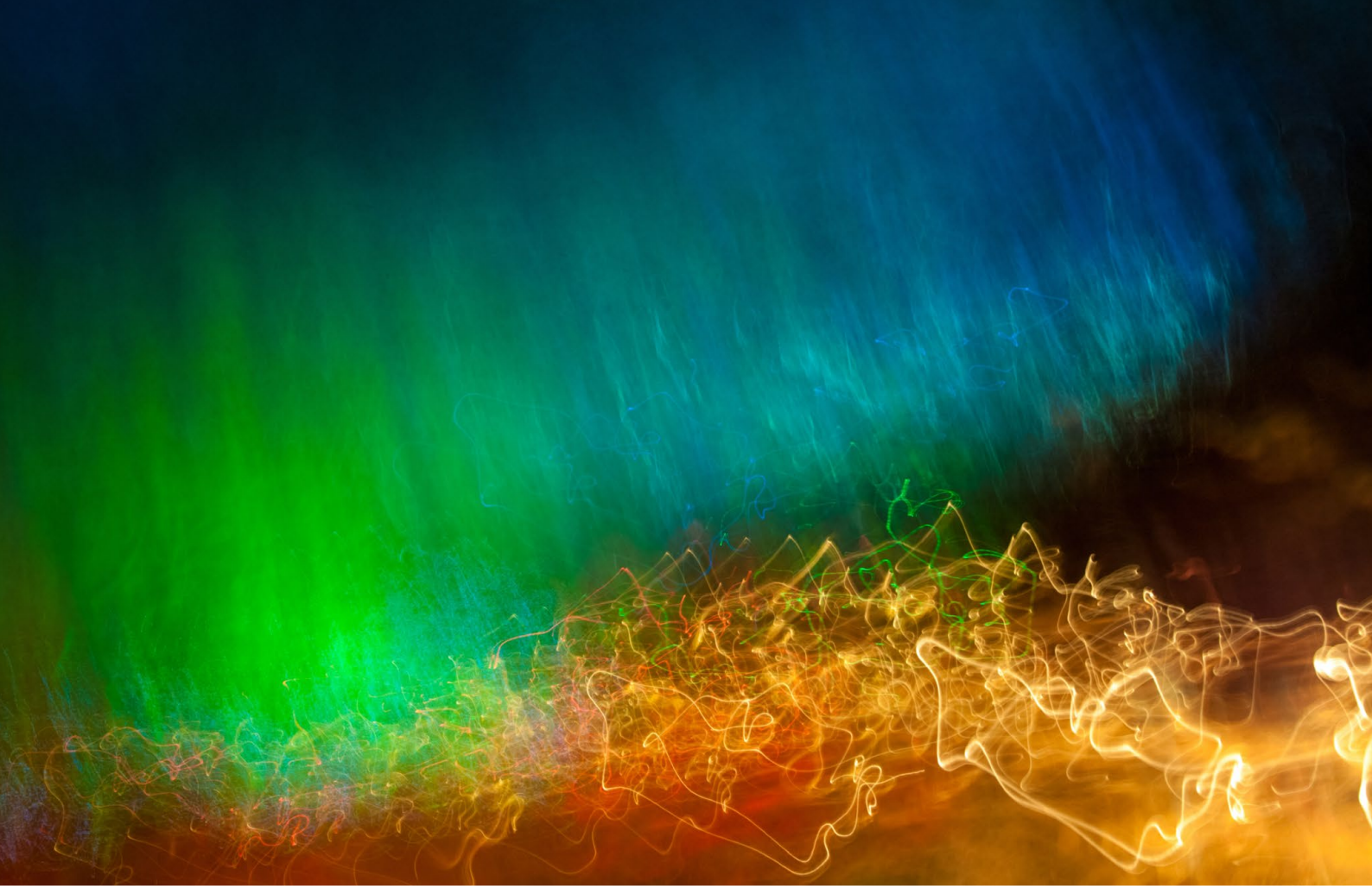
About Steve Song

Steve Song is a Mozilla Fellow and research associate with the Network Startup Resource Center (NSRC). He writes at www.manypossibilities.net

---

Internet Drift: How the Internet is Likely to Splinter and Fracture

Future-Proofing our Digital Rights



Stacie Walsh

Creating an inclusive digital future – urgent action needed

Future-Proofing
our Digital Rights

DFF Digital Freedom Fund

Stacie Walsh

Creating an inclusive digital future – urgent action needed

Emerging technologies and digital services offer incredible possibilities to create a more inclusive and accessible world. However, unless urgent action is taken to enhance digital inclusion and access, societies will become more polarised, with deepening digital and social divides. Digital exclusion will impact an individual's rights, such as the right to work, access to public services and information, civic participation, and association.

The Digital Divide: Who is at risk?

The 'digital divide' is no longer a dichotomy between who has access to the Internet and who does not. The digital divide has evolved into a broader concept including access to digital services, relevance of content, affordability and education. Factors driving digital exclusion include language, gender, (dis)abilities, age, skillset and income. As a result, offline inequalities are being reflected and accentuated in the online environment.

For example, low income households, minorities, rural populations and women are the **most at-risk of digital exclusion**. On a global scale, women 'are **12% less likely** to use the internet.' This **increases to 50%** for people with disabilities. Furthermore, for those who are able to connect, they may lack the digital savvy required to take advantage of the benefits or protect their rights online.

It is likely that the negative impacts of business models, data collection and emerging technologies will be **magnified** for people lacking digital skills and education. Marginalised users may be more vulnerable to algorithmic bias, online abuse, trolling or exploitation of their privacy, and be less likely to create – or even access – digital content. Digital divides are contributing to social and political divides across many countries and may result in **further political and economic destabilisation** within and between nations.

Divides at Every Layer

Research and reports on digital inclusion elucidate the complexity of factors influencing digital divides. For example, the difficulties of connecting to the Internet and digital services may be impacted by affordability, accessibility, or lack of skills. Lack of **affordability** can disproportionately impact women and other disadvantaged groups due to lower incomes and lack of financial inclusion. This includes the funds to connect to the Internet (e.g. mobile data or broadband) or purchase hardware (e.g. mobile phones or computers).

In terms of accessibility, for those living in rural areas, Internet connectivity may come from more expensive mobile broadband or older wired broadband infrastructure resulting in poorer quality connections or data caps which could impact the speed, quantity or quality of content delivery. Those that are able to overcome these hurdles may find a **lack of relevant content** in local languages further impacting the freedoms to seek, receive and impart information in the digital sphere. Additionally, web accessibility for those with disabilities remains low. For example, in Europe, only 37 public service websites across 7 countries were **found to be fully compliant** with European accessibility standards.

Those most at risk of digital exclusion may lack the skills required to fully benefit from the opportunities offered by the Internet or digital services, such as navigating webpages, searching or creating content, and managing user profiles. In the near future, more advanced digital skills will be needed for jobs which are currently considered manual and mid-skilled labour, such as manufacturing, administration, cooking or farming. Additionally, those lacking the educa-

tion required to enter into jobs in science and technology will be blocked from benefiting from employment opportunities in these sectors. The promise of new technologies may be outweighed by their impact on the workforce and the resulting reverberations within society.

In the near future, workplaces will require fewer people with higher level skills.

As automated and robotic technologies continue to develop, countries are already seeing a 'hollowing out' of the working class, resulting in a more polarized workforce. The **ability of people** to keep up with technology will influence how this digital divide evolves, and – unless urgent action is taken – will likely widen. Workers who are older or unable to up-skill to remain relevant may find themselves permanently excluded from the workforce. Those that are able to retrain will have the chance to forge a prosperous future. For **women**, **challenges** such as a poor work-life balance can negatively impact their time for continuing education and can create knock on difficulties re-joining fast-paced industries, such as tech, after maternity leave.

What can Digital Rights Defenders Do?

How can digital rights defenders help to create an inclusive future for the Internet and digital services in Europe? Action is needed to improve access at every layer – for instance, **enhancing** digital skills, relevant content, and inclusive workplaces. Although 'literacy' is viewed as a key element of capacity building and education, Europe is still **not good enough** at teaching digital literacy to support broader inclusion for persons with disabilities, the elderly, or other disadvantaged peoples. Resources – either digital or facilitating hardware such as home assistants – can also be developed with marginalised communities in mind to enhance inclusiveness in the digital sphere.

There are increasing concerns around algorithmic bias in digital systems and services. **Research has highlighted** the impact of developers on the resulting technology, and how technological bias **reflects and amplifies existing socio-cultural injustice.** Unless marginalized and disadvantaged persons can be involved in developing technologies, those technologies and associated business models will continue to perpetuate inequalities. Initiatives like the **UK's CyberFirst Girls** competition are a fun and imaginative approach to promoting greater inclusion in science, technology, engineering and mathematics (STEM) subjects and related fields.

Digital rights defenders can also help to **tackle** online harassment and demand accountability for online actions. This may include campaigning for im-

proved mechanisms for reporting online abuse, and greater accountability of tech platforms through robust legal frameworks. Digital rights defenders may also advocate for anonymity for dissidents and journalistic sources, within accountable, human-rights respecting online spaces.

What gets measured gets done. To further support digital inclusion, data-driven policy is essential. There have been numerous calls (including from G20 and the UN) for disaggregated data relating to gender inclusion, and the same approach is needed for other factors impacting digital inclusion such as age, (dis)abilities, and education.

Governments can support digital inclusion through **adopting relevant and specific provisions** in national digital strategies. Europe has mechanisms to **promote accessibility online** as well as **guidelines** regarding public sector procurements. These tools could be used to ensure the adoption of technologies that implement **accessibility** standards (such as IETF's standards on text-to-voice in real-time) or '**universal design**' in technical development.

If digital rights defenders do not push for concerted efforts among industry and government to adopt change, today's trends will continue and get worse. There will be increased polarization between the 'haves' and 'have nots'; more technology and services created by unrepresentative elites; and the further engraining of specific values, norms, and abilities into technologies that do not necessarily reflect society as a whole. If issues are exacerbated, European perspectives on digital rights will be threatened and it will be more difficult to find and use technologies that reflect those values. A different, more inclusive future for digital rights is still possible, if proactive steps are taken now to address challenges related to skills, workplace cultures, and digital exclusion.

About Stacie Walsh

Stacie Walsh is Internet Policy and Cybersecurity Consultant at Oxford Information Labs. Stacie is an experienced researcher, data analyst, writer, presenter and project manager, focusing primarily on the Internet addressing (DNS) ecosystem, Internet of Things (IoT), Artificial Intelligence (AI), Over-the-Top (OTT) services, and cybersecurity. Stacie is a CESG certified CyberSecurity/ Information Assurance Auditor Practitioner and holds a certificate in ISO/IEC 27001 Information Security Management Principles. In 2015, Stacie was an ICANN NextGen participant.

Creating an inclusive digital future – urgent action needed

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