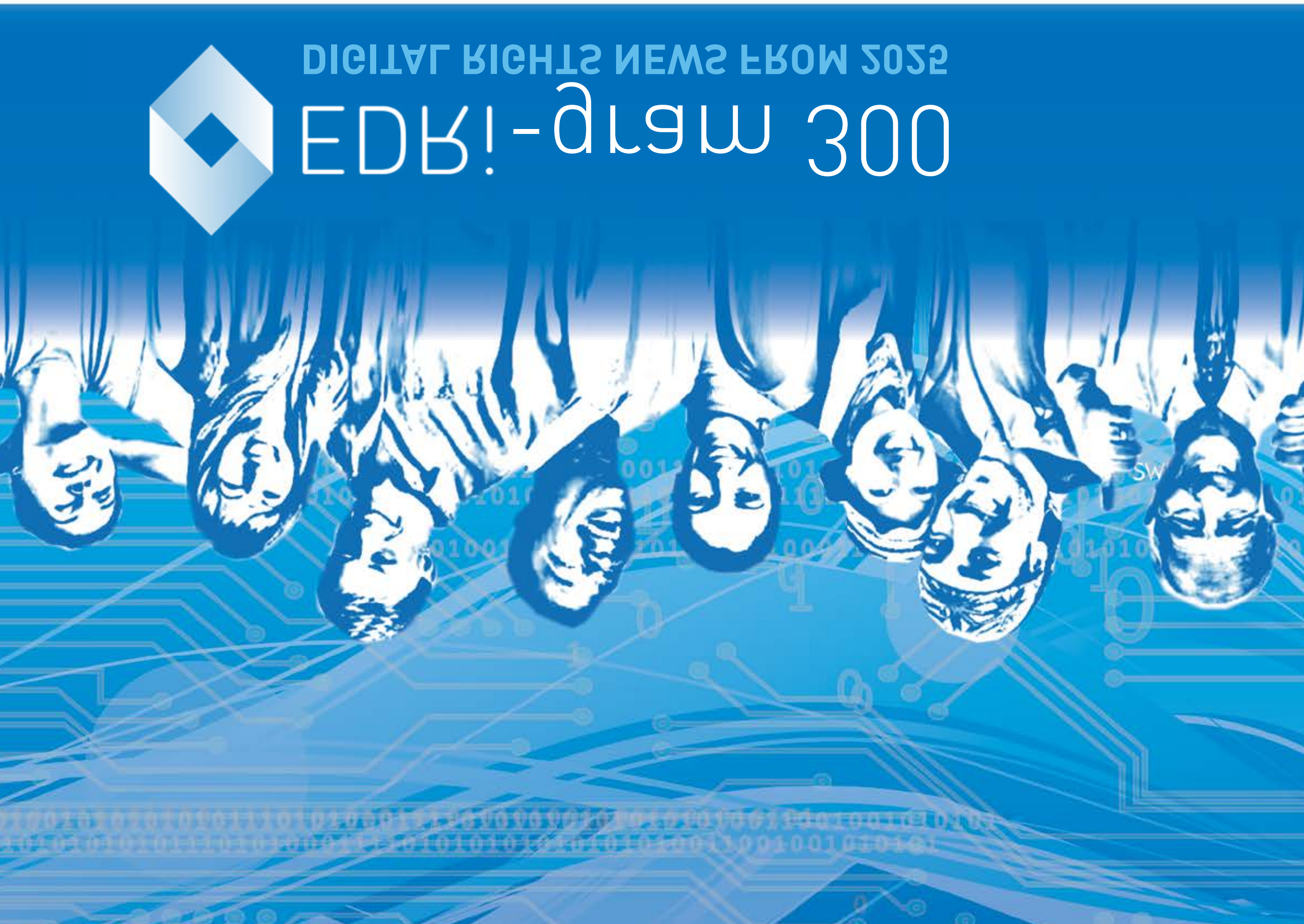
EDRi-gram 300

DIGITAL RIGHTS NEWS FROM 2025



EDRi-gram 300

DIGITAL RIGHTS NEWS FROM 2025

EDRi-gram 300 - Digital rights news from 2025

European Digital Rights (EDRi)
https://edri.org

Editors: Heini Järvinen, Joe McNamee, Kirsten Fiedler

Authors: Dunja Mijatović, Hans de Zwart, Simon Davies, Jillian C. York, Cory Doctorow, Katarzyna Szymielewicz, Joe McNamee, Jesper Lund, Kirsten Fiedler, Erich Moechl, Raegan MacDonald, Estelle Massé, Douwe Korff, Bogdan Manolea, Monica Horten, Annie Machon

FOREWORD

FOREWARNED

“For too long, we have been a passively tolerant society, saying to our citizens: as long as you obey the law, we will leave you alone. This government will conclusively turn the page on this failed approach.”[1]

- David Cameron

[1] Press release: Counter-Extremism Bill - National Security Council meeting, 13 May 2015 https://www.gov.uk/government/news/counter-extremism-bill-national-security-council-meeting

PREFACE

The EDRi-gram is the fortnightly newsletter by European Digital Rights (EDRi), a not-for-profit association of digital rights organisations from across Europe, defending human and civil rights in the field of information and communication technology. The EDRi-gram shares good news on positive developments in the defence of civil liberties and exposes and raises awareness of attacks on freedom of expression and privacy.

The EDRi-gram collates privacy advocates' news from across Europe. EDRi's members, observers and guest authors frequently contribute with reports and analysis from their home countries.

The first issue came out on 29 January 2003, and since then, 40 issues of the newsletter have been published each year thanks to the hard work of the editors Sjoera Nas from Dutch EDRi member Bits of Freedom (2003-2005), Bogdan Manolea from Romanian EDRi member Asociatia pentru Tehnologie si Internet, ApTI (2006-2014), and the current editor Heini Järvinen, EDRi's Community and Communications Manager. The EDRi-gram has a global reach and is being widely read by digital rights advocates, academics, policy-makers and interested citizens, both in Europe and around the globe.

Today, we are publishing EDRi-gram's 300th edition! To celebrate this occasion, we've collected articles from the brightest stars in the digital rights universe. This special edition, "EDRi-gram 300 - Digital rights news from 2025", reflects on the potential future threats and opportunities for digital civil rights in 10 years.

Andreas Krisch

Andreas Krisch is President of European Digital Rights (EDRi), of the Austrian Association for Internet Users (VIBE!AT) and the Austrian Forum Data Protection. In his professional capacity he is managing partner of mksult GmbH, an Austrian data protection consultancy.

Andreas regularly contributes to the European discussion on a data protection compliant adoption of Information Technology. He provides his expertise on data protection, RFID and the Internet of Things to institutions such as the European Commission, the European Parliament, the Council of Europe and the OECD, and he is member of the Austrian Data Protection Council, an advisory body to the Austrian Government.

TABLE OF CONTENTS

DIGITAL RIGHTS IN 2025 – SAME PROBLEMS

Dunja Mijatović

Dunja Mijatović, Bosnia and Herzegovina, is the OSCE Representative on Freedom of the Media. She took over this post on 11 March 2010. Mijatović is one of the founders of the Communications Regulatory Agency of Bosnia and Herzegovina. In 2007, she was elected Chair of the European Platform of Regulatory Agencies. Prior to this, she chaired the Council of Europe's Group of Specialists on freedom of expression and information in times of crisis. Mijatović is an expert in human rights; communications and media strategy, and regulatory and policy media framework. She has extensive knowledge of institution-building in transition states and many years' experience of issues related to journalist's safety and new technologies, with the emphasis on digitalisation, convergence and Internet technologies.

Gather the brightest minds and the best innovators from academia, international organisations and civil society and ask them to predict the technological landscape in 2025. The odds that they will come up with completely different visions and predictions are basically 1:10.

Unfortunately, the odds are that we will be fighting the same battles on digital rights in 10 years' time. Sure, the technology will have evolved, we will have new gadgets guiding us through our everyday lives and we will be connected to the Internet in ways we can't even grasp today.

Although I would like to say otherwise, I still think we will experience censorship, filtering and blocking of Internet sources. The major difference is that the curtailment of our digital rights will be more sophisticated. Add to that the surveillance programs infringing on the right to privacy, which are unlikely to either decrease or diminish in scope.

In ten years , we will still refer to the era we live in as the age of digitalisation – and the age of surveillance. Our fight to restore our basic human rights and to make sure they apply also on the Internet will be as fierce as today.

Human rights will still be inalienable, absolute and universal. And our main argument will remain the same; we have a right to these rights regardless of the platform through which we choose to enjoy them.

There will be one major difference. The battle for freedom on the Internet will not be the new frontline for the battle for freedom in the world. In 2025 it will be the main frontline.

Fighting the same battles for our digital rights in 2025 as we do today might not seem like something to write home about. But it is, for many reasons.

No one claims Internet regulation is an easy task or that it will be in ten years' time. Far from it. Still, there is one very easy rule when we are approached with this problem: Those who govern least, govern best. That's the headline I hope could be used for any news story on digital rights in 2025.

THE ROAD AHEAD: MARCHING BACKWARDS INTO THE FUTURE

Hans de Zwart

Hans de Zwart is Director of the Dutch digital civil rights organisation Bits of Freedom. He operates on the intersections between technology (which he prefers to be "open"), civil society, innovation and education. He believes that technology is never neutral and that design matters. He wished he was the first one to write that "technology creates feasibility spaces for social practice" (he wasn't...).

You can always talk to him about: the most recent book you have read, juggling, philosophy, free software, dominoes, or The Big Lebowski.

"People often overestimate what will happen in the next two years and underestimate what will happen in ten."

This is what Bill Gates wrote in his afterword for "The Road Ahead", his 1995 take on how our lives would change because of the "information superhighway". It is easy to look at his predictions now and point out all the things that he got wrong (he thought it wasn't likely we would receive video on our mobile devices for example), but it is more interesting to read into these predictions the preoccupations of that particular time. As McLuhan would say: We march backwards into the future.

Gates wrote quite a bit about privacy in the book. On the one hand he was concerned: "Loss of privacy is another major worry where the network is concerned. A great deal of information is already being gathered [..] and we often have no idea how it's used or whether it's accurate." But he was also naive: "A decade from now you may shake your head when you remember that there was ever a time when any stranger [..] could interrupt you at home with a phone call. [..] By explicitly indicating allowable interruptions, you'll be able to re-establish a sense of a sanctuary."

If I try to extrapolate current trends and developments ten years into the future, then it is exactly this sanctity of the home that seems to be under pressure. In the next few years the "things" in our house will all get their own operating system connecting them to the Internet. Today it is a toothbrush that can tell you whether your kids spend enough time brushing their teeth, a weighing scale that tweets your weight to the world to keep you motivated, or an electronic book that tracks your reading habits. Tomorrow it might be your washing machine ordering its own detergent or your candles tracking their own burning hours.

Today it seems like all my Internet connected devices always have some updates that need to be downloaded right when I need to use them. I often joke that I don't look forward to a future where I can't open my washing machine because it is "Downloading 3 of 8 updates", or where I can't light my candles because they are getting a firmware upgrade for a better and safer user experience. But there is a serious point to make too. Gates seemed to assume that you would be in control over your own technology. You could explicitly set your preferences and your technology would just comply. This is not the direction we are moving in now. Governments are forcing "smart" energy meters into many households that report your energy use back to headquarters, eBook providers are remotely deleting books from their customers' devices and cars can already be turned off from a distance when a car payment is overdue.

The 1995 Bill Gates would be appalled by how little control we have over our own devices today. If we continue down the current road, I think our current selves will be appalled by our future situation, too. It is therefore important to take back control over our devices to ensure that we will have meaningful agency in the coming years.

A LETTER FROM THE FUTURE

Simon Davies

Simon Davies is widely acknowledged as one of the most influential data protection and internet rights experts in the world and is a pioneer of the international privacy arena. He has founded numerous key initiatives such as Privacy International, the Big Brother Awards and Code Red. His work in consumer rights and technology policy has spanned nearly thirty years years and has directly influenced the development of law and public policy in more than 50 countries.

He has advised a wide range of corporate, government and professional bodies, including the United Nations High Commissioner for Refugees. Simon has worked in various roles in the London School of Economics since 1996, and is currently an Associate Director at LSE Enterprise.

It is 2025, and this is a scary time for privacy. The new era of interactive technology that silently grew from the early 21st century now feels like a living organism that wraps ever more tightly around us. It's not meant to be hostile, just helpful. But increasingly, all of us feel like mere subjects of a new Technological Order.

This development was once called "The Internet of Things". In its original form, this was merely a mass of radio-frequency identification (RFID) devices. Now it is the new data grid that carries more personal information than any platform in history – and it was created in less than a decade.

Almost every item on the planet now has sensor technology that interfaces with the digital ecosystem. These sensors are often locked into the mobile spectrum, pumping out vast amounts of usage data to ensure your safety.

Omnipresent health and safety control has found synergy with the technology. Even food packaging now has sensors that alert you to use-by dates and possible health risks – whether you want the information or not. Never before has Judge Brandeis's idea of the "Right to be let alone" been more meaningful.

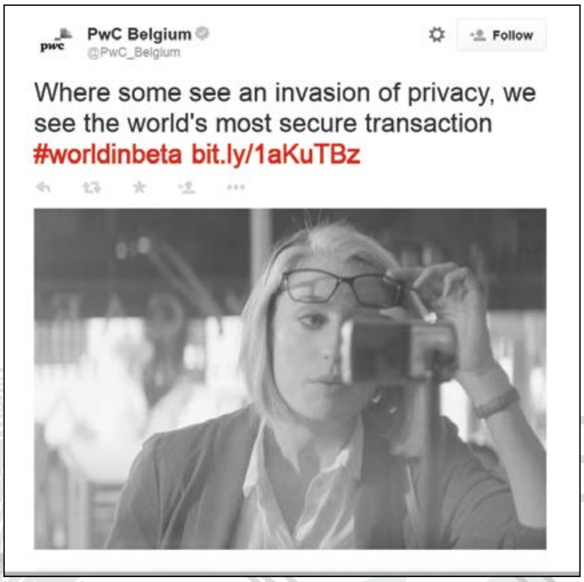
The most intricate interface involves "high risk" activities such as recreational drugs, drinking, exercise, sports and even some forms of sex. Increasingly, there's a legal obligation to directly link the items being used to the identity of an individual. In many countries you cannot even buy a bottle of whisky without a sensor being linked to your identity.

Because driving is generally considered a high risk activity, we long ago gave up any idea of the "open road". Every movement – on the road and off – is minutely analysed, and in many cases is linked to your profile of interactions with other high risk activities (such as alcohol consumption). All vehicles – even bicycles – have become surveillance devices that continuously analyse and transmit data. Indeed many common items are openly manufactured as continuous surveillance devices, including almost all doors and windows, items of clothing, road surfaces and rooftops.

We once imagined that all this communication between people and things – and things and things – could happen anonymously. And there was a brief period when such privacy was actually possible. But now the ecosystem knows what you cook, where you are, who you are with and what you're doing – together with all the dangers and variations in those patterns. It's the new social contract.

For some of us, the most unsettling feature of our life these days is the fact that many people openly publish this information, not just to their own networks, but to the world at large. Full disclosure has become the accepted way to validate your character and integrity. And full disclosure is also the best way to achieve credibility with potential employers, future friends, insurers, banks, schools and commercial organisations.

It's not all bad. Wealthy societies are certainly safer and more orderly now, but the idea that people could have freedom to do as they please and that they could control what is known about them has vanished. As long as we assume that this society is perfect, maybe we don't need to worry that dissent is impossible and our community can no longer evolve.



PwC Belgium
@PwC_Belgium

Where some see an invasion of privacy, we see the world's most secure transaction #worldinbeta bit.ly/1aKuTBz

SOCIAL MEDIA PLATFORM™: "REMOVAL OF CONTENTS NECESSARY FOR USER SAFETY"

Jillian C. York

Jillian C. York is a writer and activist who serves as the Electronic Frontier Foundation's Director for International Freedom of Expression. She is the co-founder of OnlineCensorship.org, a platform that seeks to inform the public about intermediary censorship.

The text called for a peaceful uprising in the imaginary country of Absurdistan. But regardless of the fictional nature of the post, it was swiftly removed from The Social Media Platform™, the terms of service of which began banning calls for uprisings in late 2019 under a general prohibition of "calls for changes to the political, social, economic, government or other status quo".

It was around 2010 when digital rights advocates began to really become aware of the threats to free expression posed by Internet companies, the so-called intermediaries. Prior to that, groups such as the Global Network Initiative had raised awareness of the role of intermediaries vis-a-vis governments, but until the second decade of the century, the public was generally unaware of how corporate entities like Google and Facebook controlled and manipulated content and free speech on their platforms.

The issue reached its zenith around 2018 when, following the publication of Rebecca MacKinnon's second book (a dystopian follow-up to 2012's Consent of the Networked: The Worldwide Struggle For Internet Freedom), activists began a movement dedicated to eradicating censorship from major social media platforms. While the movement had some early successes, the eventual merger of the world's most popular social media platforms into The Social Media Platform™ quickly quashed the movement. With six billion subscribers posting cat videos and daily photos of meals, the Platform™ simply became too big to fail.

Today, there's one thing activists can count on when they use social media: Censorship. The Platform™'s 173-page Community Guidelines dictate what users can and cannot write, post, or search for, with artificial intelligence text interpretation meting out swift, summary “justice”. Violators of the rules will find their accounts immediately terminated, with no chance of appeal. While some have spoken out about the rules, calling them “draconian,” “absurd” and “totally fascist”, The Platform™’s CEO claims it is necessary for user safety and that nobody is forced to sign up. Advertisers aren’t subject to the guidelines.

Although netizens still have some alternatives, such as Identi.ca, users of the service often complain that they feel they’re shouting in an echo chamber. “I’d rather use a service like Identi.ca,” said activist Allen Smithee, “but literally everyone I know is on The Platform™.”

This is entirely a work of fiction, but not an impossible future. For more information on how social networks police speech, read MacKinnon’s excellent book or my 2010 paper, “Policing Content in the Quasi-Public Sphere”.

PM LANE FOX REINSTATES MODDING

Cory Doctorow

Cory Doctorow is a non-fiction and science fiction author, activist, journalist, blogger and the co-editor of Boing Boing. He works for the Electronic Frontier Foundation and co-founded the UK Open Rights Group.

Quick: what do all of these have in common? Your gran's cochlear implant, the WhatsApp stack, the Zipcar by your flat, the Co-op's 3D-printing kiosk, a Boots dispensary, your Virgin thermostat, a set of Tata artificial legs, and cheap heads-up goggles that come free with a Mr Men game?

If you're stumped, you're not alone. But UK Prime Minister (PM) Lane Fox had no trouble drawing a line around them today during Prime Minister's Questions (PMQs) in a moment that blindsided the Lab-Con coalition leader Jon Cruddas, who'd asked about the Princess Sophia hacking affair. Seasoned Whitehall watchers might reasonably have expected the PM to be defensive, after a group of still-anonymous hackers captured video, audio and sensitive personal communications by hijacking the princess's home network. The fingerpointing from the UK Government Communications Headquarters (GCHQ) and Military Intelligence (MI6) has been good for headlines, and no one would have been surprised to hear the PM give the security services a bollocking, in Westminster's age-old tradition of blame passing.

Nothing of the sort. Though the PM leaned heavily on her cane as she rose, she seemed to double in stature as she spoke, eyes glinting and her free hand thumping the dispatch box: "The Princess Sophia affair is the latest instalment in a decades-old policy failure that weakened the security of computer users to the benefit of powerful corporations and our security services. This policy, the so-called "anti-circumvention" rules, has no place in an information society.

"Anti-circumvention pretends to be a rule against picking digital locks. These rules prohibit modifying your WhatsApp so that it can place a call without police listening in. They prohibit changing software on your National Health Service (NHS) cochlear implants to stop your conversations being analysed by terrorism scanners. They prohibit tinkering with your goggles to allow you to cheat on games, they prohibit tampering with your thermostat so that you can keep your heat turned up when the power company needs you to turn it down. They prevent 3D printers from making guns, they prevent wet printers from mixing prohibited narcotics. They allow Wonga to immobilise and repossess your artificial legs, and they stop car thieves from making off with Zipcars.

"This government supports many of these goals, but we cannot and will not support the means by which they are achieved. If three decades of anti-circumvention have taught us anything, it's that it doesn't work. Clever people have always figured out how to get round these locks and the computer scientists tell us they always will. But these rules also have a chilling effect on security research.

"Scientists who go public with information about weaknesses in systems protected by anti-circumvention are at risk of prosecution, and face powerful adversaries when they do. So, a system covered by anti-circumvention becomes a reservoir for long-lived security vulnerabilities -- programming defects that attackers like the ones who compromised Her Highness leveraged in the course of their grotesque and unforgivable crimes."

"The princess will have her systems audited by our security services, but the rest of us are not so fortunate. What do we say to the man who is robbed by thieves who take over his artificial legs? The grandmother whose privacy is violated by eavesdroppers who listen in on her most intimate conversations? The driver whose car is hijacked and driven to a remote place where she is at risk of robbery and even rape? What do we say to the family whose heat is disconnected by pranksters in the dead of winter? These are not mere hypothetical. This parade of horribles are all real-world examples from the past year. It is for these reasons that we will introduce legislation this week to eliminate all anti-circumvention statutes."

PM Lane Fox's own backbenchers grew increasingly jubilant through the speech. At the end, they were on their feet, roaring and gesturing for the cameras. And the Lab-Cons? Apart from one or two of the more savvy members, most of them seemed baffled by the whole affair.

But the PM clearly knows what she's about. She was trending throughout the Anglosphere and Commonwealth last night, and has had letters of support from Pirate Parties from Tunisia to Iceland. Elsewhere in today's edition, Italian PM Beppe Grillo's exclusive editorial supports PM Lane Fox, saying, "The Prime Minister is the only global leader who knows what she's about. The world has long waited for a political class that understands the importance of technology: finally, it has one."

The article was originally published in Wired Reports Back From 2024 (http://www.wired.co.uk/magazine/archive/2014/07/features/wired-dispatches-from-2024).

PROFILING TO SOLVE EUROPE'S DEMOGRAPHIC CRISIS?

Katarzyna Szymielewicz

Katarzyna Szymielewicz is a lawyer specialised in human rights and technology and Co-founder and President of EDRi member Panoptykon Foundation – a Polish NGO defending human rights in the context of contemporary forms of surveillance. She is Vice-President of European Digital Rights – a coalition of 33 privacy and civil rights organisations, board member of Tactical Technology Collective and Amnesty International (Poland), and Member of the Council for Digitisation in Poland.

After the failure of many public programmes aimed at getting Europe out of its demographic crisis, eyes of the governments have turned towards Internet Service Providers (ISPs). Who should know better than them how to convince younger generations to give up on clubbing and make babies?

Policy makers hope that the same companies and advertising experts who created the currently dominating demand for individualistic lifestyle, will now find a way to start another trend. An informal coalition of Internet Service Providers, led by the Social Circle and the Search Engine, accepted the challenge. This new public-private project aimed at increasing the birth rate in Europe will be rolled out in the coming months under the label "Future is Family".

"Our key challenge is to identify real obstacles that prevent citizens from creating families. After years of running public programmes that offer financial support for young couples, we understood that these are not just financial or employment related concerns. Apart from such rational calculations, we are looking at a deep, cultural trend, which can only be tackled by soft measures, such as social advertising," said EU Commissioner for Migration, Home Affairs and Citizenship, explaining public rationale behind the programme.

How can Internet generated data wealth be harnessed for public policy reasons? After the successful use of vast amounts of commercial data, such as telecommunication metadata, email contents and search engine queries for public security purposes, the task seems to be manageable. Companies that declared participation in the "Future is Family" initiative seem optimistic:

"We plan to use our cutting-edge data analytics tools and predictive profiling schemes to meet the real needs of our clients when it comes to their love and family life. Algorithms will be redesigned to identify and suggest a perfect life partner, the optimal time to get pregnant or health insurance for the whole family at a good price. Modifying news feeds to promote positive mentions of family is a socially responsible thing to do. We are excited to be part of the program, which may change the future of our societies, not only by contributing to economic growth, but also high happiness indicators. Our recent research clearly indicates that adults living single lives are more likely to suffer from depression. We have the ambition to reverse this trend. We have a social responsibility to make people feel the emotions that will promote economic growth," explained the CEO of the Search Engine.

Details of this public-private initiative are yet to be announced but it is already clear that all types of user-generated data from search engines and social media will be used to ensure extremely efficient behavioral targeting and content manipulation. Companies will be allowed to integrate data about citizens' consumer preferences, travel patterns, education, professional life, age, sexual orientation, ethnicity, history of intimate relationships and financial status. EU officials working on the programme confirm that existing data protection principles are flexible enough to justify such broad use of data, including sensitive information, when vital public interests are at stake.

In Brussels, the level of concern about possible economic and social implications of the demographic crisis has reached a point where counter-arguments are barely present in the debate. The only point discussed at the high-level meeting of relevant EU Commissioners and Internet Service Providers was citizens' privacy. What if somebody would prefer not to be included in the program? The answer was very straightforward: Citizens will be given the right to opt out or modify their "family" profile, for example by declaring their preference to remain single. However, our anonymous source in the European Commission warns that such choices may come at the price of a more expensive health insurance or a higher tax rate. It does seem that some crucial details of the "Future is Family" initiative still remain unknown and we can expect more controversies around the program.

CASH IS FOR CRIMINALS AND PAEDOPHILES

Joe McNamee

Joe McNamee is Executive Director of EDRi, having joined the organisation in 2009. He has been working in internet-related sectors almost continually since 1995, when he joined CompuServe UK as a customer service agent.

On 20 May 2025, the governor of the European Central Bank (ECB), the Director General of Europol and the European Minister for Financial Affairs announced at a press conference in Frankfurt that the Euro, in physical form, would cease to exist by the middle of 2028.

“Cash money is simply unacceptable in today’s society,” Minister Plutus announced. “With mobile banking allowing even the smallest transactions to be undertaken electronically, there is just no more excuse for the chaos that is cash”.

This analysis was backed up by the governor of the ECB. The cost of maintaining millions of coins and banknotes, transporting them around Europe, printing new cash, minting new coins is just unacceptable, he explained.

Europol Director General Gerrae Rumoribus: “Look, we’ve been saying it for ten years – if you “follow the money”, then you have no crime. Innocent people have nothing to hide – they have supermarket loyalty cards already – so why not have an electronic trace of every transaction that they make? Imagine a world with no crime, no money laundering and we save money in the process! The only people that will oppose this measure are criminals and paedophiles”.

In response to questions about the threats to the privacy of citizens, the Director General was very clear – it will not damage existing privacy rights. He explained that we already have the “only once” e-government approach launched by the 2015 Digital Single Market Communication. He reminded the one journalist at the press conference that the “only once” principle was subsequently expanded to allow access to all citizen data by all relevant national government agencies across the 28 EU Member States, following a very helpful parliamentary question from Liberal MEP Antanas Guoga in 2015.

Added to this we have the 2018 Network Access Knowledge and E-Devices Discovery (NAKEDD) Directive, which gives us access to all online searches, social media interactions and mobile location data. If we already know you are searching for health information from your online searches, if we already know that you are going to the pharmacy from your mobile location data, is it really that much of a problem that we will know exactly what you bought, when you bought it, how often you bought it and why you bought it?

All three leaders concluded the session by confirming that, as many have forecast for years, it is finally time for the EU to completely stop making cents.

NEW PRIVACY IMPACT ASSESSMENT OF DANISH E-GOVERNMENT SERVICES

Jesper Lund

Jesper Lund is Vice-Chairman of EDRi member IT-Political Association of Denmark (IT-Pol), a volunteer digital rights organisation with around 200 members. Since 2011, he has worked on data retention, privacy, government and private surveillance, and net neutrality. His daytime job, to support his passion for digital rights, is teaching financial economics.

In April 2025, an independent privacy impact assessment of the Danish public sector was published. The European Commission has often praised the Danish government for its efficient data processing practices and suggested Denmark as a role model for other Member States, even though serious privacy concerns have been raised by Danish NGOs, including EDRi member IT-Pol Denmark.

Denmark has never introduced mandatory ID cards, but every Danish resident has a social security number, which is used in all public-sector systems, from health care to tax management. The pervasive "once only" principle means that Danish citizens never have to provide the same information to two different public authorities. Instead, the various databases, all based on the same citizen ID number, are closely integrated so that data can be re-used.

The integrated databases also make it easy for the Danish government to use data about citizens for entirely new purposes. All Danish citizens are regularly subjected to profiling for welfare fraud and tax evasion. Secret data-mining algorithms with access to all databases produce lists of possible suspects. Some citizens complain about being under surveillance, but they are told that if they have nothing to hide, they have nothing to fear. Still, news media regularly cover cases where citizens with unusual behaviour are put on suspicion lists, even though they have broken no laws.

Between 2010 and 2025, the Danish model with centralised databases and the "only once" principle was gradually expanded into a public-private partnership. This was facilitated by the Danish eID system, which was developed as a joint venture with the banking sector, and by 2020 used as single sign-on for virtually every website in Denmark. With the eID system, public and private databases could be integrated in a secure way, the Danish government argued.

By 2014, the financial sector could access citizens' income data from tax authorities, for example for credit assessment. In the beginning, consent was required for every data transfer and citizens could choose to document their income in other ways. But after a couple of years, banks only accepted the automated information exchange, and consent was effectively coerced. Later the data-sharing set-up was extended to other parts of the private sector, and the government soon became the preferred data broker for private companies. Giving consent for private companies to access personal information in government databases was generally compared to clicking on the cookie consent pop-ups that had existed on websites until enforcement of article 5(3) in the E-privacy Directive was silently abandoned in 2018.

The most important part of the Danish public-private partnership for personal data is medical research. All medical records from hospitals and general practitioners are put in a central database, which is made available for research by universities and private pharmaceutical companies without consent, justified by a liberal interpretation of the research exemption in the EU's new Data Protection Regulation, which was finally adopted in 2017. Unlike most other countries, medical data from the Danish government can be combined with all kinds of socio-economic information since all databases use the same citizen ID number. Even life-style information such as alcohol consumption and eating habits can be included. In co-operation with the retail sector, Danish banks register all purchases made with credit cards, and cash is no longer accepted as payment at Danish stores.

The outcome of the privacy impact assessment came as a major surprise to the Danish government. The report concluded that the public sector data processing, and especially the partnership with private companies, undermined the privacy and data protection rights granted to Danish citizens by the Charter of Fundamental Rights of the European Unionand the European Convention on Human Rights. A number of changes must now be made in order to bring Danish e-government data protection standards in line with fundamental rights.

NEURO-IMPLANT HACK REVEALS SECRET DEALS BETWEEN HEALTH INSURERS AND EMPLOYMENT AGENCIES

Kirsten Fiedler

Kirsten Fiedler is EDRi's Managing Director, an organisation which defends human rights in the information society. After her European studies in the UK, France and Germany, Kirsten became a blogger reporting on digital rights issues and started advocating for free speech and privacy rights in the digital environment. She is also a member of Digitale Gesellschaft e.V. and the Chaos Computer Club. Born nearby Cologne, Germany, Kirsten is now based in Brussels.

Neuro-implants by Europe's largest insurance company Axia have been hacked, according to a report published by German newspaper Penrose. The company's implants connect the nervous system to the Internet in order to monitor, store and synchronise health data with individual home devices and the company's servers.

Blue Ant, a German-based neuro-hacker group, has now demonstrated that health data synchronised with the insurance company's server has been systematically transferred to employment agencies. Further investigations reveal a deal between Axia and several human resource outsourcing companies.

Implants have long made the transition from being used exclusively for severe problems such as deafness, blindness and amnesia. Although there has been resistance to the first generation of commercial brain implants, an increasing number of people are currently opting for the second – and significantly cheaper – generation, due to the discounts and other incentives offered by insurance companies.

The neuro-implants monitor blood glucose, breathing and heart rates and can therefore sense the onset of chronic illnesses or stress. Moreover, Axia recently started testing the stimulation of specific regions of the brain that are responsible for addictive reactions, for example in order to reduce nicotine and alcohol craving, with 'beneficiaries' able to benefit from cheaper insurance rates. Blue Ant demonstrated that it was possible to access this latest generation of implants and to re-programme stimulations sent by the implants to the brain.

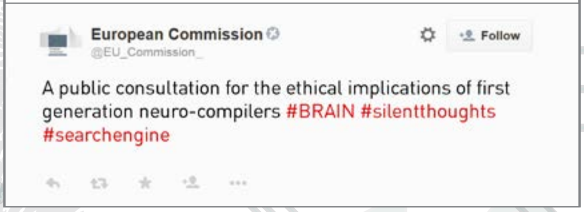
An open letter by thirty-six civil rights groups published yesterday, argued that this incident shows, once again, that citizens no longer have control over their personal data. The organisations criticised the fact that health data are being shared with human resource companies, led to a situation where these are able to create detailed risk profiles based on the job applicants' information. Applicants can then be accepted or rejected due to information that is not available to them.

It has indeed become increasingly difficult for people to be aware of what personal data is circulating about them and to change information held by companies that is false or outdated. In recent years, this has leding to various negative consequences for individuals, ranging from price discrimination to arrest orders.

In their letter, the organisations therefore call for the revision of an eight-year old law that is simply no longer fit for an era of permanently connected citizens. The last reform of privacy rules that was finalised in 2017, failed to provide for meaningful protections especially with regard to the so-called "legitimate interest" exception that allows data to be collected and re-used by third parties, including for profiling.

Today, as demonstrated by Blue Ant, this means that insurance companies are completely free to unilaterally decide that their interest in processing citizens' data is greater than any possible harm to citizens from this processing. Consent is not needed if the company feels that it has a "legitimate interest" in processing data. As revealed by the hack, these data are now being passed on to other companies that are processing personal information for reasons that are completely unrelated and incompatible with the original purpose.

In related news:
European Commission's B.R.A.I.N research project is currently holding a public consultation on the ethical implications of first generation neuro-compilers. These consist of implanted interfaces connected to the Internet that will be able to automatically translate clearly articulated silent thoughts into an online search engine and project a summary of the results directly into the brain.



A public consultation for the ethical implications of first generation neuro-compilers #BRAIN #silentthoughts #searchengine

FIRST COURT HEARING OF "SCHREMS VS THE EUROPEAN COMMISSION" CASE

Erich Moechel

Investigative journalist Erich Moechel primarily writes for ORF.at, the webportal of the public broadcaster ORF in Vienna. After a career in Austrian daily and weekly print media and radio 1983-1995, he turned to WWW-publishing only in 1996. Erich M. first became publicly known to a wider public when he published the so called ENFOPOL papers containing the secret EU GSM surveillance plans in 1998.

Today's initial hearing in the lawsuit commonly called "Schrems versus the European Commission" at the European Court of Justice (CJEU) saw a record-breaking number of high profile defendants.

Thirteen former EU Commissioners, including two Vice Presidents and a former head of Unit of the Commission face a crucial CJEU decision. All of the defendants have been indicted at their respective national courts before, some are already appealing convictions of data fraud, wilful deceit of the European public, embezzlement or similar clauses. Three of the appeals are against convictions of espionage for a foreign power at courts in Portugal, Sweden and Belgium. All of these cases concern the roles of the Commissioners in international agreements such as the "Safe Harbor" agreement, or agreements on the wilful de facto theft and export of Passenger Name Records (PNR) or financial data that had been bundled to one lawsuit in 2023 and sent to the CJEU for a framework decision.

Plaintiff Max Schrems is a professor of international law at the Sorbonne and best known for his successful lawsuit against Facebook in 2021. Schrems had sued Facebook for wilful, repeated and organised data larceny in 270 million European cases and won 19 billion euro compensation.

Note : Both the author and European Digital Rights know that such activites fall outside the real scope of the Court of Justice of the European Union. As Police Chief Wiggum of Springfield Police Department once said, the law « is powerless to help you, not punish you ».

THE YEAR 2025: A NEW HOPE FOR PRIVACY

Raegan MacDonald

Raegan MacDonald is European Policy Manager at EDRi member Access' Brussels office. She specialises in net neutrality, privacy and data protection. Raegan is a member of the Steering Group for Code Red, an ambitious global initiative providing resources and tactical advice to human rights groups and human rights defenders across the world. She is also an Advisory Board member of the Brussels Privacy Hub, an academic research institute focused on privacy and data protection. Since March 2014, Raegan is a Privacy by Design Ambassador, an award from the Privacy Commissioner of Ontario, Canada.

Estelle Massé

Estelle Massé is Policy Analyst at Access. From Brussels, she works on net neutrality, data protection, data retention and trade agreements. Prior joining Access, Estelle interned with European Digital Rights (EDRi) and graduated with a Master in European Law from the University of Granada in Spain.

July 2025, Brussels - Yesterday, members of a global privacy movement gathered in front of government buildings and corporate headquarters around the world, just as they have done every day for the past several months.

The privacy campaign, inaccurately described as privacy "riots" by some media outlets, has grown steadily since late 2019, when a string of high-profile data breaches shook the public, spurring citizens to demand an end to what they call "data appropriation".

Until 2019, most of the people who are now part of this mass mobilisation didn't seem to understand the importance of privacy in their lives. All of that changed on the morning of 8 April, when a flood of sensitive financial data was leaked through a massive breach of the Terrorist Financial Tracking Programme (TFTP) databases, leading to millions of people becoming bankrupt from accounts that had been emptied. Most citizens hadn't even known about TFTP, part of a nearly decade-old programme ostensibly developed to detect and prevent terrorist crimes. Citizen outrage deepened when an investigation after the breach revealed that the programme never led to the arrest of a single suspected terrorist, yet a terrorist group had successfully used it to expose the private data of millions of people around the world.

In the aftermath of this unprecedented data breach, additional breaches in the private sector fuelled the movement's progress. None was more rousing than the Smart Home scandal of 2021. Often referred to as the "breach that broke the camel's back", the scandal erupted after it was revealed that Smart Home alarm systems had systematically been recording private conversations taking place in people's homes. Not only were conversations being recorded, but they were secretly being shared with law enforcement and intelligence agencies. These data were merged with Intenet browsing data, mobile location data and supermarket loyalty card data to generate new information guessing at the likelihood of criminality, health problems, increased insurance risks, financial stability and other commercially valuable information

Now, four years after the Smart Home scandal, privacy protests take place daily, from New York to Brussels, Sydney to Cape Town, Delhi to Buenos Aires. Most of the protests are peaceful "sit ins," where activists gather in front of landmark buildings. Government officials have responded to these protests by arguing that spy programmes and information sharing with corporations are vital to security. They have successfully partnered with social media companies to pollute news feeds with critical news articles, misleading information about low turnout to the demonstrations and mood manipulation, to discourage activism.

Fortunately there is a glimmer of hope. Now mired in crisis, government officials have signalled that they are willing to meet with leaders in the privacy movement to hear their demands. Technology companies, now hobbled by bad publicity and consumer boycotts, have begun to experiment with new approaches and business models that respect the privacy of users' data. It may have taken a global crisis, but 2025 could be the year we get our privacy back.

THE RED PIXEL CURTAIN

Bogdan Manolea

Bogdan Manolea was the EDRi-gram editor between 2006 and 2014. He still lives in Bucharest, Romania. He is the Executive Director of the Romanian EDRi member Association for Technology and Internet (ApTI).

What's tiny, dark and knocking at your door? The future.

1 May 2025. The day when the so-called "new Internet infrastructure" rolls out after the old Internet was deprecated following massive Distributed Denial of Service (DDoS) attacks that made accessing any web page almost impossible. It is still unclear who was behind those attacks, but we know the result today - three major Internets and hundreds of smaller ones:

The European Internet, called EUNet, is now a functional reality. The long lasting desire of some bureaucrats has won, despite all possible technical, economic and societal arguments. All European Internet Service Providers (ISPs) and mobile operators must from now on use the EUNet, a space where "all Europeans will be safe", as the European Commission President Nicolas Sarkozy advertised in his manifesto for a cleaner Internet since he took over the Brussels position in 2019. Now this "civilised zone of the digital world" is the new mandatory Internet of the European Union Federation - a digital world where no unwelcome content is allowed, where there's no counterfeiting and no copyright infringement. At least this is how it was promoted before the former Internet was abandoned. Everyone will have complete freedom to be fully protected from anyone with views that might be unwelcome. As Sarkozy had promised, Europe redefined its freedom in ways that ensured that terrorists could never take it away.

But I don't know how the EUNet works...

The FreedomNet, which was set up by the US, UK, Australia, Japan and Canada is the other part of the former Internet. It inherited a major part of the old features of the Internet from 2017, after the revelations of James, Jones and Jimmy had shown that the United States National

Security Agency (NSA) was actually a major shareholder in Facebook, Google and Yahoo, allowing them to not only have direct access to the data collected through these services, but to also merge the databases. Based on the Digital Safe Harbor Agreement between the US and the EU, some websites and services are accessible from one network to another. It's like the limited duplication of functionality in certain apps for Android and iOS in 2015, but slightly better.

But I don't know how the FreedomNet works, either...

Look no further than Enlightenment Internet, nicknamed the "red pixel curtain". It's red, according to the colour of the first letter of the logo of Yandex, the mandatory search engine that opens instantly as the home page of every browser accepted in the network. The Enlightenment Internet was the idea of Putin, during his sixth presidential term. His IT team took the "best" out of the open source software of the FreedomNet and EUNet in a new proprietary system.

The automated copyright infringement detection tool in EUNet has been re-purposed to identify and deny posting of all content that could be considered as unfair criticism to the current political leaders. Browsing and e-mail data are merged with location data and facial recognition to identify individuals who might use the EUNet for evil purposes and automatically disconnect them. The system builds on the great "child-protection-from-bullying" feature and has been transformed into a "mandatory-Internet-ID" system that tracks and stores all your digital activies for six years in a central server system hosted in the Antartic. Besides Russia and China that actually manage the entire Enlightenment Internet's content and infrastructure, other Asian countries and European countries now outside the European Union Federation were slowly but surely included in the largest digital network of the world, as part of a carrot-or-stick game with economic sanctions.

But I don't want to know how the Enlightenment Internet works. It's just too depressing.

The reality is that we've destroyed the Internet that we had expected to be able to pass on to future generations as our generation's greatest legacy. Now that we've lost it, it would be a good time to invent time travel, go back 10 years and start supporting digital freedoms. Because the price of liberty is eternal vigilence. It is time we started paying it.

All characters, countries and situations appearing in this work are fictitious. Any resemblance to reality is purely coincidental and should be treated as a technical red pixel failure.

2025 – WHAT ARE THE ODDS FOR A COPYRIGHT CRISIS?

Monica Horten

Monica Horten is a Visiting Fellow, London School of Economics and Political Science. She is a member of two European expert groups, including being an independent expert on the Council of Europe's Committee of Experts on Cross-border Flow of Internet Traffic and Internet Freedom. She is the author of two books - A Copyright Masquerade: how corporate lobbying threatens online freedoms & The Copyright Enforcement Enigma: Internet politics and the Telecoms Package - with a third forthcoming in 2016. Her Iptegrity blog has generated a core readership among the Brussels policy community. She has been an invited speaker at conferences around Europe. Her academic research, which includes several peer-reviewed academic papers, has had measurable impact both in the media and in scholarly journals. In a private consulting role, she assists with policy analysis and reports.

A prediction about the future of copyright is always a little tricky, especially in the complex world of the Internet. Are we going to see a resolution to the attacks on Internet intermediaries? Are we going to see vertically integrated intermediares welcoming calls for them to become Internet police? Will we see a drama turn into a crisis?

From a digital rights perspective, a key issue will be how the entertainment industries will manoeuvre politically. These are global corporations, who are engaged in global political campaigns in order to enforce a system of copyright that ultimately protects their monopoly businesses. Over the past twenty years, these corporations have called for a re-invention of the Internet to suit business interests. Their main tactic is to lobby for liabilityprovisions for Internet Service Providers (ISPs), to coerce them to monitor and police the Internet. That's why we've seen "three strikes" measures that require them to disconnect people from the Internet if they are accused of breaching copyright law. They have also successfully demanded the implementation of an array of court injunctions, which force intermediaries to restrict web content.

There is now a growing body of research and case law to show how these restrictive actions can restrict free speech. The risk is that legitimately shared content is restricted also. There are various ways that this risk manifests itself, depending on the exact technical procedure for implementing the court-ordered measures. But that the risk is real , is not in doubt, as illustrated recently when legitimate customers of the Cloudflare service found themselves on the wrong side of a copyright blocking injunction.

The abutment of free speech rights and copyright creates an edginess to policy-making. It is exciting, and dramatic, but also tough. There is no straightforward decision path based on economic evidence. Instead, diligent policy decision-making is about balancing rights, and this puts policy-makers between a rock and a hard place.

However, copyright has found ways to squeeze through. The attempts to include copyright and intermediary liability into trade agreements such as Anti-Counterfeiting Trade Agreement (ACTA) and Trans-Pacific Partnership (TPP) is well known. Less well understood is how copyright is sneaking into filtering measures.

Rights-holder lobbying is relentless. Pleading that they are victims of a terrible Internet scourge, the entertainment industries have embedded themselves in lobbying coalitions and government committees. They have politicised their business issues in order to earn State backing for enforcement of their copyrights. In the past 10 years, we've seen huge pressure wielded as the entertainment corporations persistently turn to parliaments – both national and European – with demands to "clean" the Internet. They've drafted amendments and even entire laws, handing policy-makers ready-made solutions. In political moves that have confounded copyright traditionalists, the rights-holder lobbyists have repeatedly targeted telecoms law. The desired level of Internet restrictions has been stepped up each time.

Free speech rights provide the only bulwark against these ever-increasing Internet restrictions. Digital rights campaigning has played an important role in supporting that bulwark against the weight of entertainment industry lobbying departments. As a consequence, the political tension in this policy area is high.

The European Union wants to reform copyright. However, it is not even clear what would be meant by copyright reform under these circumstances. For some people, it means harmonising the exceptions to authors' rights. For others, it means freeing up distribution of content. Any such proposals will be sure to result in rights-holders swinging in with counter-measures for stronger enforcement. They will be re-imagining the Internet, phase 2.0. In this environment, copyright reform for the Internet era will become a high-wire act.

Turning to the question we began with, we may well wonder how the ongoing political drama will play out. More precisely, what are the odds on a political resolution for copyright reform by 2025? It's clear that copyright policy is not isolated, and any changes will result in significant effects outside the entertainment industries. If the balance is not handled carefully, the drama could well turn into a crisis.

DANGEROUS DATA

Douwe Korff

Douwe Korff is Emeritus Professor of International Law at London Metropolitan University and an Associate of the Oxford Martin School of the University of Oxford.

This short article draws on a 2013 Council of Europe report, written by the author, on "The use of the Internet & related services, private life & data protection: trends & technologies, threats & implications".

The Internet of Things will generate enormous amounts of data that are directly or indirectly linked to us, our mobile phones, homes and cars. But other major data sources are also increasingly made available online, with little constraint for wider use: population-, company- and land registers, statistical data on health, the environment, crimes or traffic incidents, and others. Many of these data sources will become "richer" - more detailed, and more personal - because of the Internet of Things.

Increasingly, governments wish to make these "rich data resources" available for socially beneficial uses, such as determining environmental factors that lead to lower crime rates, or discovering links between social factors and health. Researchers are naturally keen on them; and companies want to exploit them for commercial purposes. What is more, they all want to be able to combine, match and analyse these data, from all these sources. This accumulation of vast and complex information databases, and their exploitation, is referred to as "Big Data".

In theory, from these "big" resources, far-reaching inferences can be drawn, on which business and government decisions will increasingly come to rely. However, it is not easy to turn "Big but dumb" data into "Smart Data" (the new catchword). The data need to be cleverly "mined" in order to extract relevant, useful information and, especially, to discover "the hidden pattern, the unexpected correlation". Moreover, the logic used in the analyses - the profiling algorithm - is increasingly "improved" by the computer itself, using "artificial intelligence" - putting it increasingly outside the control not only of regulators, but of the organisations using it.

However, the capability of analysts to capture human behaviour in computer code or algorithms is not as infallible as often claimed. In practice, profiles and “human behaviour models” suffer from serious statistical limitations and often perpetuate social inequality and discrimination. Yet at the same time, because these algorithms are so “clever” and dynamic, they become utterly intransparent and consequently almost impossible to challenge.

This poses a fundamental threat to the most basic principles of the rule of law and the relationship between citizens and governments or between customers and businesses in a democratic society. We must become more aware of that threat, and counter it.

ENDitorial:
WHISTLEBLOWERS ARE HISTORY

Annie Machon

Annie Machon was an intelligence officer for the UK's MI5 in the 1990s, before leaving to help blow the whistle on the crimes and incompetence of the British spy agencies.

She is now a writer, media commentator, political campaigner, and international public speaker on a variety of related issues: the war on terrorism, the war on whistleblowers, the war on drugs, and the war on the internet. She is also the European director of LEAP and a founding board member of Code Red. Annie has an MA (Hons) Classics from Cambridge University.

From the perspective of 2025, as I sit at my keyboard drinking a whisky and writing my scurrilous memoirs, it seems strange that there was even a concept of "whistleblowers" - brave individuals who risked their jobs, their very way of life and even their freedom to shine light in the dark corners of corporate crimes and government lies.

Yet even as recently as a decade ago, in the world of intelligence, where secrecy was paramount, where crimes could be hushed up, and where there was no avenue for voicing concern and dissent, it was perhaps inevitable that whistleblowers such as Senator Edward Snowden continued to take such risks.

Until recently, whistleblowers had a bad rap in the media, deemed to be traitors, grasses or snitches. However, rather than a phenomenon to be feared, if handled correctly the concept of whistleblowing gradually came to be seem as beneficial to organisations.

This progress fills me with pride, as I have a nodding acquaintance with the process. In the 1990s, I worked as an intelligence officer for the UK domestic Security Service, generally known as MI5, before resigning to help my former partner and colleague David Shayler blow the whistle on a catalogue of incompetence and crime. As a result, we had to go on the run around Europe, lived in hiding and exile in France for three years, and saw our friends, family and journalists arrested around us. I was also arrested, although never charged, and David went to prison twice for exposing the crimes of the spies. It was a heavy price to pay.

However, it could all have been so different if the UK government had agreed to take his evidence at the time of spy crimes, undertaken to investigate them thoroughly, and implemented the necessary reforms. This would have saved us a lot of heartache, and could potentially have improved the work of the spies. But the government's instinctive response then was always to protect the spies and prosecute the whistleblower, while the mistakes and crimes go uninvestigated and unresolved. Or even, it often appeared then, to reward the malefactors with promotions and awards.

The draconian Official Secrets Act (1989) imposed a blanket ban on any disclosure whatsoever. As a result, we the citizens had to take it on trust that our spies worked with integrity. There was no meaningful oversight and no accountability.

Many good people did indeed sign up to MI5, MI6 and the Government Communications Headquarters (GCHQ), as they wanted a job that could make a difference and potentially save lives. However, once on the inside they were told to keep quiet about any ethical concerns: "don't rock the boat, and just follow orders".

In such an environment there was no means of raising concerns, no accountability and no staff federation. This inevitably led to a general consensus – a bullying "group think" mentality. This in turn led to mistakes being covered up rather than lessons learned, and then potentially down a dangerous moral slide.

As a result, after 9/11 we saw scandal heaped upon intelligence scandal, as the spies allowed their fake and politicised information to be used to make a false case for illegal wars across the Middle East; we saw them descend into a spiral of "extraordinary rendition" (ie kidnapping) and torture, for which they were successfully sued if not prosecuted; and we saw them facilitate dodgy deals in the desert with dictators.

But all was not bleak, even then. In 2013, Dr Tom Fingar received The Sam Adams Award for Integrity in Intelligence in Oxford for his work on compiling the US National Intelligence Estimate of 2007. In this he summarised the conclusions of all sixteen US intelligence agencies by saying that Iran had ceased trying to develop a nuclear weapons capability in 2003.

There was immense political pressure on him to suppress this evidence, but he went ahead with the report and thereby single-handedly halted the US government's rush to war with Iran in 2008. By having the courage to do his job with integrity, Dr Fingar was responsible for saving countless lives across Iran.

But in other sectors, mistakes were just as life threatening and the need for exposure just as great. At around the same time, in the UK, many senior medical whistleblowers were emerging from within the National Health Service (NHS), detailing mistakes and incompetence that put the public at risk. Alas, rather than learn from mistakes, all too often NHS bosses either victimised the whistleblowers by suspending them or ruining their reputations, or they insisted that they sign gagging orders and then covered up the mistakes. Neither option was a good outcome either for staff morale or for patient safety.

Similarly, during those years, we saw many whistleblowers emerge from the banking and finance sector. All too often, the whistleblowers were victimised but the banks carried on as normal until they crashed the global economy yet again.

While the culture of cover-up existed, so too did whistleblowers. However, after the Snowden disclosures and the flood of whistleblowers after him, lessons were learned.

Employers instituted cultures of trust and accountability, employees with concerns were fairly heard, the appropriate action taken, and justice done. As a result, the needs and imperatives behind whistleblowing disappeared. Potential problems were nipped in the bud, improving public trust and confidence in the probity of the organisation and avoiding all the bad publicity following a whistleblowing case.

Plus, of course, the potential whistleblowers had a legitimate avenue to go down, rather than having to turn their lives inside out – they no longer needed to jeopardise their professional reputation and all that went with it such as career, income, social standing and even, potentially their freedom.

Placing sound procedures in place to address staff concerns proved to be a win-win scenario – for staff efficiency and morale, the organisations' operational capability and reputation, and the wider public, too.

One could but dream, in 2015.

RECOMMENDED ACTION

Fight for your privacy!

Join the daily global privacy movement gatherings in front your local government buildings and corporate headquarters, and show the decision-makers that your privacy matters!

Say NO to neuro-compilers!

Answer to the public consultation by European Commission's B.R.A.I.N research project on the ethical implications of first generation neuro-compilers!

EDRi-gram is a fortnightly roundup of digital news, published by European Digital Rights (EDRi), a not-for-profit association of digital civil rights organisations from across Europe.

European Digital Rights
Rue Belliard 20, 1040 Brussels
https://edri.org
@edri
edrigram@edri.org
tel. +32 (0) 2 274 25 70