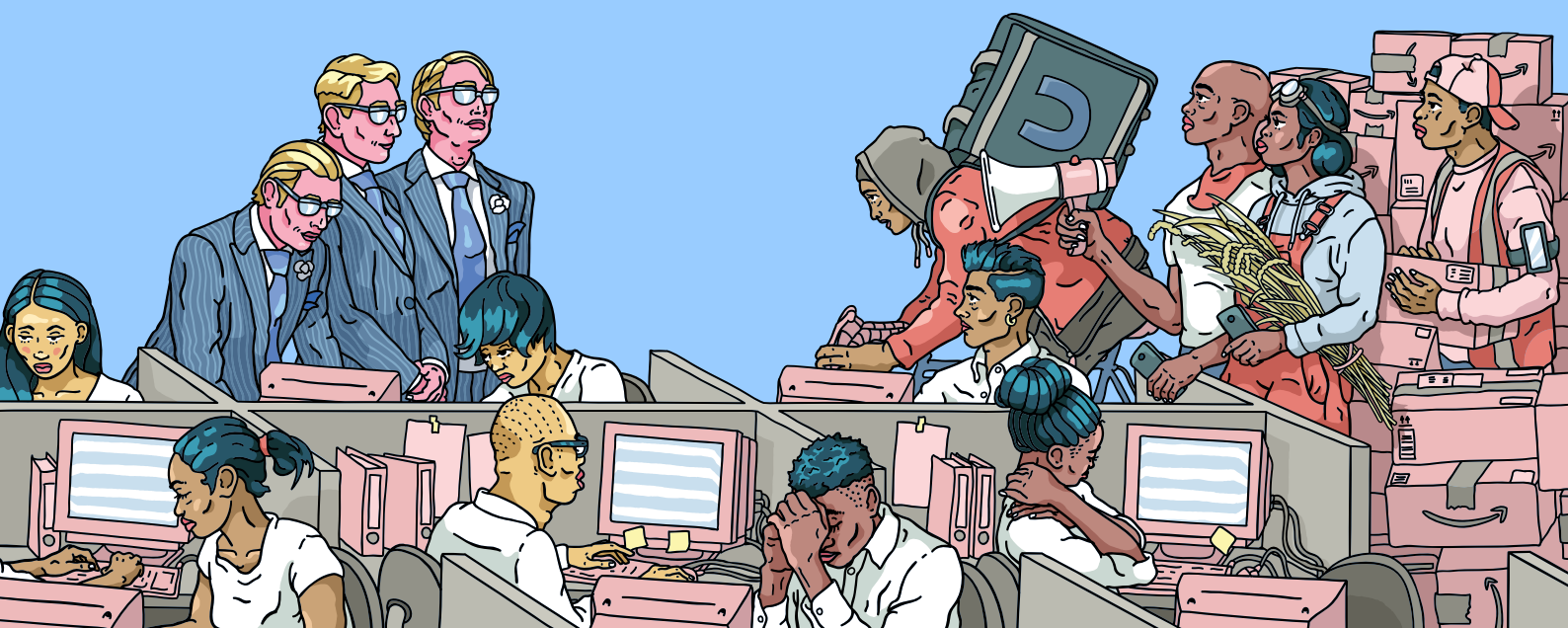
tni 50 years 1974 - 2024

WEEK 5

Digitalisation and the security state



1 Introduction: nothing new under the sun?

"STATE SURVEILLANCE IS AS OLD AS THE STATE,"[1] as are debates on how that surveillance should be regulated and controlled. In Britain, as soon as a postal service was introduced, authorities began opening correspondence between suspected subversives and radicals. In 1840 the service was made far cheaper – and thus more widely-used – and in 1844 a political scandal known as the postal espionage crisis unfolded when these spying powers became widely-known to the public.

The historian David Vincent has argued that this crisis "contained in embryo all the main features of the international controversy" that emerged following the disclosure of hundreds of top secret documents by former US National Security Agency contractor Edward Snowden, starting in June 2013.[2] From those disclosures, we now know that spy agencies in the United States, the United Kingdom and their allies have access to unfathomable quantities of data generated by individuals in the course of their everyday activities.

As Vincent has shown, there are a number of parallels between these two events. What is undoubtedly different, however, is the amount of data that digital technologies make it possible to collect, produce, store and transmit about their users. For corporations concerned with monitoring and interpreting peoples' behaviour in order to turn a profit, and for state agencies concerned with doing so in order to maintain control, the possibilities offered by digital technologies are vast.

Digitalisation is a massive boon to the security state, even if certain technologies and practices (in particular, end-to-end encryption[3]) have provoked ire and outrage from governments. This is increasingly the case with the trend towards "interoperability", through which different datasets can be compared, merged and used together by interlinking different databases and information-processing systems. Through this process, even data that may originally have been anonymous can be combined with other datasets to identify individuals. Indeed, studies have found that supposedly anonymous data can never truly be anonymous.[4]

Database dangers

One powerful historical example of the dangers of bureaucratic databases comes from the experience of German occupation in Norway compared to Finland. Over 50% of the 1,400 Jews in Norway in 1942 were exterminated, while the figure for Denmark was under 1% out of 5,600 (and under 0.5 % out of 2,300 for Finland). Why the much higher percentage for Norway? There are several reasons, one of them being that Norway had excellent registers pertaining specifically to Jews.

Thomas Mathieson argues that today 'The new, technically extremely innovative, combinable, hidden and cross-border uncontrollable data-based registration systems which are presently rushing forward, constitute an increased, enormous threat which cannot be ignored by anyone preoccupied with police and political control after 2000.'[5]

Despite the benefits that digitalisation provides to powerful institutions, its benefits for ordinary people are also extensive. The ease with which they allow communication between people has made it possible for new protest and resistance movements to emerge and coordinate against unjust laws, policies and practices. The increasing available of digital information facilitates the work of investigators, researchers and analysts seeking to uncover crimes of the powerful. While offering enormous potential new powers to states and corporations, digitalisation also offers new possibilities for resistance.

2 Digitalisation and the security state

To begin with, it is worth outlining what is meant here by the terms **"DIGITALISATION"** and **"SECURITY STATE"**.

We consider digitalisation to be a process by which activities and information that were not previously recorded in any durable way, or which were stored on analog storage media (paper, tapes, microfilm, etc.), come to be recorded on digital media.

Digitalisation is, in short, the process by which digital data and/or information is produced. Examples include the recording of individuals' music preferences and listening habits by online streaming platforms; the generation of long-term records of whom an individual has conversations with and when those conversations take place, via apps such as Whatsapp and Signal; or logs of an individuals' location and everyday habits through the logging of Global Position Satellite (GPS) data created by smartphone users.

What this means is well summed-up by a paper produced by the Portuguese Presidency of the Council of the EU some 15 years ago:

> ***"Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations, and create huge opportunities for more effective and productive public security efforts."***[6]

As for the security state, it serves here as convenient shorthand for those agencies, institutions, bodies – whether public or private – that have a role in facilitating or implementing laws and policies of repression or control. The security state is not necessarily a fixed entity or set of entities (for example, the companies contracted by the state to power a particular function may change over time), but rather an amalgamation or 'assemblage' of entities used to carry out functions concerned with surveillance and control of the population (or, at least, those elements of the population deemed troublesome, subversive, or disorderly). In this regard, it encompasses institutions such as the police or border agencies but can also include schools, doctors, landlords and employers, as exemplified by the UK's "Prevent" counter-terrorism scheme[7] and "hostile environment" for undocumented migrants.[8]

In the context of digitalisation, it is vital to consider the security state as encompassing both public and private entities. As a declassified report by the Senior Advisory Group to the US Office of the Director of National Intelligence noted:

> ***"The government would never have been permitted to compel billions of people to carry location tracking devices on their persons at all times, to log and track most of their social interactions, or to keep flawless records of all their reading habits. Yet smartphones, connected cars, web tracking technologies, the Internet of Things, and other innovations have had this effect without government participation. While the IC [intelligence community] cannot willingly blind itself to this information, it must appreciate how unfettered access to CAI [commercially-available information] increases its power in ways that may exceed our constitutional traditions or other societal expectations."***[9]

Ultimately, what digitalisation means for the security state is a vast increase in the potential for surveillance and data collection, and thus a vast increase in the potential control that can be exercised over the population. It is vital to note, however, that it is by no means certain that this potential will be realised: governments may choose not to pursue certain possibilities, they may not have the resources to do so, or they may face fierce enough opposition to surveillance powers that they are forced not to exercise them. Before turning to look at how the digitalisation of the security state can affect the rights of individuals and groups, we will consider some of the basic principles underpinning state surveillance and data collection powers.

3 State surveillance and data collection: basic principles

In theory – and, in particular, in liberal democratic political and legal theory – any measure through which the authorities are empowered to collect information on individuals must meet a number of basic principles.

First of all, those measures should be governed by the law – yet many surveillance or data collection measures are put in place despite being illegal. In the latter category are examples such as the mass surveillance of telecommunications traffic conducted by the UK's signals intelligence agency, Government Communications Headquarters (GCHQ);[10] the creation of a file known as the 'Gangs Matrix' by the Metropolitan Police, found to be racist by a regulatory body;[11] the French police's use of facial recognition software;[12] or the Russian authorities' use of facial recognition software to track down peaceful protesters.[13]

It is noteworthy that in each of these cases, new surveillance and data-gathering measures were introduced in secret. Meaningful, public, democratic debate about the measures; evaluations of how they operate, their effectiveness and whether they meet their objectives; and mechanisms of independent oversight and control (for example, authorisation by courts and review by supervisory bodies) may all help to avoid the introduction of invasive, abuse and illegal practices, and to ensure that surveillance powers are kept under control.

However, new surveillance or data collection measures should not be introduced simply because governments decide to do so. Within the type of human rights framework set out in international law, the authorities have to **demonstrate that those measures are necessary** – as, undoubtedly, some of them are. Few people would argue that it is illegitimate for there to be video surveillance installed around critical infrastructure such as power stations, for example.

In Europe, there is substantial jurisprudence on this question in both national courts, as well as supranational tribunals such as the Court of Justice of the European Union and the European Court of Human Rights. As explained by the European Data Protection Supervisor, the EU's independent data protection authority:

> ***"Necessity shall be justified on the basis of objective evidence and is the first step before assessing the proportionality of the limitation. Necessity is also fundamental when assessing the lawfulness of the processing of personal data. The processing operations, the categories of data processed and the duration the data are kept shall be necessary for the purpose of the processing."***[14]

Of course, governments frequently claim that a measure is necessary without providing any meaningful evidence that this is the case. Once again, it is vital that the public, experts, and civil society organisations are able to intervene in debates on these issues in order to demand genuine demonstrations of and evidence for the necessity of a particular measure.

If a measure can be classified as necessary, the authorities should also demonstrate that it is proportionate. Put another way, they must demonstrate that the limitations they wish to impose on any particular right are justified. To quote the European Data Protection Supervisor again:

> ***"...proportionality requires that advantages due to limiting the right are not outweighed by the disadvantages to exercise the right... Safeguards accompanying a measure can support the justification of a measure. A pre-condition is that the measure is adequate to achieve the envisaged objective. In addition, when assessing the processing of personal data, proportionality requires that only that personal data which is adequate and relevant for the purposes of the processing is collected and processed."*** [15]

This framework – of legality, necessity and proportionality – clearly has advantages over systems in which the authorities simply do as they wish, with no meaningful oversight, control or restrictions on their activities. However, it also has limits. For example, it makes it possible to argue that in a world where so much data is available, it is necessary and proportionate for authorities to have access to it for security purposes. This leaves little room for principled political or moral disagreements with surveillance and data collection measures.

4 Digitalisation and the security state: potential rights violations

a) Freedom from discrimination

Digital technologies can be used to gather and share information on peoples' nationality, ethnicity, religion, politics views, or gender (or other personal characteristics or beliefs) far more quickly and easily than was ever possible with paper-based data collection methods. This is particularly true with the advent of "computer vision" technologies, which can be trained to recognise, record and track people and objects. Historic practices of discrimination and exclusion can thus be turbo-charged by digital technologies, further amplifying imbalances of power between powerful institutions and ordinary people.

Facial recognition technology is perhaps the best-known form of computer vision technology, but the same types of system could also be plugged into a city's CCTV to make it possible to track the movements of people wearing a certain type of clothing, or carrying particular placards or banners. In recent years there have been huge political and legal disputes over the legitimacy of the use of facial recognition technology – in particular by the police – and steps have been taken by governments to regulate it.

The most notable example so far has come in the European Union, with the Artificial Intelligence Act – but despite the best efforts of human rights campaigners and some parliamentarians, governments have managed to include in the law significant exemptions for law enforcement and national security use of the technology.[16]

It is by now well-known that many facial recognition algorithms fail to recognise non-white people and women at the same rate as they do white people and men, due to them being trained on discriminatory data sets – for example, images primarily of white men. Politicians, experts and civil society groups have made numerous calls for these flaws to be fixed, which is entirely justified. However, there is a risk that in calling for improvements in the accuracy of such technologies, their usage can be more easily-justified by governments.

b) Freedom of thought and opinion

Digital platforms – for example, Facebook or X – can be used to mine data on individuals and groups and then used for profiling and targeting. This is how the business model of many online platforms works: users' behaviours and interactions are mapped and recorded, then sold on to advertising companies and data brokers.[17]

The use of your online habits to try to sell you shoes may seem relatively innocuous, but what if those habits were used instead to feed you political propaganda? The practice of online political micro-targeting is by now well-established, raising concerns due to the ways in which 'it could be used to increase polarization of the electorate, and identify and target weak points where groups and individuals are most vulnerable to strategic influence, amongst others.'[18]

In western states, many politicians have accused Russian intelligence agencies of engaging in such practices in a bid to undermine liberal democracies – a claim that is no doubt true, but also conveniently distracts from the political failings of those liberal democracies over the last 40 years as inequality has soared and public services have been increasingly privatised. And, of course, interference in other states' elections is by no means limited to the world's more authoritarian states, as the history of the CIA amply demonstrates.[19]

Whoever is behind it, the use of online platforms to feed the public with political propaganda is intended to sway peoples' thoughts and opinions in one direction or another. This is, of course, the point of all political advertising: but where the source of the information is unclear or unknown, it becomes impossible for the audience to critically evaluate it. There is thus a crucial need for strict, enforceable rules on the transparency of online advertising of all forms, as well as strict rules on how peoples' online behaviour can be stored, sold and used to track and profile them.

c) Freedom of association and freedom of expression

It is well established that surveillance measures can have a "chilling effect" upon the exercise of individual rights, discouraging people from expressing their opinions, attending protests, or joining a trade union (amongst other things) if they know that their presence is likely to be put on record by the authorities, or if they are likely to face other unpleasant consequences.[20] The digitalisation of the security state can extensively amplify this effect, at the same time as bolstering the powers of the authorities to monitor and track dissidents.

For example, in relation to protest, digital technologies make it possible to record, track and log everyone in attendance, and then to track their attendance at other protests in the future.[21] That, in turn, makes it possible to develop a profile of an individual's political preferences and beliefs, as well as the people they associate with. Police may then seek to target those on whom they have information, for example to "discourage" them from attending protests, arrest people pre-emptively,[22] or to encourage them to act as informants.[23] At the same time, digital technologies also facilitate the sharing of information by informants on their targets – as the case of the UK's best-known "spycop", Mark Kennedy, makes clear.[24]

This problem is further amplified by the popularity of social media platforms such as Facebook and X, where the views freely expressing by people can be hoovered up the authorities and used to profile them. The information gathered by the police that is generated through the use of social media platforms has been termed SOCMINT, or social media intelligence (akin to OSINT, open source intelligence; or HUMINT, human intelligence).[25] Many activists who came of age prior to the advent of social media have sought to discourage the practice of organising protests through platforms such as Facebook, as doing so can automatically provide the police with a list of who is interested in attending, though the ease with which such platforms can be used to reach large numbers of interested people interested means their calls have often fallen on deaf ears.

This problem is not limited to engagement in protests. For example, in early 2021 in France, the government approved three decrees that allow the state to gather data on the political opinions, trade union activities and religious beliefs of people who could "harm the integrity of the territory or institutions of the Republic", a vague term that expands the scope of police files far beyond what was previously permitted.[26] In the UK, collusion between companies and state agencies in a practice known as "blacklisting" saw hundreds of trade union activists illegally barred from working in the construction industry in a bid to prevent the organisation and mobilisation of workers against poor pay and working conditions.[27]

d) Freedom of movement

Digital surveillance technologies are increasingly central to the regulation and control of international migration. States have amassed vast databanks of biographic and biometric data on visa applicants, tourists, business travellers and others, and are actively seeking to expand the information they collect and how they use it – for example, by using predictive algorithms to determine the level of "threat" posed by an individual, to determine if they warrant further searching or questioning by border officials.[28] Through the use of new data collection and processing technologies, states (with the assistance of corporations) aim to make regular migration swifter and more convenient – albeit at the price of travellers handing over increasing amounts of personal data to the authorities. Digital technologies and communication networks also make it possible to extend state borders far beyond a country's physical boundaries – many states require "pre-checks" of air passengers before they depart, in order to determine if they have permission to travel or not.[29]

However, many people are forced to cross borders in an "irregular" manner, and they too are subject to an increasing array of digitised surveillance measures. The world's most technologically advanced states – in particular, European nations and the USA – employ drones, radar, satellites, blimps, planes and helicopters and a wide array of other sensors and tracking technologies to detect and monitor people travelling to, or attempting to cross, their borders.[30] While self-evidently denying peoples' right to freedom of movement across the globe, this also impinges upon the right to seek asylum. By preventing people from accessing their territory, wealthy states make it impossible for people to lodge a claim for international protection. The use of digital surveillance and data-gathering technologies is intimately linked to the effort to limit the number of refugees able to enter the world's richer states.

Even when refugees are able to enter the territories of those states, digital technologies will be used to register and track their claims, and even to aid in their assessment. The authorities in a number of states have used systems for extracting vast quantities of data from mobile phones to try to check the veracity of peoples' claims about their country of origin or their journeys; while in Germany the authorities were using automated dialect analysis tools to try to determine peoples' country of origin. An extensive report by the University of Oxford found digital technologies being used for border surveillance; immigration forecasting; processing of residency and citizenship applications; document verification; risk assessment; speech recognition; distribution of benefits; matching tools; mobile phone data extraction; and electronic monitoring of asylum applicants.[31]

The use of digital technologies to restrict freedom of movement does not only apply to the crossing of state borders. During the COVID-19 pandemic, many states introduced contact tracing apps that were used to determine whether or not an individual or an area posed a risk of infection and to permit or deny people the right to leave their homes or enter a particular place or area. Many of these apps were designed by big tech companies – for example, Google – in collaboration with state authorities, providing a clear example of how the data that is gathered and processed by companies can be used by governments for surveillance and tracking of the population.

e) Privacy and data protection

Any surveillance or data collection is an infringement of privacy. To be justified, they must be legitimate, necessary and proportionate, and subject to the requisite checks and balance – for example, independent authorisation by a judge or other independent authority, and be subject to independent monitoring and review. Data processing systems and technologies should also be designed with privacy in mind, a principle often referred to as "privacy by design".

Whenever a breach of the right to privacy is justified, the institutions processing data must then respect rules on data protection. For example, the EU's General Data Protection Regulation requires compliance with a number of basic principles:

- Lawfulness, fairness and transparency
- Purpose limitation: data should only be used for the purpose for which they were collected
- Data minimisation: only the minimum amount of data necessary should be processed
- Data accuracy: data must be accurate
- Storage limitation: data should only be stored for a specified time and afterwards deleted or, at least, made anonymous
- Integrity and confidentiality: data must be stored securely, there should be controls on who is authorised to access it, and it should be kept confidential
- Accountability: those who process the data must be accountable for the ways in which they process it, for example by data-processing institutions keeping records to demonstrate compliance with the rules.

f) Right to an effective remedy

If an individual's data is misused by an authority that stores or processes it, the data subject (the individual on whom data is processed) must have access to an effective remedy allowing them to challenges that misuse. This generally requires recourse to an independent administrative and/or judicial mechanism that allows them to challenge that misuse and have data corrected or deleted if deemed necessary. The use of new technologies such as predictive algorithms, machine learning, "artificial intelligence" can pose challenges to the right to an effective remedy due to problems with determining how or why a decision or assessment has been made. For example, it must be possible for the authorities to show how an algorithm used by the authorities to determine whether or not an individual poses a security threat has come to that decision. This requires mechanisms built into the design of data processing systems that make it possible to trace and explain the decision-making or assessment process so that it can be meaningfully reviewed by humans.

5 Challenges, victories and successes

There have been a huge number of important victories against attempts by states and corporations to wield more power over individuals and society through digital technologies.

Court cases in Europe have set limits on states' ability to retain biometric data on individuals,[32] to retain information on peoples' use of the internet and telephones,[33] and on the tracking and surveillance of air travel.[34] Protest movements have halted the widespread use of facial recognition surveillance (notably in Belgrade[35]), the introduction of identity cards for the entire population (in the UK[36]), and the installation of extensive networks of CCTV cameras (in Greece[37]). Regulatory bodies have halted or limited the use of facial recognition cameras in public (in Italy[38]), the scraping of photos from the internet to power facial recognition software, and against the gathering of data from migrants and refugees to feed police databases (in Spain[39]).

Alternative digital technologies are also widely-used by individuals and organisations to protect their privacy and shield themselves from surveillance. Messaging apps such as Signal, email encryption through PGP, browsers such as Tor, and a multitude of other tools and apps have been developed that do not gather the swathes of personal data that are used by corporations and the state to profile and track individuals. Designers have even proposed forms of anti-surveillance clothing[40] and makeup.[41] These technologies and tactics provide huge benefits to journalists, lawyers, medical professionals, protest groups and campaigners. However, they often come under attack from the authorities and are still only used by a minority of the population. Often, the difficult of using them makes them unattractive to individuals, and legal changes to restrict the powers of states and corporations remains necessary to prevent the realisation of the intensive surveillance made possible by the digitalisation of the security state.

NOTES

1 https://www.statewatch.org/media/documents/analyses/no-244-gchq-intercept-commissioner.pdf

2 https://www.historyandpolicy.org/policy-papers/papers/surveillance-privacy-and-history

3 See, in particular, the ongoing debate over government attempts to access encrypted material in the name of dealing with child sexual abuse material, for example in the EU: https://edri.org/our-work/is-surveilling-children-really-protecting-them-our-concerns-on-the-interim-csam-regulation/

4 https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds

5 https://www.statewatch.org/media/documents/analyses/no-163-globalisation-of-control-1999.pdf

6 Tony Bunyan, 'The Shape of Things to Come: the EU Future Group', Statewatch, September 2008, p.34, https://www.statewatch.org/media/documents/analyses/the-shape-of-things-to-come.pdf

7

8

9 Office of the Director of National Intelligence Senior Advisory Group Panel on Commercially Available Information, 'Report to the Director of National Intelligence', January 2022, p.13, https://www.odni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf

10 https://www.amnesty.org/en/latest/news/2021/05/uk-surveillance-gchq-ecthr-ruling-2/

11 https://www.theguardian.com/uk-news/2018/nov/16/met-police-gang-matrix-breached-data-laws-investigation-finds

12 https://disclose.ngo/en/article/the-french-national-police-is-unlawfully-using-an-israeli-facial-recognition-software

13 https://hudoc.echr.coe.int/app/conversion/pdf/?library=ECHR&id=003-7694109-10618091&filename=Judgment%20Glukhin%20v.%20Russia%20-%20use%20of%20facial-recognition%20technology%20against%20Moscow%20underground%20protestor.pdf

14 https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

15 https://edps.europa.eu/data-protection/our-work/subjects/necessity-proportionality_en

16 https://edri.org/our-work/eu-ai-act-deal-reached-but-too-soon-to-celebrate/

17 https://privacyinternational.org/long-read/2433/i-asked-online-tracking-company-all-my-data-and-heres-what-i-found

18 https://academic.oup.com/idpl/article/11/4/348/6355314?login=false

19 https://www.wnyc.org/story/history-us-intervention-foreign-elections/

20 https://www.opensocietyfoundations.org/uploads/c8c58ad3-fd6e-4b2d-99fa-d8864355b638/the-concept-of-chilling-effect-20210322.pdf

21 https://phm.org.uk/blogposts/dangers-of-technological-surveillance-in-policing-public-protests/

22 https://www.statewatch.org/statewatch-database/uk-arrests-raids-and-wedding-parades-by-chris-jones/

23 https://www.theguardian.com/uk/2009/apr/24/strathclyde-police-plane-stupid-recruit-spy

24 Kennedy, a police officer, infiltrated the UK and European environmental direction action movement for years, and was provided with a digital watch that allowed him to record and transmit conversations to his superiors.

25 https://www.tandfonline.com/doi/full/10.1080/02684527.2012.716965

26 https://www.statewatch.org/news/2021/january/france-green-light-for-police-surveillance-of-political-opinions-trade-union-membership-and-religious-beliefs/

27 https://www.thecanary.co/uk/analysis/2023/02/15/governments-and-police-colluded-with-private-agencies-to-blacklist-activists-report-confirms/

28 https://www.statewatch.org/automated-suspicion-the-eu-s-new-travel-surveillance-initiatives/

29 https://www.statewatch.org/analyses/2021/uk-nationality-and-borders-bill-biometric-permission-to-travel-scheme-will-affect-tens-of-millions-of-people/

30 https://www.statewatch.org/publications/reports-and-books/europe-s-techno-borders/

31 https://www.rsc.ox.ac.uk/publications/automating-immigration-and-asylum-the-uses-of-new-technologies-in-migration-and-asylum-governance-in-europe/@@download/file

32 https://hudoc.echr.coe.int/eng?i=001-90051

33 https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

34 https://edpb.europa.eu/our-work-tools/our-documents/statements/statement-implications-cjeu-judgment-c-81719-use-pnr-member_en

35 https://edri.org/our-work/serbia-unlawful-facial-recognition-video-surveillance-in-belgrade/

36 https://www.gov.uk/government/news/identity-cards-are-to-be-scrapped

37 https://www.researchgate.net/publication/280574976_The_Super-Panopticon_Scandal_of_the_Athens_2004_Olympics_and_its_Legacy

38 https://www.statewatch.org/news/2021/april/italy-interior-ministry-s-facial-recognition-system-is-unlawful/

39 https://elpais.com/espana/2023-09-26/el-defensor-del-pueblo-cuestiona-a-frontex-por-sus-interrogatorios-a-los-migrantes-recien-llegados-en-patera.html

40 https://adam.harvey.studio/stealth-wear/

41 https://adam.harvey.studio/cvdazzle

The Transnational Institute (TNI) is an international research and advocacy institute committed to building a just, democratic and sustainable planet. For nearly 50 years, TNI has served as a unique nexus between social movements, engaged scholars and policy makers.

www.TNI.org

CO-SPONSORED BY:

SOMO

IT for Change

statewatch

DigitalCapitalismCourse.tni.org