GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Association for Progressive Communications (APC),
Article 19, and Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch

2019

Global Information Society Watch 2019
Artificial intelligence: Human rights, social justice and development

Operational team
Valeria Betancourt (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Maja Romano (APC)

Project coordination team
Valeria Betancourt (APC)
Cathy Chen (APC)
Flavia Fascendini (APC)
Alan Finlay (APC)
Mallory Knodel (ARTICLE 19)
Vidushi Marda (ARTICLE 19)
Leila Nachawati (APC)
Lori Nordstrom (APC)
Maja Romano (APC)

GISWatch 2019 advisory committee
Namita Aavriti (APC)
Rasha Abdul Rahim (Amnesty International)
Alex Comninos (Research ICT Africa)
Malavika Jayaram (Digital Asia Hub)
J. Carlos Lara (Derechos Digitales - América Latina)
Joy Liddicoat (Centre for Law and Emerging Technologies, University of Otago)
Andrew Lowenthal (EngageMedia)
Micaela Mantegna (Geekylegal/Machine Intelligence Lab, Center for Technology and Society, San Andres University)
Valeria Milanes (Asociación por los Derechos Civiles)

Project coordinator
Maja Romano (APC)

Editor
Alan Finlay (APC)

Assistant editor and proofreading
Lori Nordstrom (APC)

Publication production support
Cathy Chen (APC)

Graphic design
Monocromo

Cover illustration
Matías Bervejillo

We would like to extend a special note of thanks to a number of authors who have made ad honorem contributions to this edition of GISWatch.
We gratefully acknowledge the following:

Philip Dawson and Grace Abuhamad (Element AI)
Anita Gurumurthy and Nandini Chami (IT for Change)
Rasha Abdul Rahim (Amnesty International)

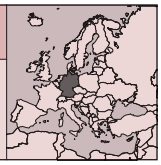
APC would like to thank the Swedish International Development Cooperation Agency (Sida) and ARTICLE 19
for their support for Global Information Society Watch 2019.

Published by APC
2019
Printed in USA

Global Information Society Watch 2019 web and e-book
ISBN 978-92-95113-13-8
APC Serial: APC-201910-CIPP-R-EN-DIGITAL-302

GERMANY

BIOMETRICS AND BODY POLITIK: THE RISE OF AUTOMATED SURVEILLANCE IN GERMANY



Centre for the Internet and Human Rights (CIHR), European University Viadrina
Mathana Stender
https://twitter.com/StenderWorld

Machine-readable humans

As technology has made our lives easier, it has also numbed us to the potential threats that can be posed by new forms of "convenience". Putting one's iPhone in front of your face to unlock it with FaceID, instead of entering a short string of numbers, is an alluring prospect for some, but the impact of the development and proliferation of human-sensing technologies has broad societal repercussions, particularly for society's most vulnerable.

We are subjected to distributed-yet-persistent digital surveillance, where sensors that are able to discern minute details from our bodies have been installed all around us. Because no two sets of fingerprints or irises or voices are exactly the same, each human body contains physical identifiers that are unique to the individual. Using computer vision technology combined with algorithmic decision making, biometric identity management and access control systems capture and analyse our permanent, immutable characteristics, and are being increasingly used for automated surveillance.[1] These systems, while claiming to differentiate, classify and categorise people, are however flawed due to biased data and technical limitations. Though constrained by various limitations, the systems have become increasingly adopted by both companies and governments to streamline surveillance.

With biased assumptions built into training of models, and flawed labelling of training data sets,[2] this class of technologies often do not differentiate between who is surveilled; anyone who passes through their sensor arrays are potential subjects for discrimination.

Surveillance does not happen in a vacuum. The use of biometric and automated access control mechanisms is increasing globally at an alarmingly high rate: India's compulsory Aadhaar biometric ID system has records from well over a billion individuals, while 23 million people were blocked from travelling in China last year due to their low social credit scores.[3] Biometric access has now become a gatekeeper to both basic services and the freedom of movement.

Automated facial recognition in action

Biometric surveillance and access control involves the computational analysis of parts of a person's physical attributes – fingerprints, facial features, retina or voice. In order for a system to recognise one's immutable characteristics, they must compare input against a database to identify key features. When the result of a facial feature map leads to a particular conclusion about the subject being surveilled, which is dynamically generated by an algorithm, this is known as "automated facial recognition" (AFR).

Sometimes this AFR takes the form of verification: is a person who they say they are (or, more accurately, do the physical characteristics being "scanned" by a system match the system's records for this person)? In other cases, however, biometrics are used to analyse or extrapolate an aspect of a person's identity. An automated biometric system might be looking to see if a person is a child or adult, or seek to classify one's ethnicity and age. Other, more invasive forms of AFR might be assessing someone's sexual orientation,[4] or assigning a score pertaining to the likelihood that they will commit a crime.[5]

Over the past few years, both the German government and the European Union (EU) have turned

1 Ohrvik-Stott, J., & Miller, C. (2019). *Responsible Facial Recognition Technologies*. Doteveryone. https://doteveryone.org.uk/wp-content/uploads/2019/06/Doteveryone-Perspective_Facial-Recognition-1.pdf

2 "Many companies report high accuracies using a data set called Labeled Faces in the Wild, but this data set only contains 5,171 people. Most large cities are in the millions. What works for 5,000 doesn't necessarily work for 5 million." Interview with AFR researcher Adam Harvey, 11 June 2019.

3 Kou, L. (2019, 1 March). China bans 23m from buying travel tickets as part of 'social credit' system. *The Guardian*. https://www.theguardian.com/world/2019/mar/01/china-bans-23m-discredited-citizens-from-buying-travel-tickets-social-credit-system

4 Gutierrez, C. (2019, 29 June). Unregulated facial recognition technology presents unique risks for the LGBTQ+ community. *TechCruch*. https://techcrunch.com/2019/06/29/unregulated-facial-recognition-technology-presents-unique-risks-for-the-lgbtq-community

5 Du, L., & Maki, A. (2019, 24 March). These Cameras Can Spot Shoplifters Even Before They Steal. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-03-04/the-ai-cameras-that-can-spot-shoplifters-even-before-they-steal

to biometric systems as they deal with a humanitarian crisis. Political instability brought about by the Syrian civil war and the rise of ISIS threatened the lives of millions of people, triggering one of the largest mass migrations of externally displaced persons in the 21st century. As millions of people fled war-torn lands, Europe witnessed a massive influx of refugees and asylum seekers. In 2015, the German government granted asylum to one million refugees,[6] a decision that would further galvanise xenophobia through political propaganda, and, within two years, propel a far-right political party into a strong position of political power.[7] The government's response to the crisis was to create a new biometric identity system for refugees, a system that was eventually integrated into a new EU-wide biometric identity management surveillance system that went far beyond its original intent. By 2019, biometric surveillance and algorithmic policing had become normalised to the extent that members of the European Parliament (MEPs) voted in favour of the creation of a biometric database that would centralise law enforcement, immigration and other information on over 350 million people.

Surveillance-as-a-service: Bodies and borders

Biometric sensors often use new algorithmic processes to leverage existing infrastructure. In Germany, where there are 6,000 CCTV cameras[8] scattered throughout the country's roughly 900 train and metro stations alone, existing capacity for a widespread surveillance network is already in place. Unlike in the past, however, when there were not enough humans to watch all the recorded video, meaning that much footage was seen only in cases where evidence of crime was needed, recent advancements in computer-vision AI can now "watch" CCTV footage in real time and automatically notify authorities when something "suspicious" has occurred.[9]

Sometimes, seemingly benign uses of new technologies can show how ill conceived technology implementation can be. Algorithmic-driven biometric systems are inherently problematic not only because there is so much cultural and ethnic diversity in humanity, but also because, in a day and age where characteristics like gender are fluid, such systems may be built on data sets that are developed using binary parameters and rudimentary perceptions of performativity-based gender analysis.

Prevailing winds

The origins of Germany's biometric identity registries coincided with the large uptick in refugees and asylum seekers into Germany and the EU in 2013[10] that had been triggered by the war in Syria and other instability. An EU system centralised the identity of those seeking asylum in the EU along with their fingerprints into a unified database called the Eurodac system. The system, and its Automated Fingerprint Identification System (AFIS), were created to facilitate the "Dublin Regulation", which stipulated that refugees apply for protection in (and only in) the first European country that they arrive at. All asylum seekers, regardless of the location of their asylum claim, would now also have their fingerprints and photos aggregated in the Eurodac.[11]

While EU legislation was rolling out its biometric registry for refugees, Germany was developing its own plans. In December 2015, the German cabinet approved a measure establishing the creation of identity cards for refugees.[12] Former German Interior Minister Thomas De Maiziere, who oversaw the issuance of the new identity card, was a proponent of a form of social engineering. He alarmed advocates when he spoke about the need for "Leitkultur", the idea of instilling dominant (German) cultural values in refugee seekers.[13]

The implementation of biometrics would soon reach German citizens. Documents revealed by the German media in 2016 showed a draft plan by the Interior Ministry to deploy AFR in areas ranging

6 Werber, C. (2015, 26 August). Germany is the first European country to free Syrian refugees from a draconian bureaucratic "trap". *Quartz*. https://qz.com/488413/germany-is-the-first-european-country-to-free-syrian-refugees-from-a-draconian-bureaucratic-trap

7 Clarke, C. (2017, 25 September). German elections 2017: Full results. *The Guardian*. https://www.theguardian.com/world/ng-interactive/2017/sep/24/german-elections-2017-latest-results-live-merkel-bundestag-afd

8 Global Rail News. (2017, 2 August). Facial recognition technology to be trialled at Berlin railway station. *Global Rail News*. www.globalrailnews.com/2017/08/02/facial-recognition-technology-to-be-trialled-at-berlin-railway-station

9 Glaser, A. (2019, 24 June). Humans Can't Watch All the Surveillance Cameras Out There, So Computers Are. *Slate*. https://slate.com/technology/2019/06/video-surveillance-analytics-software-artificial-intelligence-dangerous.html

10 OECD. (2015, 22 September). Comprehensive and co-ordinated international response needed to tackle refugee crisis. https://www.oecd.org/migration/comprehensive-and-co-ordinated-international-response-needed-to-tackle-refugee-crisis.htm

11 https://ec.europa.eu/home-affairs/what-we-do/policies/asylum/examination-of-applicants_en

12 Copley, C. (2015, 9 December). German cabinet approves identity card for refugees. *Reuters*. https://www.reuters.com/article/us-europe-migrants-germany-idUSKBN0TS1K620151209#ODikvJ2zgKwilx4w.97

13 DW. (2017, 30 April). German interior minister speaks out in favor of 'Leitkultur' for immigrants. *DW*. https://www.dw.com/en/german-interior-minister-speaks-out-in-favor-of-leitkultur-for-immigrants/a-38643836

from shopping malls to train stations and airports.[14] The plan received some push-back at the time from opposition parties and the media. In June the following year, a resolution from the Conference of Independent Data Protection Authorities of Federal and State Governments (DSK) stated the threat to society posed by AFR technology in no uncertain terms: the "use of video cameras with biometric facial recognition can completely destroy the freedom to remain anonymous in public spaces. It's practically impossible to evade this kind of surveillance, let alone to control it."[15] Despite such a warning, the technology was not put on hold.

One high-profile case from 2017 that shocked the nation saw a German army officer publicly named Franco A. charged with a terror-related plot to assassinate German officials all the while posing as a Syrian refugee (the charges were later dropped for lack of evidence).[16] Prosecutors disclosed that the man was looking to frame refugees in a "false flag" attack and thus further degrade public opinion toward asylum seekers.[17] Because the army officer and would-be terrorist had been able to enrol for asylum seeker services posing as a Syrian, the government decided that biometrics could prevent a repeat of the incident. Yet another biometric regime was implemented for refugees and asylum seekers, as the government proclaimed "no more Franco A.s".[18] This system saw the roll-out of speech analysis, which the government claimed could analyse linguistic dialects to verify a place of origin.[19]

In 2017, an AFR pilot project deployed by the Interior Ministry, German federal police departments and Germany's Deutsche Bahn rail company[20] was introduced into one of the capital's sprawling metro systems. Known as Safety Station Südkreuz, the programme enrolled 300 individuals who volunteered to have their faces used to help train the system in exchange for a EUR 25 Amazon voucher.[21].

In other parts of Germany, individual states have implemented their own AFR schemes. Section 59 of a 2019 Saxon police law, titled "Use of Technical Means in Order to Prevent Serious Cross-border Crime", created a new security zone 30 kilometres into Saxony from the Czech and Polish borders. The civil society group Digital Courage[22] warned that "the planned border surveillance places large parts of Saxony under some sort of state of emergency," adding that this was a "statement of distrust toward our Czech and Polish neighbours"[23] and "by implementing these changes, the Saxon Judiciary and Police will take on characteristics of a preventive state."[24]

In line with the DSK's 2017 statement, certain elements of the German government seem to be coming around to the idea that algorithmic governance is a pressing issue. In June 2019, while speaking at an AI conference in Dresden, German Chancellor Angela Merkel again addressed the need for automated decision-making technologies to be deployed under more formal governance oversight mechanisms: "We need [regulation], I'm convinced of that. Much of that should be European regulation."[25] Unclear, however, is how Germany will balance privacy, the politicisation of domestic security issues and EU data-sharing regulations.

By January 2019, the Schengen Information System (SIS II) alone contained nearly 240,000 fingerprints,[26] a further expansion of AFIS.[27] In April 2019, MEPs passed legislation establishing the creation of the Common Identity Repository (CIR). A shared Biometric Matching Service will provide "fingerprint and facial image search services to

14 Knight, B. (2016, 26 October). Germany planning facial recognition surveillance. *DW*. https://www.dw.com/en/germany-planning-facial-recognition-surveillance/a-36163150

15 Data Protection Conference (DSK). (2017, 30 March). Einsatz von Videokameras zur biometrischen Gesichtserkennung birgt erhebliche Risiken [The use of video cameras for biometric facial recognition poses considerable risks]. https://www.datenschutzkonferenz-online.de/media/en/20170330_en_gesichtserkennung.pdf

16 DW. (2018, 7 June). German court throws out terrorism charges against soldier. *DW*. https://www.dw.com/en/german-court-throws-out-terrorism-charges-against-soldier/a-44116741

17 DW. (2018, 12 December). German soldier charged with plotting to kill politicians while posing as refugee. *DW*. https://www.dw.com/en/german-soldier-charged-with-plotting-to-kill-politicians-while-posing-as-refugee/a-41766093

18 Chase, J. (2017, 27 July). German refugee agency unveils new asylum identity technology. *DW*. https://www.dw.com/en/german-refugee-agency-unveils-new-asylum-identity-technology/a-39857345

19 Ibid.

20 Global Rail News. (2017, 2 August). Op. cit.

21 Delcker, J. (2019, 19 April). Big Brother in Berlin. *Politico*. https://www.politico.eu/articleberlin-big-brother-state-surveillance-facial-recognition-technology

22 https://digitalcourage.de

23 van der Veen, M., & Lisken, S. (2019, 22 January). Police Laws in Saxony: Czech, Polish and German Criticism on Plans for Facial Recognition in the Border Region. *Digital Courage*. https://digitalcourage.de/blog/2019/police-laws-in-saxony

24 Interview with Friedemann Ebelt of Digital Courage, 5 July 2019.

25 Delcker, J. (2019, 24 June). AI experts call to curb mass surveillance. *Politico*. https://www.politico.eu/article/eu-experts-want-curtailing-of-ai-enabled-mass-monitoring-of-citizens

26 Bundesministerium des Innern, für Bau und Heimat. (2019, 23 January). Zahlen zu Speicherungen in polizeilichen EU-Datenbanken (2018). https://andrej-hunko.de/start/download/dokumente/1287-speicherungen-polizeiliche-eu-datenbanken-2018/file [note: written response from the President of the German Parliament to Andrej Hunko, a member of Germany's Die Link party]; Sánchez-Monedero, J. (2018). *The datafication of borders and management of refugees in the context of Europe*. Data Justice Project. https://datajusticeproject.net/wp-content/uploads/sites/30/2018/11/wp-refugees-borders.pdf

27 https://ec.europa.eu/home-affairs/content/automated-fingerprint-identification-system-afis_en

cross-match biometric data present on all central systems".[28] ZDnet, quoting EU officials, reported how the CIR will create new rules for data sharing and "would include the Schengen Information System, Eurodac, the Visa Information System (VIS) and three new systems: the European Criminal Records System for Third Country Nationals (ECRIS-TCN), the Entry/Exit System (EES) and the European Travel Information and Authorisation System (ETIAS),"[29] giving law enforcement agencies unprecedented access to personal information such as names and biometric data. The CIR will combine law enforcement, immigration data and other data into a searchable database containing the records of 350 million people who live in and travel to Europe.

Throughout the same time period when the new biometric identity management systems were created with the aim of policing groups like refugees along Germany's eastern border, a new and highly troubling domestic threat began to emerge. The rise of well-trained, highly organised, overtly violent far-right groups have evaded surveillance and in certain cases – like that of Franco A. – actually attempted to carry out atrocities while on the government's payroll. In fact, more than 400 cases of right-wing extremism in the German army alone were under investigation as of April 2018,[30] and by mid-2019, Germany's domestic intelligence service, the Federal Office for the Protection of the Constitution (BfV), was aware of 24,100 right-wing extremists in Germany, more than half of whom were thought to be "violence-oriented".[31] While refugee dialects were being analysed, the messages of the violent right-wing movement were finding new, home-grown adherents.

Blindspots and camouflage

Originally, fingerprints of asylum seekers and visa applicants in Europe were entered into a highly restricted database, searchable by only certain law enforcement agencies under specific protocols.[32] Over time, however, biometric records were repurposed for more general security screening. The infusion of biometric surveillance in German society has taken a few years and in many cases occurred in a piecemeal fashion. What was once billed as a system to verify refugee identity and status has built up an invasive capacity; the ability to police the most vulnerable has given way to a European-wide access control mechanism based on immutable physical characteristics.

When policies are reactive to hyperbolic rhetoric, the result can be turning a blind eye to actual threats to a peaceful society. On 2 June 2019, Germany was shocked by a politically motivated assassination of an outspoken pro-immigration politician by a man who, despite a long history of anti-immigrant violence, was not present on the "watch list" of the BfV.[33] Walter Lübcke, a regional leader from Merkel's CDU party, was shot in the head by a handgun at close range outside his home in Kassel in central Germany's Hesse. The same month, the BfV reported that a group of 30 extremists, most of whom were associated with Germany's police or military, had used police databases to compile a list of the names and addresses of 25,000 people, most of whom were active in various political parties and, according to Deutsche Welle (DW), Germany's public international broadcaster, supported "pro-refugee" policies.[34]

Despite calls from policy makers and AI experts, public figures must do more to educate themselves and the public regarding the shortcomings of this new technology. Some of this education involves a critical re-evaluation of what AFR fundamentally is. "Decision makers need to highlight policy around data sourcing and consent," said Adam Harvey,[35] a Berlin-based researcher and artist who studies AFR. "They need to understand that AI products are data-driven products and therefore data sets are part of the product, not an externality."

Conclusion

Despite the push by some of Germany's leaders to increase the cultural assimilation of refugees, the worrying prospect of a society-wide surveillance state powered by biometric access control mechanisms now looms large over the entire German society. In a

28 European Commission. (2018). *EU Interoperability Framework For Border Management Systems: Secure, safe and resilient societies*. https://www.securityresearch-cou.eu/sites/default/files/02.Rinkens.Secure%20safe%20societies_EU%20interoperability_4-3_v1.0.pdf

29 Cimpanu, C. (2019, 22 April). EU votes to create gigantic biometrics database. *ZDNet*. https://www.zdnet.com/article/eu-votes-to-create-gigantic-biometrics-database

30 DW. (2018, 12 April). Cases of far-right extremism on the rise in German military. *DW*. https://www.dw.com/en/cases-of-far-right-extremism-on-the-rise-in-german-military/a-43352572

31 Knight, B. (2019, 27 June). Germany records small uptick in far-right extremist violence. *DW*. https://www.dw.com/en/germany-records-small-uptick-in-far-right-extremist-violence/a-49379510

32 Monroy, M. (2019, 23 January). Significantly more fingerprints stored in the Schengen Information System. *digit.site36.net*. https://digit.site36.net/2019/01/23/significantly-more-fingerprints-stored-in-the-schengen-information-system

33 Knight, B. (2019, 26 June). Suspect in German politician's murder confesses. *DW*. https://www.dw.com/en/suspect-in-german-politicians-murder-confesses/a-49357904

34 Knight, B. (2019, 29 June). German neo-Nazi doomsday prepper network 'ordered body bags, made kill lists'. *DW*. https://www.dw.com/en/german-neo-nazi-doomsday-prepper-network-ordered-body-bags-made-kill-lists/a-49410494

35 Interviewed by the author. Disclosure: the author was a contributing researcher to megapixels.cc, a project co-founded by Harvey.

country where 20th century atrocities still loom large, evident in discussions on education,[36] and in the recent offer of reparations to Holocaust survivors,[37] the country's approach to how it deals with the world's most vulnerable[38] is a new test of a nation's resilient openness. With the rise of an automated infrastructure, individuals and advocates must be vigilant to safeguard human rights protections. Depending on the system design for algorithmic decision making, certain attributes – like being a police officer or member of the military – may lower the risk score of an individual, yet the number of enlisted extremists is mind-blowingly high.

The non-unified approach by German states and the federal government to both domestic laws and EU obligations put the most vulnerable at risk of having their rights eroded by algorithmic bias and automated discrimination. As biometric systems enter our lives, we also run the risk of normalising invasive surveillance. AFR can also lead to automated human rights abuses, or at least can take humans out of the loop in safeguarding against decisions to ensure that human rights are upheld. In 2018, a record number of refugees were deported from Germany to other EU countries.[39] If this trend is exacerbated by xenophobic policy making or reliance on biased data sets, innocent people may be deported or denied entry into Germany.

German activists working on such issues have warned that "in a free democracy, there is no place for mass surveillance."[40] Ubiquitous AFR can also have a chilling effect on people's actions, as the prospect of "always being watched" by the state can "nudge" our actions for fear of reprisal. Such systems do not appear overnight, however, and the slippery slope from "security" to draconian social control is often paved with seemingly mundane technological steps. Yet once biometric databases like the CIR are accessible by enforcement agencies, regulatory oversight is needed to protect (and deter) against adversarial and unsanctioned actions.

Advocates should see this as a local, regional, national and international issue. Once a person's biometrics are entered in a database, they in many ways are at the mercy of automated systems. Perhaps the only way for someone to be completely safeguarded from automated biometric bias is for the systems to not exist at all.

Action steps

While biometrics are increasingly being used for surveillance, identity management and access control, such a deployment entails cooperation of a wide range of actors. For activists, this means pressurising companies, appealing to governments and lobbying members of parliament.

- *Transparency:* "There may be many more data sets that we don't yet know about that are private," noted Adam Harvey, the AFR researcher.[41]
- *Direct advocacy:* Activists can put pressure on private companies who may seek to sell their biometric access control technologies to governments. Advocacy, geared towards boycott calls, labour-based organising such as employee walk-outs, and other direct-action campaigns have been shown to be effective in some cases.[42]
- *Research:* By unmasking the origins of data sets and procurement practices for the data contained in the data set,[43] advocates can learn more about potential biases in data procurement, labelling and use.
- *Legislative lobbying:* Create model legislation and replicate strategies used by cities like San Francisco[44] to ban AFR use by municipalities.
- *Strategic litigation:* Contest the constitutionality of regulations by governments to prevent the aggregation of various aspects of their surveillance infrastructure.

36 PBS Frontline. (2005, 31 May). Holocaust Education in Germany: An Interview. *PBS*. https://www.pbs.org/wgbh/pages/frontline/shows/germans/germans/education.html

37 Der Spiegel. (2013, 29 May). Germany to Pay 772 Million Euros to Survivors. *Der Spiegel*. https://www.spiegel.de/international/germany/germany-to-pay-772-million-euros-in-reparations-to-holocaust-survivors-a-902528.html

38 Werber, C. (2015, 26 August). Op. cit.

39 The Local. (2019, 21 January). Germany deported record number of refugees in 2018 to EU countries: report. *The Local*. https://www.thelocal.de/20190121/germany-deported-record-number-of-refugees-in-2018-report

40 Interview with Friedemann Ebelt of Digital Courage, 5 July 2019.

41 Interview with AFR researcher Adam Harvey, 11 June 2019.

42 Fang, L. (2019, 1 March). Google Hedges on Promise to End Controversial Involvement in Military Drone Contract. *The Intercept*. https://theintercept.com/2019/03/01/google-project-maven-contract

43 Murgia, M. (2019, 6 June). Microsoft quietly deletes largest public face recognition data set. *Financial Times*. https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2

44 Sheard, N. (2019, 14 May). San Francisco Takes a Historic Step Forward in the Fight for Privacy. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2019/05/san-francisco-takes-historic-step-forward-fight-privacy

GLOBAL INFORMATION SOCIETY WATCH 2019

Artificial intelligence:
Human rights, social justice and development

Artificial intelligence (AI) is now receiving unprecedented global attention as it finds widespread practical application in multiple spheres of activity. But what are the human rights, social justice and development implications of AI when used in areas such as health, education and social services, or in building "smart cities"? How does algorithmic decision making impact on marginalised people and the poor?

This edition of Global Information Society Watch (GISWatch) provides a perspective from the global South on the application of AI to our everyday lives. It includes 40 country reports from countries as diverse as Benin, Argentina, India, Russia and Ukraine, as well as three regional reports. These are framed by eight thematic reports dealing with topics such as data governance, food sovereignty, AI in the workplace, and so-called "killer robots".

While pointing to the positive use of AI to enable rights in ways that were not easily possible before, this edition of GISWatch highlights the real threats that we need to pay attention to if we are going to build an AI-embedded future that enables human dignity.

GLOBAL INFORMATION SOCIETY WATCH
2019 Report
www.GISWatch.org

APC
ARTICLE 19
Sida