Privacy International — Written evidence (NTL0051)

Intro

Privacy International (PI) is a London-based non-profit, non-governmental organisation that researches and advocates globally against government and corporate abuses of data and technology. It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change. PI challenges overreaching state and corporate surveillance so that people everywhere can have greater security and freedom through greater personal privacy. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international organisations like the Council of Europe, the European Parliament, the Organisation for Economic Cooperation and Development, the UN Office of the High Commissioner for Human Rights and the UN Refugee Agency.

The UK House of Lords Justice and Home Affairs Committee seeks written contributions for its current inquiry into the use of new technologies and the application of the law. The Committee has a particular focus on use of advanced algorithmic tools in activities to discover, deter, rehabilitate or punish people who breach the law in England and Wales. Border management may also be under consideration.

In our submission and in responding to the questions, we have highlighted a large number of technologies. We believe that the Committee could focus specifically on the following areas:

1. Data Analytics and integration software (and hardware) which may involve the use of advanced algorithmic tools, in the context of digital forensics. Here we are referring to the use of digital forensics tools which analyse data extracted from digital devices, including mobile phones but extending to other electronic devices. It includes data extracted using cloud extraction and potentially the integration of additional data from other databases. These are used in policing and immigration contexts and questions arise over their impact on decision making. Within this topic is the issue of reliability of extracted data and questions surrounding the commercial tools used.
2. Social media monitoring and decision making. Here we refer to the increasing use of social media monitoring and how it may inform decision making, including the use of algorithmic tools.
3. Live facial recognition technology (LFRT). Here we discuss the dangers of this invasive technology and the attempts by law enforcement and governmental agencies to propose a draft guidance for the use by police in the UK.

Response to questions

1. Do you know of technologies being used in the application of the law? Where? By whom? For what purpose?

Device Extraction

Law enforcement in the UK use mobile phone extraction technology. This has come to light through Privacy International's ground-breaking work in this area and is documented in the reports of the Information Commissioner and Law Commission who made detailed recommendations in relation to search warrants for digital evidence.

There is, however, a lack of information on the purpose of and any safeguards surrounding mobile phone extraction and the Information Commissioner has been critical in her report. Specifically, she identified excessive processing of personal data. We are concerned that mobile phone extraction and associated analytics capabilities could be used for intelligence gathering purposes and in cases such as the Gangs Matrix which was the subject of a damning report from Amnesty International.

There is a further lack of transparency in relation to the use of cloud extraction technologies, data integration and analytics capabilities. We note that in relation to cloud extraction technologies, the list of applications which companies state can be accessed is vast.[1]

In relation to who can utilise device extraction powers, the Police, Crime, Sentencing and Courts (PCSC) Bill provides an indication at Schedule 3 'Authorised persons' those who may or will conduct device extractions. This includes Immigration Officers. There is currently a lack of transparency around use of extraction powers by anyone other than the police.

We note that the PCSC Bill does not limit the powers to mobile phone extraction but refers to 'device extraction.' This refers to any device on which information is capable of being stored electronically and any component of such a device.[2]

There is a paucity of information on extraction from other types of devices, which could include devices such as Amazon Echo, Google Home, Fitbit, connected toys, Smart TVs and a plethora of others connected devices in the so-called 'internet of things'. Device extraction has not been subject to the same level of scrutiny as mobile phone extraction. In 2017 Privacy International sent Freedom of Information requests to police forces in the UK, seeking information on device extraction. We are aware that devices such as vehicle infotainment systems are of interest to law enforcement and governmental agencies. We reported in December 2017 that the Metropolitan Police Agency's Digital Control Strategy identifies infotainment systems in cars as a new forensic opportunity.

Surveillance at the border

An array of digital technologies are being deployed in the context of immigration and border enforcement and administration with little public scrutiny, often in a regulatory or legal void and without careful understanding and consideration of

[1] https://privacyinternational.org/long-read/3300/cloud-extraction-technology-secret-tech-lets-government-agencies-collect-masses-data
[2] https://privacyinternational.org/news-analysis/4586/policing-bill-unsatisfactory-debut-statute-books-mobile-phone-extraction

the impact on migrant communities at the border and beyond. Technologies include mobile phone extraction, social media monitoring and algorithmic decision making.

Privacy International wrote a detailed report about the UK's migration surveillance regime. Specifically, we believe the following areas require urgent attention: data extraction; aerial and space surveillance; data services and analytics; Home Office Biometrics and Law Enforcement Data Service; status checking; Equipment interference powers; international data sharing; GPS location tracking in immigration bail.

There is a lack of publicly accessible guidance, policy and legislation on the use of new technologies and data intensive systems. This must include legislation, policies, guidance, instructions, and data protection impact assessments. In addition, security must form part of risk assessments as the Home Office authorities gather increasing amounts of data which is at risk not only of data breach but abuse by non-state actors and other states. Once we store data it becomes vulnerable to a breach due to accident, carelessness, insider threat, or a hostile opponent. Poor practices in handling the data including the ignorance of the way data was obtained, can undermine the prosecution of serious crimes as well as result in the loss of files containing intimate details of people who were never charged.

Facial Recognition Technology (FRT)

Law enforcement agencies in the UK are also currently expanding their use of facial recognition technology (FRT). In the context of policing, FRT may involve the use of cameras, which can capture individuals' facial images and process them in real time ("live FRT") or at a later point ("Static" or "Retrospective FRT"). The collection of facial images results in the creation of "digital signatures of identified faces", which are analysed against one or more databases ("Watchlists"), usually containing facial images obtained from other sources to determine if there is a match. This image processing can be done with the purpose of either identifying someone at that moment, training the facial recognition system to get better at identifying, or feeding their face to the system for further uses.

For example, in August 2021, the Deputy Mayor for Policing and Crime has recommended the approval of an award for over £3 million for the Retrospective Facial Recognition software contract. Further, in May 2021 the College of Policing launched a public consultation into the development of its draft national guidance on the use of live facial recognition technology (LFRT) by the police. Privacy International, Liberty, Big Brother Watch, Defend Digital Me and Open Rights Group submitted a joint response to the consultation, outlining that LFRT poses significant and unmitigable risks to our society. We have also issued an open letter, supported by over 30 civil society organisations, calling for a ban of this invasive technology.[3]

[3] https://privacyinternational.org/advocacy/4616/pi-and-30-csos-unite-against-use-live-facial-recognition-technology

The use of LFRT represents a huge shift in the relationship between the individual and the State. The implications come not solely from privacy and data protection perspectives, but from the larger ethical question for a democratic society permitting and seemingly condoning the rollout of such intrusive technology. LFRT also raises significant problems for our human rights, such as freedom of expression and freedom of assembly.

We are concerned that LFRT may be used in a broad range of public gatherings such as sporting events, music concerts, and protests, threatening protected rights. Further, deployments of this surveillance technology could mirror and exacerbate existing disproportionate policing practices towards minority communities.

Additionally, On 27 May 2021, PI filed complaints against Clearview AI with the UK and French data protection authorities (ICO and CNIL). Simultaneously, mirror complaints were filed by Hermes Centre for Transparency and Digital Human Rights in Italy, Homo Digitalis in Greece, and noyb - the European Center for Digital Rights in Austria. Clearview is a facial recognition company claiming to have built "the largest known database of 3+ billion facial images". It uses an "automated image scraper" to search the web and collect any images that it detects as containing human faces. All these faces are then run through its proprietary facial recognition software, to build a gigantic biometrics database. Clearview then sells access to this database to private companies and law enforcement authorities. There are reports of police forces in the UK having trialled the facial recognition technology, and the ICO is currently investigating to determine whether it is compatible with privacy and data protection law (alongside many other regulatory investigations across the world, and lawsuits in the US). Clearview is a chilling example of a particularly intrusive technology having been developed and deployed without any assessment of impact on fundamental rights, without adhering to principles of transparency and accountability, and without any safeguards. The use of FRT by both police and/or private actors has a seismic impact on the way our society is policed and broadly monitored. It will result in the further normalisation of surveillance across all societal levels and accordingly contribute to the "chilling effect" on the exercise of fundamental rights, such as our freedom of expression or our right to protest.

With the recent public health emergency triggered by the novel Coronavirus (COVID-19), both private and public actors have taken this opportunity to roll out intensive FRT systems in far more instances of individuals' everyday lives. The introduction of FRT which, in light of COVID-19, might contain far more intrusive capabilities, such as ability to recognise faces wearing masks, once again emphasises how it can also affect people exercising their fundamental rights.

Social media intelligence (SOCMINT)

Social media intelligence (SOCMINT) refers to the techniques (including manual techniques) and technologies that allow the monitoring and gathering of information on social media platforms such as Twitter and Facebook. This can provide valuable intelligence to those who want to monitor, profile, and manipulate people and groups.

SOCMINT includes monitoring of content - such as messages or images posted - and other data which is generated when someone uses a social media networking site. The information that can be obtained from social media includes public interactions - private interactions, including person-to-person, person-to-group, and group-to-group.

The methods of obtaining and analysing social media accounts can take various forms and usually involves the manual or automatic review of content posted in public or private groups or pages; review of results of searches and queries of users; review of activities or types of content of users' post; or scraping - extracting data, including the content of a web page - and replicating content in ways that are directly accessible to the person gathering SOCMINT. Notably, SOCMINT may include tools to collect, retain and analyse a vast range of social media data and interpret that data into trends and analyses.

We live in an age where our communications and interactions with individuals, friends, organisations, governments, and political groups take place on social media. It has provided an opportunity for the instantaneous transfer and publication of our identities, views, interactions, and emotions.[4] The growing intrusion by government authorities risks impacting what people say online, leading to self-censorship, with the potential deleterious effect on free speech and other fundamental rights.[5] It is already being used to monitor recipients of welfare, as part of immigration enforcement mechanisms[6], as well as to crack down on civil society.[7]

We may have nothing to hide, but if we know our local authority is looking at our Facebook page, we are likely to self-censor. The impact is a reframing of social media platforms, users and data in terms of intelligence gathering and criminality. Whilst we may be living much of our lives onto social media sites, we provide information - however innocuous - that we are unlikely to share with local authorities when asked directly, unless we are given proper reason and opportunity to object.

2. What should new technologies used for the application of the law aim to achieve? In what instances is it acceptable for them to be used? Do these technologies work for their intended purposes, and are these purposes sufficiently understood?

New technologies should only be used for the application of the law if the aim is to improve the quality, transparency, and delivery of justice. In other words, if they can produce fairer outcomes than could be achieved without recourse to

[4] See Privacy International campaign "When social media makes you a target": https://privacyinternational.org/when-social-media-makes-you-target

[5] For more information refer to Privacy International's archive of examples of abuse resulting from the use of social media monitoring: https://privacyinternational.org/examples/social-media-surveillance-socmint

[6] Privacy International, "Surveillance Company Cellebrite Finds a New Exploit: Spying on Asylum Seekers", 3 April 2019: https://privacyinternational.org/long-read/2776/surveillance-company-cellebrite-finds-new-exploit-spying-asylum-seekers

[7] Privacy International, "Bahrain threatens crackdown on followers of anti-government social media accounts", 3 June 2019: https://privacyinternational.org/examples/3069/bahrain-threatens-crackdown-followers-anti-government-social-media-accounts

technology. We have all too often observed new technologies being deployed with a promise of greater efficiency in law enforcement, only to result in even greater harm to the rule of law, fundamental rights and open justice.

At a general level, it is only acceptable to use new technologies for the application of the law if this is justified by an ex-ante assessment of the impact on fundamental rights (such as through Human Rights Impact Assessments (**"HRIA"**) or Data Protection Impact Assessments (**"DPIA"**)), with a strict assessment of the necessity and proportionality of using these technologies for their stated purpose. Any deployment must then be accompanied by safeguards to ensure transparency and use for strictly defined purposes, and mechanisms of oversight and remedy in case of abuse.

On a more granular level, the instances in which it is acceptable for new technologies to be used will vary depending on the type of technology. For example, it should never be acceptable to use live facial recognition technology. Due to the impermissibly intrusive nature of this technology, PI submits that live or real-time FRT should never be deployed in public spaces or for mass surveillance purposes.

Static or retrospective FRT is unlawful if deployed in bulk/indiscriminately (mass surveillance approach). However, it could be lawful and may be acceptable if deployed in a targeted way and in accordance with a series of strict safeguards, including legality, necessity and proportionality.

Do these technologies work for their intended purposes, and are these purposes sufficiently understood?

Digital extractions

Extraction from digital devices is complex and technical. It should only be undertaken by properly trained officers in order to ensure that privacy is protected so far as it can be, data is properly interpreted, and information accessed and used responsibly.

However, investigators who operate mobile phone extraction technologies often have little or no forensic training and are increasingly reliant on extraction devices whose capabilities they do not understand.

A lack of expertise, coupled with the vast and ever-increasing amount of data that can be obtained can easily lead investigators to misinterpret evidence:

a) They might pursue lines of enquiry based on what they happen to have time to look at in the extracted data, or seek confirmation of their existing suspicions by interpreting every data point as supporting their line of enquiry while ignoring others ("confirmation bias").
b) They might not understand the differences between printed evidence and digital evidence, as the latter often raises difficulties in distinguishing original from copy evidence, as well as effective use and interpretation of metadata.
c) A lack of training exacerbates the risk of bias.

Live Facial Recognition Technology (LFRT)

Whilst there is a strong emphasis from public and private bodies that the use of Live Facial Recognition Technology (LFRT) enables the fighting of crime, research indicates that this technology does not work effectively for its intended purposes.

The Independent Report on the London Metropolitan Police Services' Trial of LFRT has indicated that only 19% of the matches collected through the use of LFRT were correct. Further, over 60% of matches were found to be incorrect following an identity check.

Further, the potential of bias and discrimination arising from the use of LFR technology - as recognised in the "*Bridges Appeal*"[8] - raises concerns around whether invasive technology of this type can ever be used safely for its intended purpose.

There are significant concerns about the fact that LFRT can be used in ways which are discriminatory. This should be taken in conjunction with discriminatory policing practices, which may influence the way data is inserted into watchlists as well as when the LFRT is being used. Additionally, there have been reports of the inherent bias of the LFR technology itself, raising concerns over its ability to effectively recognise faces of women or ethnic minorities, thereby leading to discrimination.

As a result of these issues, we do not believe that LFRT can work effectively for its intended purpose.

SOCMINT

Our previous research indicated that the use of SOCMINT appears to be used by local authorities to discredit vulnerable families in order to refuse support. In our experience, information on social media accounts is often wildly misinterpreted by local authorities who can make serious and unfounded allegations.[9]

We are concerned that not enough consideration has been given to the inherent lack of social context, data integrity, authenticity, and veracity of conversations that may take place on social media, leading to potential misinterpretation of - and reliance upon - misleading 'evidence'. As a result, we do not believe that the use of social media intelligence is sufficiently reliable for their intended purpose.

3. Do new technologies used in the application of the law produce reliable outputs, and consistently so? How far do those who interact with these technologies (such as police officers, members of the judiciary, lawyers, and members of the public) understand how they work and how they should be used?

---

[8] R (on the application of Edward Bridges) v the Chief Constable of South Wales Police [2020] EWCA Civ 1058

[9] https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020_0.pdf

Digital Extraction

The delivery of justice is dependent on the integrity and accuracy of evidence and trust that society has in it. Here we look at current debates surrounding digital forensics and reliability of extracted data. The focus has largely been on the police which underscores the lack of scrutiny in relation to use of mobile phone extraction by immigration officers.

Ignorance of the way device extraction tools work is dangerous for the proper functioning of the criminal justice system. As Dr Jan Collie, Managing Director and Senior Forensic Investigator at Discovery Forensics, highlighted to the House of Lords Science and Technology Select Committee in 2019:

> "What I am seeing in the field is that regular police officers are trying to be digital forensic analysts because they are being given these rather whizzy magic tools that do everything, and a regular police officer, as good as he may be, is not a digital forensic analyst. They are pushing some buttons, getting some output and, quite frequently, it is being looked over by the officer in charge of the case, who has no more training in this, and probably less, than him. They will jump to conclusions about what that means because they are being pressured to do so, and they do not have the resources or the training to be able to make the right inferences from those results. That is going smack in front of the court."

Dr Gillian Tully, former UK Forensic Science Regulator commented to the committee that:

> "There is a lot of digital evidence being analysed by the police at varying levels of quality. I have reports coming in in a fairly ad hoc manner about front-line officers not feeling properly trained or equipped to use the kiosk technology that they are having supplied to them."

The Serious Fraud Office told the committee that that 'provenance and integrity of material obtained from digital devices is a key area'.

In relation to a study on bias in digital forensics, former Forensics Science Regulator Dr Gillian Tully commented in May 2021 that:

> "I cannot overemphasise the importance of forensic scientists understanding the potential for unintentional bias, and of ensuring they take measures to minimise risks."

Ian Walden, a professor of information and communications law at Queen Mary, University of London, commenting on the same study said that:

> "Not only should we not always trust the machine, we can't always trust the person that interprets the machine."

The study found that the type and amount of evidence "found" by experts on a suspect's computer hard drive to implicate or exonerate them depended entirely on the contextual information they were given about the investigation. Even

those presented with the same information often reached different conclusions about the evidence.

If we are in a position where forensic scientists are being advised about the potential for unintentional bias, then the concern about bias in relation to those who are not trained forensic scientists is surely much greater.

A further word of warning comes from the Police Foundation report:

> "There is a consensus among digital forensics stakeholders that the digital knowledge of frontline police officers involved with forensics needs to be improved. This is not only includes specific software but also digital forensic procedures. We were told that officers can at times ask for too much information and consider it to be urgent or they cannot explain why they need what they are requesting. We were told that sometimes inexperienced investigators do not understand what a reasonable line of enquiry is nor how to preserve digital evidence.
>
> There is a need for much clearer national guidance for police officers regarding the examination of digital evidence. We suggest that there should be minimal intrusion relative to the needs of the investigation."

Despite the above concerns, the House of Lords Science and Technology Select Committee concluded in their investigation into digital forensics that there was little strategy to address very real problems:

> "the rapid growth of digital forensic evidence presents challenges to the criminal justice system. We were not presented with evidence of any discernible strategy to deal with them." (House of Lords, 2019)

Finally, the Information Commissioner's recent report on mobile phone extraction highlights low rates of compliance with Forensic Science Regulator's codes of practice and conduct for forensic science providers and practitioners in the criminal justice system.

Facial Recognition Technology (FRT)

As outlined above, there have been significant concerns about the accuracy of the use of live and static facial recognition technologies. These concerns highlight the inability of technology to identify credible matches, as well as being prone to bias and discriminatory use. Further, a report by Big Brother Watch[10] indicated that automated facial recognition used by police in the UK is astoundingly inaccurate. Such misidentifications, in the context of law enforcement, can have serious consequences for people and are likely to disproportionately affect black and minority ethnic groups.

SOCMINT

[10] https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf

The use of SOCMINT also raises significant concerns in relation to accuracy of information. Making judgements based on social media is plagued by problems of interpretation. What does it mean when you 'like' or share a post on Facebook? Are you endorsing it, raising awareness, or opposing it? What intelligence can be gained from who you interact with and the photos you post?

Whilst this approach, which results in different exploitation of individuals' social media, is approved by the Investigatory Powers Commissioner - the regulator who oversees use of surveillance powers by public authorities in the United Kingdom - there has been a notable absence of public and parliamentary debate. Key questions such as the legitimate aim of such activities and whether social media monitoring is necessary and proportionate in the different contexts it is being deployed by local authorities have not been debated publicly, nor appear to have been considered at a local level in sufficient detail. In most cases classed as 'overt' social media monitoring, there is rarely any form of authorisation and there is an absence of audit and accountability.

PI's research[11] has revealed that understanding of what is overt or covert and what constitutes directed surveillance under RIPA is far from clear. Overt social media monitoring involves the "Casual (one-off) examination of public posts on social networks as part of investigations undertaken is allowable with no additional RIPA consideration."[12] Whereas "Repetitive examination/monitoring of public posts as part of an investigation" constitutes 'covert' monitoring and "must be subject to assessment and may be classed as Directed Surveillance as defined by RIPA."[13]

Our research found that 60% of Local Authorities who use 'overt' social media monitoring do not provide training for staff. There was no clear procedure in the guidance or policy documents disclosed.[14] The large majority of local authorities who use overt social media monitoring appear to have no processes or procedures in place to audit this surveillance tactic, have no idea how often overt social media monitoring is being used nor are therefore able to assess whether it is being used in a way that is legitimate, necessary, proportionate, and effective. Whilst a few local authorities sought to estimate their usage, others said social media monitoring occurred on a daily basis and some said the information might be logged on the case file but not centrally so were not able to respond.

This lack of clear information indicates there is a risk that overt social media monitoring is being used by officials on an ad hoc basis without any assessment of whether it is effective. The failure to monitor the 'overt' use of social media monitoring raises questions about how Local Authorities can assess whether

---

[11] https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020_0.pdf

[12] https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020_0.pdf

[13] Arun District Council Guidance on the Use of Social Media in Investigations

[14] https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020_0.pdf

'overt' social media monitoring is effective and improves rather than undermines the quality of decision making. As noted above, even if it was effective, the absence of public and parliamentary debate over use of overt social media monitoring means a failure to assess the legitimate aim, necessity and proportionality of these activities.

When decision making has serious consequences for an individual, this brings the added risk that comes from unequal access to data, unequal access to justice and the inability to challenge incorrect assumptions that influence or determine human decision making.[15]

PI's research also indicated that there is no quality check on the effectiveness of this form of surveillance on decision making. Social media monitoring is used by the local authorities without individuals' knowledge or awareness, in a wide variety of their functions, predominantly intelligence gathering and investigations. We are concerned that not enough consideration has been given to the inherent lack of data integrity, authenticity, veracity or the social context of conversations that may take place on social media. Leading to potential misinterpretation and reliance upon misleading 'evidence'.

Based on guidance from the Investigatory Powers Commissioner[16], Local Authority policies reflect the belief that "the author has a reasonable expectation of privacy if access controls are applied." But "where privacy settings are available but not applied the data may be considered open source and an authorisation [to access it] is not usually required."[17]

We are concerned that the arbitrary distinction of privacy settings to decide whether or not something is 'open source' in relation to social media is flawed and unsophisticated. As noted by authors Lilian Edwards and Lachlan Urquhart, privacy settings constantly change and can apply differently to different content. In addition, social media sites are motivated by making user content as public as possible and thus difficult for an individual to protect. We further note they may differ depending on other factors such as jurisdiction and device used.

This puts the onus on individuals to understand and check their privacy settings, and fails to recognise that:

1. Privacy settings vary from platform to platform and also change constantly over time in a way that requires constant vigilance of users to maintain a privacy status quo.
2. People share vastly more personal information about themselves, their friends and their networks than they would if a local authority requested this type of information.

---

[15] H. McDonald, The Guardian, "AI system for granting UK visas is biased, rights groups claim", 29 October 2019: https://www.theguardian.com/uk-news/2019/oct/29/ai-system-for-granting-uk-visas-is-biased-rights-groups-claim

[16] Office of Surveillance Commissioners, Procedures and Guidance, "Oversight arrangements for covert surveillance and property interference conducted by public authorities and to the activities of relevant source", July 2016 : https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf

[17] Ibid.

3. Control of what data about you is made public on social media is not simply a matter of easy voluntary choice. For example, in 2018 a Facebook bug changed 14 million people's privacy settings.[18]

This approach to social media settings further fails to adapt to what society believes should be counted as public or private, or indeed to our own ideas and presumptions about what we post on social media and who should have access to it and for what purposes.

The use of social media surveillance techniques is not just limited to the United Kingdom. In 2020, PI revealed how documents obtained by the European Union Agency for Law Enforcement Training (CEPOL) suggest that the latter is facilitating training in social media monitoring and other surveillance techniques.[19] It is important to emphasise that the risks surrounding the use of social media monitoring by public authorities and law enforcement do not only pertain to the right to privacy but may often negatively impact the exercise of other fundamental rights, especially the rights to freedom of expression and to peacefully protest, threatening the very existence of modern democracies.

If left unregulated, the routine collection and processing of publicly available information for intelligence gathering may lead to the kind of abuses we observe in other forms of covert surveillance or other police operations. The potential abuse could involve the systematic targeting of certain ethnic and religious groups by law enforcement agencies. It is impossible to guarantee that there is no racial or religious bias in online monitoring if there is no notice, transparency, supervision and oversight of the police social media intelligence activities.

As public authorities and law enforcement agencies are often secretive about the use of social media monitoring and sources of information, it can be extremely difficult for individuals to challenge any allegations, especially for those who have limited education or don't speak English as a first language. This puts the onus on individuals to understand and check their privacy settings, and fails to recognise that control of what data about you is made public on social media is not simply a matter of easy voluntary choice.

We therefore argue that the use of 'overt' social media monitoring should, at the very minimum, include provisions for the effective exercise of individuals' data protection rights, as well as transparency and accountability mechanisms, including independent oversight.

4. How do technologies impact upon the rule of law and trust in the rule of law and its application? Your answer could refer, for example, to issues of equality. How could any negative impacts be mitigated?

Technologies are most often developed by private entities and deployed in close cooperation with them. These public-private technology partnerships are taking

[18] S. Frenkel, The New York Times, "Facebook Bug Changed Privacy Settings of Up to 14 Million Users", 7 June 2018: https://www.nytimes.com/2018/06/07/technology/facebook-privacy-bug.html

[19] https://privacyinternational.org/long-read/4289/revealed-eu-training-regime-teaching-neighbours-how-spy

on a new form, diverging from traditional public procurement relationships. We observe much more co-dependency between the parties, whereby the state may be developing new systems or processes entirely reliant on the services of one company, and the company may be receiving access to data or other information for use in developing its own services. Beyond a simple "one-off" commercial relationship, these partnerships are often built over courting, promises of attaining perfect truth, and ever more private access to data – often circumventing public procurement rules and impeding on fundamental rights in the process.

The privatisation of public responsibilities can be deeply problematic if deployed without the safeguards required to ensure civil liberties and human rights are not quietly abused. This is particularly true when the systems deployed are used for surveillance and mass processing of personal data. Private companies have been known to play with the limits of what can legally and ethically be done with individuals' identities and data, without the same level of accountability required of public authorities – a significant affront to fundamental rights when used to deliver a public service.

To address these issues, PI believes that strong safeguards should be implemented by public authorities and companies who intend to enter into such partnerships - these should ensure transparency, compliance with procurement procedures, legality, necessity & proportionality, accountability, oversight and redress. We provide more detail about what these safeguards should contain in our responses to other questions below.

5. With regards to the use of these technologies, what costs could arise? Do the benefits outweigh these costs? Are safeguards needed to ensure that technologies cannot be used to serve purposes incompatible with a democratic society?

We have outlined at length in responses to previous questions the costs that can arise from the use of these technologies. For certain technologies, the benefits never outweigh the costs (such as live FRT). For others, whether the benefits outweigh the costs will vary between different use cases, and will depend on the implementation of appropriate safeguards.

To ensure that technologies cannot be used to serve purposes incompatible with a democratic society, legality, necessity and proportionality safeguards must be implemented. First, the use of a technology or system to deliver public functions can only ever be legitimate if it is "legal", in the sense of falling under an appropriate legal framework that authorises such technology to be used for such purposes. If not, the technology must not be experimented with nor deployed before appropriate statutory legislation is passed. A proper legal framework must also contain specific policies and guidance governing the use of the technology.

In addition, any interference with fundamental rights must be necessary and proportionate. Any technology deployed by the state that interferes with citizens' fundamental rights must demonstrate the specific nature of the threat or issue that it seeks to address, and show that the interference is "in proportion to the

aim and the least intrusive option available".[20] This can be ensured by carrying out, as part of a HRIA or DPIA:

(1) a necessity assessment, to clearly demonstrate that recourse to a particular technology or data analytics system is necessary to achieve defined goals, rather than a mere advantage. As part of this assessment, any projected positive effects of a technology must be assessed through a collection of independent evidence sources and comparative practices.
(2) a proportionality assessment, to measure the adverse impact on citizens' rights and civil liberties and demonstrate that it is justified by a corresponding positive impact on citizens' welfare. These assessments must take into account the potential chilling effects on rights such as the rights to freedom of expression and freedom of assembly, which can be affected by surveillance and data processing systems in ways that can be difficult to anticipate and measure.

6. What mechanisms should be introduced to monitor the deployment of new technologies? How can their performance be evaluated prior to deployment and while in use? Who should be accountable for the use of new technologies, and what accountability arrangements should be in place? What governance and oversight mechanisms should be in place?

A fundamental pre-requisite to appropriate monitoring of the deployment of new technologies is transparency – especially when the technologies at stake are developed and/or deployed in collaboration with private entities. Public-private partnerships often suffer from a lack of transparency, due to companies' commercial interests in preserving confidentiality in their proprietary systems and algorithms – and we have often seen states liberally use that justification to withhold as much information as possible about details of a surveillance or data analytics technology. Transparency must be present at every step of deployment – from public tender processes to policies around deployment of technologies, to the impact or results of deployments. This is essential for the public and civil society to grasp the extent of and the modalities of surveillance and government through data. In practice, this requires:

(1) all documentation about the deployment (contracts, MoUs, DPIAs, data protection policies, use policies, Data Processing Agreements…) to be made publicly available;

(2) a public record of surveillance technologies to be set up containing details and purpose of technologies, their coverage (geography, time), and identified risks to individuals' rights and measures taken to mitigate those;

(3) technologies to be fully auditable, for third parties to be able to understand what data the technology has access to, how it analyses the data and draws conclusions, and what role it performs in the public authority's decision-making process.

[20] Office of the United Nations High Commissioner, The Right to Privacy in the Digital Age (30 June 2014), para 23. Available from https://undocs.org/A/HRC/27/37.

As part of the process for selecting a new technology and designing its deployment, authorities should ensure that a DPIA and HRIA are performed. If the authority is contracting with a private entity, it should ensure that the latter has performed Human Rights Due Diligence at early stages in the design and development of a technology, and commit to performing HRDD at deployment and use stages as well. Authorities must award a contract and start deployment of a technology only after these assessments have been performed, published and made available for review by independent oversight bodies and the public for a specified amount of time.

As to accountability, the core principle should be that responsibilities are clearly defined. This means identifying obligations, duties and standards that shall be imposed upon each actor of the deployment – for example through the inclusion of references to recognised codes or tailor-made policies. When a public authority contracts with a private entity, it should ensure that the company adopts the provisions of any relevant laws, guidelines, or codes by which the public authority is bound. This should be explicitly provided for in the documentation governing the partnership. In addition, this documentation should append an agreed-upon human rights framework which shall govern the deployment of the technology throughout its lifecycle. Once a technology is approved for use, a technology use policy must be developed to govern the public authority's use of the technology that defines clear boundaries for the purpose and use of the technology, with an exhaustive list of authorised uses and a non-exhaustive list of prohibited uses. Any use of the technology that does not comply with this policy must undergo a new approval process determining whether the new use can adhere to the technology use policy, and if not, a separate use policy must be developed for that new use. Finally, algorithms and other decision-making processes deployed as part of a technology must be open to scrutiny and challenge – by being auditable. The ability to audit technologies is particularly essential in order to provide adequate oversight and redress (for example, if a technology has led to a result that is later challenged in court or used as evidence, the proper administration of justice requires the technology to be entirely auditable).

As to oversight, an independent oversight body must be designated for every technology deployment - depending on the technology and authority involved, this could be bodies like the Information Commissioner's Office or the Investigatory Powers Commissioner's Office, or other appropriate body. This oversight body should be responsible for:

(1) reviewing, approving or rejecting new proposals for use of the technology or system deployed as part of the PPP,
(2) undertaking regular public consultations on the impact of a technology on the rights of civilians and the achievement of its intended objective(s), and

(3) receiving grievances and mediating those between the public and the entities using the technology.

When a technology is likely to affect certain communities in a disproportionate way, the oversight body should institute a "civilian control board" composed of individuals directly affected by the technology, in particular those at risk of

discrimination. This control board may be tasked with receiving and voicing grievances as to the impact of the technology on individuals' rights and freedoms. Throughout the lifecycle of a technology's deployment, public authorities ought to record indicators of performance of the technology such as successes, failures, accuracy levels, purpose and outcome. Through an independent oversight body, and in collaboration with a civilian control board, they should carry out regular audits of the technology and updates to relevant HRIAs and DPIAs. These audits should include regular consultations with groups and individuals affected by the technology (in particular those at risk of discrimination) and with CSOs, to evaluate the ongoing or potential impacts of the technology in a holistic way.

7. How far does the existing legal framework around new technologies used in the application of the law support their ethical and effective use, now and in the future? What (if any) new legislation is required? How appropriate are current legal frameworks?

Device Extraction

In June 2020 the Information Commissioner's Office released its critical report on the use of extraction technology. The ICO called for reforms and safeguards to protect an individual's data from unnecessarily intrusive practices. The ICO echoed PI's concerns that currently there is no clear legal basis, policy guidance or independent oversight for police forces' use of extraction technology.

The Law Commission in its report recommended a wider review of the law governing the acquisition and treatment of electronic material in criminal investigations, which is not confined solely to search warrants.

The Police, Crime, Sentencing and Courts Bill at Chapter 3 includes provisions for 'extraction of information from electronic devices'. Privacy International have serious misgivings about the powers set out in the Police Crime Sentencing and Courts Bill. We have made detailed submissions to the Joint Committee on Human Rights and note the Committee are awaiting a response from the Home Office to questions they have posed.

We are concerned that the powers in the draft PCSC Bill and associated guidance in the Code avoid dealing with the existing problems. Rather than address concerns raised by the ICO and striving to create a legal framework that is publicly accessible, clear, precise, comprehensive and non-discriminatory, in the words of the ICO "There is a risk the Bill simply adds to the existing set of powers available to police."[21]

The Bill relies solely on voluntary provision of an electronic device which does not appreciate either the inherent power imbalance between the police and individuals; or the breadth of data which can be obtained - of which an individual will have little understanding. The proposals ignore the recommendations of the Information Commissioner and Law Commission and do not clarify powers of seizure and extraction.

[21] https://ico.org.uk/media/about-the-ico/documents/2620093/ico-investigation-mpe-england-wales-202106.pdf

Consent or voluntary agreement sound empowering. It gives the appearance of control by an individual of their device and their data. But it does not appreciate the power imbalance between the state and an individual. Given the inherent power imbalance between the police and the user, the instances in which provision of a device will be truly voluntary is questionable. The ICO state in their report that individuals may be worried that a decision not to consent will impact on the progress of their case, especially when the electronic devices are taken from victims of rape and sexual assault.[22]

Provisions for voluntary agreement fail in other respects. As pointed out in Committee Debates:

- There is no definition of 'agreement' in the legislation to specify that it must be informed and freely given, to avoid abuse of this power
- There is no requirement for authorities to be specific about what data they are seeking. yet only with specificity can the data owner give informed agreement to extraction.
- The Bill does not define what constitutes a reasonable line of inquiry. Without a clear definition, immigration officers will be able to rely on merely reasonable belief and relevance, creating a risk of embedding a culture of wholesale downloads and intrusion into privacy.

In relation to Immigration Officers, we note not only the vulnerability of the circumstances of migrants but language barriers. Further, seizing phones completely cuts individuals off from communications with their family members in their countries of origin.

The Bill is notably silent on the ability of the individual to withdraw their agreement to the provision of their device i.e., request its return and whether an individual can cease their agreement to the gathering and storage of their data.

Further, the lack of information provided to the individual regarding the extraction, examination, retention, deletion, sharing and search parameters undermines the idea that providing the device can be properly informed. An individual will not be aware whether data will be extracted from the Cloud, what search parameters exist (if any) or whether advanced machine learning technology will be used.

Whilst there may be a case for a process by which a victim can voluntarily provide a device to police containing a specified text message or photo, to introduce voluntary agreement as the only solution to the absence of clear legal basis to use extraction technology is a missed opportunity.

As Vera Baird QC pointed out in evidence to the Bill Committee, the Bill describes information to extract as relevant but does not make reference "to the very important turn of phrase in the legislation, which is a 'reasonable line of inquiry.' It is much broader".[23]

---

[22] https://ico.org.uk/media/about-the-ico/documents/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

[23] https://privacyinternational.org/news-analysis/4586/policing-bill-unsatisfactory-debut-statute-

FRT

In relation to the use of facial recognition technology, law enforcement agencies consistently rely on common law policing duties, Human Rights Act 1998, the Freedom of Information Act 2000, the Protection of Freedoms Act 2012, the Data Protection Act 2018, UK General Data Protection Regulation and the Equality Act 2010 to establish the legal basis for the use of facial recognition technology'.[24] This is very problematic, considering that the majority of these sources either relate to public access to information regarding police activity and do not establish explicit legal authorisation for the use of FRT technology as such.[25] The difficulty with relying on the common law duties of police as sources of implicit legal authorisations is the ambiguity that will arise in relation to its use. It is questionable how far this would be compatible with the 'in accordance with the law test' set out by the human rights law, which requires several different elements to be fulfilled. Relying on the vague and ambiguous 'common law duties' cannot protect against the arbitrary rights interferences and foreseeability with respect to how the law will be applied.[26]

As outlined by Professor Pete Fussey and Dr Daragh Murray, 'without explicit legal authorisation in domestic law it is highly possible that deployment of facial recognition technology…may be held unlawful if challenged before the courts'.[27] We also note that MPs in the House of Commons Science and Technology Committee called for the police use of LFRT to be suspended until further a legislative framework is applied to the technology.[28]

SOCMINT

Social media is an attractive source of data for a wide variety of government authorities and private companies. A plethora of sites and apps provide a vast trove of information about individuals, as social media platforms increasingly play a vital role in the development of an individuals' private, social and political life as well as their online identity.

For many they constitute the digital life setting of today's civic spaces where people formulate and discuss ideas, raise dissenting views, consider possible reforms, expose bias and corruption and organise to advocate for political, economic, social and environmental and cultural change.

As such engagement with these platforms can reveal personal preferences, political and religious views, physical and mental health and the identity of an individuals' friends and family. Social media can contain additional data which

---

books-mobile-phone-extraction

[24] https://assets.college.police.uk/s3fs-public/2021-05/live-facial-recognition-app.pdf

[25] http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf

[26] http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf p. 8-9

[27] http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf p. 9

[28] UK House of Commons Science and Technology Committee, The work of the Biometrics Commissioner and the Forensic Science Regulator: Nineteenth Report of Session 2017–19 (HC 1970, 18 July 2019)
https://www.publications.parliament.uk/pa/cm201719/cmselect/cmsctech/1970/197003

the user may not be aware of, for example, 'tweets' posted from a mobile phone can reveal location data.

SOCMINT requires more specific regulation, policies and safeguards that consider the unique and specific nature of social media: a privately owned space where people share freely.

The least regulated aspect of social media intelligence relates to the surveillance and monitoring of publicly available data on social networking sites.

We are concerned that despite the likelihood that SOCMINT techniques are widely used across government and by police forces in the UK, there has been no proper review of use across government which leads to inconsistent approaches, legal grey areas and potential for misuse or abuse of sensitive information relation to individuals.

8. How can transparency be ensured when it comes to the use of these technologies, including regarding how they are purchased, how their results are interpreted, and in what ways they are used?

Please see above our response to question 6 (transparency, accountability, and oversight).

9. Are there relevant examples of good practices and lessons learnt from other fields or jurisdictions which should be considered?

The Public Oversight of Surveillance Technology (POST) Act passed by the New York City Council in June 2020: this Act ensures transparency of surveillance technologies used by the NYPD. It requires that the NYPD publishes draft impact and use policies for surveillance technologies (describing how the technology will be used, the limitations in place to protect against abuse, and the oversight mechanisms governing use of the technology), at least 90 days before a new surveillance technology is used. These are published on the NYPD website.

10. This Committee aims to establish some guiding principles for the use of technologies in the application of the law. What principles would you recommend?

We have outlined many principles and safeguards across our answers to previous questions, please see above.

1 October 2021