



THE 'AUTHORITARIAN USE OF TECHNOLOGY': A Global Report

October 2026

privacyinternational.org



ABOUT PRIVACY INTERNATIONAL

Governments and corporations are using technology to exploit us. Their abuses of power threaten our freedoms and the very things that make us human. That's why Privacy International campaigns for the progress we all deserve. We're here to protect democracy, defend people's dignity, and demand accountability from the powerful institutions who breach public trust. After all, privacy is precious to every one of us, whether you're seeking asylum, fighting corruption, or searching for health advice. So, join our global movement today and fight for what really matters: our freedom to be human.



Open access. Some rights reserved.

Privacy International wants to encourage the circulation of its work as widely as possible while retaining the copyright. Privacy International has an open access policy which enables anyone to access its content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons Licence Deed: Attribution-Non-Commercial-No Derivative Works 4.0. Its main conditions are:

- You are free to copy, distribute, display and perform the work;
- You must give the original author ('Privacy International') credit;
- You may not use this work for commercial purposes;

You are welcome to ask Privacy International for permission to use this work for purposes other than those covered by the licence.

Privacy International is grateful to Creative Commons for its work and its approach to copyright. For more information please go to www.creativecommons.org.

Privacy International
62 Britton Street, London EC1M 5UY, United Kingdom
Phone +44 (0)20 3422 4321
privacyinternational.org

Privacy International is a registered charity (1147471), and a company limited by guarantee registered in England and Wales (04354366).

CONTENTS

INTRODUCTION	6
WHAT DO WE MEAN BY 'AUTHORITARIAN USE OF TECHNOLOGY'?	6
METHODOLOGY	8
THE AUTHORITARIAN USE OF TECHNOLOGY AND ITS IMPACT ON HUMAN RIGHTS	8
 CHAPTER 1: FACIAL RECOGNITION TECHNOLOGYINTRODUCTION	11
HOW DOES FRT WORK?	12
WHAT IS FRT?	12
WHY IS IT CONCERNING?	13
WHAT CAN MAKE THE USE OF FRT AUTHORITARIAN?	16
EXAMPLES OF THE AUTHORITARIAN USE OF FRT	17
THE USE OF FRT AT PROTESTS	17
BRAZIL	19
ISRAEL AND THE OCCUPIED PALESTINIAN TERRITORIES (OPT)	21
THE UNITED KINGDOM (UK)	22
HUMAN RIGHTS AND DATA PROTECTION IMPLICATIONS	28
CONCLUSIONS.....	30
 CHAPTER 2: MOBILE PHONE EXTRACTION	33
INTRODUCTION	34
WHAT IS MPE?	34
HOW DOES MPE WORK?	35
WHY IS IT CONCERNING?	37
WHAT CAN MAKE THE USE OF MPE AUTHORITARIAN?.....	38
EXAMPLES OF THE AUTHORITARIAN USE OF MPE	40
THE USE OF MPE AGAINST HUMAN RIGHTS DEFENDERS AND ACTIVISTS	40
THE USE OF MPE AGAINST JOURNALISTS.....	41
THE USE OF MPE AGAINST MIGRANTS.....	43
HUMAN RIGHTS AND DATA PROTECTION IMPLICATIONS	45
CONCLUSION.....	47

CHAPTER 3: SPYWARE	49
INTRODUCTION	50
WHAT IS SPYWARE?	50
HOW DOES SPYWARE WORK?	51
WHAT MAKES THE USE OF SPYWARE AUTHORITARIAN?	52
EXAMPLES OF THE AUTHORITARIAN USE OF SPYWARE	52
NSO GROUP AND THE PEGASUS SCANDAL	53
2.B. COUNTRY EXAMPLES	55
EUROPE: POLAND, GREECE, SERBIA AND THE EU PARLIAMENT PEGA INQUIRY	55
EGYPT	56
EL SALVADOR	57
US (IMMIGRATION AND CUSTOMS ENFORCEMENT – ICE)	59
MEXICO	59
SUDAN	60
ARMENIA	61
THE USE OF SPYWARE IN THE GULF COUNTRIES OF BAHRAIN, UNITED ARAB EMIRATES AND SAUDI ARABIA	61
SPYWARE AGAINST GULF DIASPORA LIVING IN THE UK: LITIGATION AS AN AVENUE OF RESISTANCE	62
BAHRAIN	64
UAE	65
SAUDI ARABIA	66
HUMAN RIGHTS AND DATA PROTECTION IMPLICATIONS	66
CONCLUSIONS	69
CHAPTER 4: SOCIAL MEDIA INTELLIGENCE MONITORING	71
INTRODUCTION	72
HOW DOES SOCMINT WORK?	72
WHAT IS SOCMINT?	72
WHAT CAN MAKE THE USE OF SOCMINT AUTHORITARIAN?	75
EXAMPLES OF THE AUTHORITARIAN USE OF SOCMINT	77
UNITED STATES (US)	77
MEXICO	79
ISRAEL	79

TURKEY	79
COLOMBIA	80
UNITED KINGDOM (UK)	80
HUMAN RIGHTS AND DATA PROTECTION IMPLICATIONS	82
CONCLUSIONS.....	84
 CHAPTER 5: MASS COMMUNICATIONS INTERCEPTION	86
WHAT IS COMMUNICATIONS INTERCEPTION?	87
INTRODUCTION	87
HOW DOES COMMUNICATIONS INTERCEPTION WORK?	88
BULK COMMUNICATIONS INTERCEPTION	89
INTERNATIONAL MOBILE SUBSCRIBER IDENTITY (IMSI) CATCHERS	89
THE ROLE OF GOVERNMENTS AND THE PRIVATE SURVEILLANCE INDUSTRY IN MASS COMMUNICATIONS INTERCEPTION.....	89
WHAT MAKES THE USE OF MASS COMMUNICATIONS INTERCEPTION AUTHORITARIAN?.....	90
EXAMPLES OF THE AUTHORITARIAN USE OF MASS COMMUNICATIONS INTERCEPTION	91
VENEZUELA: SPYING ON MAJOR TELECOMS.....	91
IMSI CATCHERS	92
THE USE OF BULK COMMUNICATIONS INTERCEPTION IN LIBYA	93
HUMAN RIGHTS AND DATA PROTECTION IMPLICATIONS	93
CONCLUSION	95
 CONCLUSION.....	96

INTRODUCTION

Worldwide, we have been observing and monitoring an increase in states' adoption of authoritarian practices and policies. This is either facilitated by new and emerging technologies, or embodied in their very deployment in order to stifle dissent, assert control and diminish human rights. We have coined the term '*authoritarian use of technology*' to describe this global phenomenon.

We are deeply concerned by this growing trend and its impact on the enjoyment of human rights, and felt it necessary to compile this report in order to evidence the types of technologies involved, the ways in which they are being deployed that is causing significant harm, as well as providing examples of use, including country case studies where we are seeing the prolific authoritarian use of technology.

Privacy International (PI) is a global advocacy and campaigning organisation that works at the intersection of technology and human rights. PI campaigns against companies and governments who exploit our data and technologies. We expose harm and abuses, mobilise allies globally, campaign with the public for solutions, and pressure companies and governments to change. As part of our work on this report, we consulted with our network of partners and other civil society organisations from around the world who share an interest in both individually and collectively exploring and challenging the use of authoritarian technologies and tech-enabled authoritarian practices, and in seeking change.

What do we mean by 'authoritarian use of technology'?

In this report, we use the term "authoritarian use of technology" to describe how digital technologies are being deployed — both online and offline — by authoritarian and democratic regimes alike.

We believe that the authoritarian use of technology goes beyond the unlawful use or abuse of technologies by states that PI has been monitoring and exposing for years. Technology's authoritarian use results in a broader societal level, or systematic, undermining of democratic principles, erosion of the rule of law, exertion of significant social and political control, or normalisation of the surveillance of individuals and their communities, particularly those already at risk.

This phenomenon is global in scope. Governments and other actors — including international organisations and corporations — are leveraging technology as a tool to exercise control and exert power, resulting in the quashing of fundamental freedoms, heavily restricting civic spaces, and curtailing the exercise of basic human rights. Surveillance technologies are being expanded and entrenched with the purpose of exerting control over entire populations and groups of people at risk, such as human rights defenders (HRDs), journalists, lawyers, activists, dissidents and those from minority ethnic, national and religious backgrounds.

We understand the authoritarian use of technology to ultimately have an effect which causes widespread suppression, or involve a 'chilling effect', due to spreading a fear of reprisal, and which serves not only to infringe upon the rights of certain individuals, but of whole communities and populations, including the rights to freedom of expression, association,

and privacy.¹ This in turn has a corrosive effect on democratic institutions, mechanisms of accountability, oversight and redress, and the fabric of open societies.

The authoritarian use of technology encompasses instances where technologies are abused or misused for intrusive surveillance or other harmful practices in both public and private spheres. Indeed, instead of protecting individuals and communities, authoritarian uses of technology facilitate their targeting, persecution or ostracism.

Authoritarian technology can be used in border contexts against individuals who are migrating; in political contexts against those exercising freedom of speech and dissenting from the governing power; in security contexts where state security forces interfere with personal freedoms by taking baseless or disproportionate measures to monitor, track and control people in public spaces; or in conflict settings where technology serves to undermine or violate humanitarian law rather than uphold it.

Such practises often take place where legislative, technical and regulatory safeguards to oversee the deployment of such technologies are weak, incomplete, unenforced, lacking entirely or even explicitly serving to bolster and uphold technologies' weaponisation as tools of oppression and in turn their authoritarian use.

We use the term “authoritarian use of technology” to refer to how digital technologies are being used by both authoritarian and democratic regimes online and in public spaces to:

- undermine democratic principles and rule of law,
- exert social and political control over society, and
- normalise and expand the surveillance of individuals and communities at risk;

And in a context where:

- the deployment is occurring without appropriate legislative, technical and regulatory safeguards.;
- the uses of such technologies are not subject to public and democratic scrutiny such as open, inclusive, and meaningful consultations with an array of stakeholders including civil society and affected groups;
- technologies are openly proposed as tools of oppression and repression by promoters, e.g. companies, and deployers, e.g. governments;
- technologies that are intended to fulfill other purposes in society are misused and abused for surveillance;
- there is an erosion of the right to privacy as well as other fundamental rights including the rights to freedom of assembly and expression; and
- the technology is disproportionately targeting individuals and communities at risk including dissidents and political opposition, journalists and human rights defenders.

Not all the above factors need to be satisfied to identify an authoritarian use of technology

1 A/HRC/62/45, 'Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', Gina Romero, 21 April 2026, at 41, <https://docs.un.org/en/A/HRC/62/45>

Methodology

The report is devised into chapters that focus on a specific technology. The technologies that the report looks at include the use of Social Media Intelligence (SOCMINT), Facial Recognition Technology (FRT), Mobile Phone Extraction (MPE), mass communications surveillance (such as bulk interception and IMSI catchers) and spyware.

Within each chapter we include examples and case studies of authoritarian uses of the technology, which can be within a specific country context or regarding how the tech is being used to target a specific group of people such as human rights defenders or journalists.

These case studies and examples not only document incidents of these technologies being used around the world in an authoritarian manner but also conveys that these are not isolated examples and part of a wider emerging trend of the authoritarian use of technology. To this end by using examples to map out the shifting terrain of civic spaces in different regions, the report aims to highlight the rise of the authoritarian use of technology and document how this phenomenon is cutting across borders, cultures and jurisdictions and consequentially in what ways it is manifesting, and to what effect, in social fabrics across the world.

The authoritarian use of technology and its impact on human rights

Across different contexts, regions and actors, this report illustrates that authoritarian uses of surveillance technologies have repeatedly resulted in serious and systemic human rights harms. The five technologies examined, namely facial recognition technology, mobile phone extraction, spyware, social media and intelligence monitoring, and mass communications surveillance, give rise to recurring and interrelated human rights concerns.² The human rights and data protection implications of each authoritarian use are analysed in more detail in each chapter. This section presents a brief overview of the human rights and data protection challenges presented across all technologies.

Unpacked throughout this report, these concerns include profound interferences with the right to privacy; spillover effects on freedom of expression, assembly, and association; discriminatory or disproportionate targeting of certain groups such as journalists, activists, migrants, and political opponents; and the creation of chilling environments that suppress dissent and democratic participation.³ Frequently deployed opaquely and without adequate legal basis, oversight, or effective remedies, these technologies enable mission creep, entrench impunity, and consolidate authoritarian power.⁴

Systemic interference with the right to privacy

The principal human rights concern across the authoritarian use of these five technologies is the systematic interference with the right to privacy. These uses involve highly intrusive

² See chapters 1 to 5.

³ Gina Romero et. al., "'PUSHED INTO THE SHADOWS': Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association', United Nations Special Procedures, 2026 <https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf>

⁴ A/HRC/62/45, 'Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', Gina Romero, 21 April 2026, <https://docs.un.org/en/A/HRC/62/45>

surveillance of the private lives of individuals facilitated by the processing and analysis of vast and diverse volumes of data, which enables a context of pervasive surveillance and exposes sensitive aspects of their lives, such as political and religious beliefs, personal relationships, health, and sexual orientation, among others.⁵ In addition, authoritarian uses of spyware, mass communication surveillance and mobile phone extraction stand out as qualitatively different in terms of the scale and depth of the intrusiveness.

Erosion of and chilling effect on enjoyment of broader fundamental rights and freedoms

The privacy violations are often linked to broader harms and to other rights, especially freedom of expression, freedom of assembly and association, access to information, and the right to an effective remedy.⁶ Coupled with the fact that all these technologies produce a chilling effect, i.e. awareness or suspicion of surveillance leading individuals to self-censor, disengage, or alter behaviour, all of the authoritarian uses in question contribute to the collective weakening of civil society, silencing of pluralism and dissent, and erosion of democratic accountability.⁷

Disproportionate or discriminatory targeting of certain groups in society

Moreover, across the technologies examined, authoritarian uses routinely involve disproportionate or discriminatory targeting of certain groups, namely journalists, HRDs, activists, political opponents, migrants, asylum seekers, and other marginalised groups.⁸ On the opposite end of the spectrum, targeting is frequently enabled by the use of indiscriminate or mass surveillance measures⁹ deployed without individualised suspicion and in the absence of a demonstrable, legitimate aim.¹⁰ Such practices are incompatible with international human rights law, which requires that any interference with fundamental rights be strictly lawful, necessary, and proportionate.¹¹

Absence of clear legal bases, effective safeguards, and independent oversight

Across the authoritarian uses of technologies examined, the absence of clear legal bases, effective safeguards, and independent oversight, combined with pervasive opacity and secrecy, means that the uses of these technologies are not being subject to legal, regulatory and democratic scrutiny creating a conducive environment for abuse and unrestrained power.¹² Furthermore, this deprives affected individuals of the ability to take informed action to protect their rights. When surveillance measures are conducted without transparency and judicial authorisation, they leave individuals unaware that their rights have been interfered

5 Ibid.

6 Ibid.

7 Ibid.

8 A/HRC/62/45, 'Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', Gina Romero, 21 April 2026, at 38-38, <https://docs.un.org/en/A/HRC/62/45>

9 Ibid.

10 Privacy International, 'Mass Surveillance', <https://privacyinternational.org/learn/mass-surveillance>

11 A/HRC/62/45, 'Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', Gina Romero, 21 April 2026, at 38-38, <https://docs.un.org/en/A/HRC/62/45>

12 Privacy International, 'Protest surveillance into court', <https://privacyinternational.org/report/5468/protest-surveillance-court>

with and unable to challenge the lawfulness or necessity of such measures. These conditions severely undermine the right to an effective remedy and entrench structural impunity, particularly in security and intelligence contexts.

The lack of accountability of non-state actors

A further key concern is the role and involvement of the private sector in authoritarian technologies. Few governments are developing and designing their own surveillance tools, so many of them contract companies to provide them with the technology.¹³ As we have documented, these Public-Private Partnerships are often not subject to robust due diligence and oversight.¹⁴ We have observed that companies continue to enter into relationships with governments with poor human rights records and are failing to assess how their services and products are and/or could be linked to potential human rights violations.¹⁵ Another aspect of the role of companies is those who directly/indirectly facilitate government surveillance because of their poor practices and policies which leave our data and the infrastructure vulnerable to being exploited by governments to enable their invasive surveillance practices as we've seen in the case of MPE, SOCMINT, spyware and communication surveillance.

13 Privacy International, 'Safeguards for Public-Private Surveillance Partnerships', December 2021 <https://privacyinternational.org/sites/default/files/2021-12/PI%20PPP%20Safeguards%20%5BFINAL%20DRAFT%2007.12.21%5D.pdf>

14 Ibid.

15 For example, see Chapter 2: Mobile Phone Extraction, pg. 34.

An abstract network diagram composed of numerous light blue circles of varying sizes connected by thin, light blue lines. The circles are distributed across the right half of the image, with some larger circles acting as hubs. The lines create a complex, web-like structure that fills the right side of the frame.

01

Facial Recognition.

Introduction

Facial Recognition Technology (FRT) allows for the authentication and the automatic identification of individuals. It is a technology that uses a camera to capture images of people's faces and then extracts and processes their biometric data to verify an individual or identify a match against an existing image.¹⁶

We are observing FRT being increasingly deployed as a mass surveillance tool as part of the wider expansion of authoritarian practices by a range of actors in public spaces such as at protests and to monitor specific communities, to exert control and stifle dissent, which seriously undermines our rights and freedoms as a society.

What is FRT?

FRT involves the use of cameras to capture digital images of individuals' facial features, and the automated processing of their biometric data to identify, authenticate/verify, or categorise individuals. It works by capturing a facial image and extracting the biometric facial data to create a 'digital signature' of the identified face, which is as unique to an individual as their fingerprint. This image is then stored and compared against an existing image to verify an individual or identify a match. FRT software works in three steps:

1. Face detection: which involves an image being processed to detect a face using cameras with software that collects and processes data about an individual's face.
2. Face printing: which occurs when the software extracts facial features and summarises these features into numbers to make a "face print," which is as unique as a fingerprint.
3. Face matching: which occurs when the software tries to match two or more faceprints to determine if they are the face of the same person.

How does FRT work?

The technology can be used for 'one to one matching' whereby the image is compared against an image the person has already provided, for example it may be used to unlock their devices, authorise payments or sign up for services to verify that it is the person requesting access.¹⁷ However, the use of facial recognition is where the technology captures, processes and analyses the facial image against images held in a database or a 'watchlist', usually containing facial images obtained from other sources to determine a match.¹⁸

16 Joy Buolamwini et. al., 'Facial Recognition Technologies: A Primer', May 2020, <https://people.cs.umass.edu/~elm/papers/FRTprimer.pdf>

17 INCLO, 'Eyes on the Watchers: What is FRT?', <https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/what-is-frt/>

18 Ibid.

FRT is increasingly being deployed by law enforcement for policing purposes to prevent and detect crime such as by identifying wanted or missing persons.¹⁹ FRT is also being used by private entities including banks, supermarkets, nightclubs and gyms on both clients/customers and employees for purposes such as age verification, crime prevention, access control, and workplace monitoring as well as in educational settings.²⁰

FRT can be live or retrospective. Live FRT captures individuals' images and processes their biometric data to find a match in **real time**. This means that digital images of individuals' faces are captured and processed against a database to identify someone on the spot. Whereas retrospective FRT captures digital images of individual's facial features but processes them at a later point, meaning that the processing of the biometric data to identify a match against a database or watch list is done at a later time. Both types have the capability to identify or authenticate individuals on a mass scale. Which means it is no longer directed/targeted to specific individuals but whole spaces.²¹

Some police forces also have 'Operator Initiated Facial Recognition' which is effectively FRT on a mobile phone, which involves the capturing and processing of an individual's facial image on the phone itself and using an app installed on the phone to find a match on a database.

Inferential recognition technologies is another form which refers to emotion or behaviour recognition technologies for the purpose of detecting and predicting human conditions or intentions, such as anger, fear, or predicting a crime.²² For example, emotion recognition tech has been used in educational settings to identify facial expressions like whether a student is bored in class, also known as emotion recognition.²³

Why is it concerning?

FRT works by processing individuals' biometric data, which is extremely sensitive as it is permanently and irrevocably linked to an individual's identity. These systems are highly intrusive because they rely on the capture, extraction, storage and/or sharing of people's biometric facial data - often in absence of explicit consent or prior notice.²⁴ The use of FRT interferes with fundamental rights such as the right to privacy, and if deployed in particular settings such as in public spaces such as on public transport, at protests, educational spaces or cultural events, can have implications for the enjoyment of further fundamental rights such as the right to freedom of assembly and expression, and the right to education, religion and association.²⁵

19 Ibid.

20 Privacy International, 'PI's briefing: A critical examination of facial recognition implementation in educational spaces', 2024, <https://privacyinternational.org/advocacy/5469/pis-briefing-critical-examination-facial-recognition-implementation-educational>

21 INCLO, 'Eyes on the Watchers: What is FRT?', <https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/what-is-frt/>

22 Christiane Wendehorst and Yannic Duller, 'Recognition and Behavioural Detection, Policy Department for Citizens' Rights and Constitutional Affairs', August 2021, [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU\(2021\)696968_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/696968/IPOL_STU(2021)696968_EN.pdf)

23 Meaghan Tobin and Louise Matsakis, 'China is home to a growing market for dubious "emotion recognition" technology', Rest of World, 25 January 2021, <https://restofworld.org/2021/chinas-emotion-recognition-tech/>

24 Privacy International, 'Facial Recognition', <https://privacyinternational.org/learn/facial-recognition>

25 Privacy International, 'UK MPs Asleep at the Wheel as Facial Recognition Technology Spells the End of Privacy in Public', 7 November 2023, <https://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public>

There are also fundamental problems with the technology itself such as some software having inherent bias.²⁶ Further risks arise from how and where it is being deployed, how facial images are collected, by who and for what purposes, compilation of watch lists, or use of databases containing facial images for the automated identification of individuals. Some of these issues we highlight below.

The use of LFRT in public spaces

Live FRT (LFRT) deployed in public spaces is the most invasive type and use of FRT as it involves capturing digital images of anyone who comes within the vicinity of the camera as they go about their daily lives, usually without their knowledge and consent.²⁷ This type of deployment of FRT equates to mass surveillance and can never be justified given its disproportionate interference with individuals' privacy.

Bias and inaccuracies

FRT has been proven to be biased and inaccurate leading to misidentifying people²⁸, particularly women²⁹, black people³⁰ and people from other ethnic minorities.³¹ These concerns are further compounded if the technology uses additional analytics features which increasingly rely on artificial intelligence (AI) applications. This further compound concerns around accuracy and can lead to discrimination as AI algorithms can be built and trained on biased datasets.³²

FRT watch lists and databases

Another concern with FRT is the process by which law enforcement and private sector entities compose watch lists and what databases they access to conduct FRT searches to identify matches.

Law enforcement often claims their watch lists are composed only of individuals who are suspects of serious crimes or missing persons, but in fact they can contain images of victims or witnesses,³³ and more recently children.³⁴ Currently the UK College of Policing guidance

26 Joy Buolamwini, 'Unmasking the bias in facial recognition algorithms', 13 December 2024, <https://mitsloan.mit.edu/ideas-made-to-matter/unmasking-bias-facial-recognition-algorithms>

27 Ibid.

28 Johana Bhuiyan, 'First man wrongfully arrested because of facial recognition testifies as California weighs new bills', The Guardian, 27 April 2023, <https://www.theguardian.com/us-news/2023/apr/27/california-police-facial-recognition-software>

29 Trevor Collins, 'Facing gender bias in facial recognition technology', Help Net Security, 27 August 2020, <https://www.helpnetsecurity.com/2020/08/27/facial-recognition-bias/>

30 Thaddeus L. Johnson and Natasha N. Johnson, 'Police Facial Recognition Technology Can't Tell Black People Apart', Scientific American, 18 May 2023, <https://www.scientificamerican.com/article/police-facial-recognition-technology-cant-tell-black-people-apart/>

31 Drew Harwell, 'Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use', The Washington Post, 19 December 2019, <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>

32 Teo Canmetin, Juliette Zaccour and Luc Rocher, 'Why We Shouldn't Trust Facial Recognition's Glowing Test Scores', Tech Policy Press, 18 August 2025, <https://www.techpolicy.press/why-we-shouldnt-trust-facial-recognitions-glowing-test-scores/>

33 See: <https://www.herts.police.uk/police-forces/hertfordshire-constabulary/areas/about-us/live-facial-recognition-lfr-technology/live-facial-recognition-lfr-technology/>

34 Mosha Borak, 'More missing children than transparency in UK police live facial recognition watchlists', Biometric Update, 5 December 2025, <https://www.biometricupdate.com/202512/more-missing-children-than-transparency-in-uk-police-live-facial-recognition-watchlists>

to police forces on how they compile a watchlist for LFRT purposes, and states that the watch lists can include victims and witnesses, as well as photographs obtained via non-police sources.³⁵

There have also been problems with the use of police accessing non-police databases for the purpose of FRT searches. This can be through privately compiled databases by companies such as Clearview AI³⁶ and PimEyes.³⁷ Clearview, claims to have built “the largest known database of 3+ billion facial images” using an “automated image scraper” to search the web and collect any images that it detects as containing human faces.³⁸ All these faces are then run through its proprietary facial software, to build a gigantic biometrics database.³⁹ Clearview then sells access to this database to private companies and law enforcement authorities.⁴⁰ Legal action has been launched against Clearview’s practices⁴¹, in countries with biometrics or data protection regulation, including the UK⁴², Italy⁴³, France⁴⁴ and Greece.⁴⁵

PimEyes acts as a facial recognition ‘search engine’ allowing users to upload photos and identify where images of an individual appear elsewhere on the internet.⁴⁶ UK police had been using it for FRT searches but have since been banned from accessing it.⁴⁷

Law enforcement has also been accessing other public databases such as passport and immigration databases for FRT searches, giving them millions of photographs of members of the public for FRT searches, and indiscriminately interfering with the privacy of every person in these databases.⁴⁸ This raises concerns of ‘mission creep’ where data or a

35 See: <https://www.college.police.uk/app/live-facial-recognition/live-facial-recognition>

36 See: <https://www.clearview.ai/>

37 See: <https://pimeyes.com/en>

38 Privacy International, ‘Clearview and the long arm of the law’, 17 December 2025, <https://www.privacyinternational.org/long-read/5715/clearview-and-long-arm-law>

39 Ibid.

40 See: <https://www.clearview.ai/clearview-2-0>

41 Privacy International, ‘Get out of our face, Clearview!’, <https://privacyinternational.org/campaigns/get-out-our-face-clearview>

42 Privacy International, ‘Challenge against Clearview AI in Europe’, <https://privacyinternational.org/legal-action/challenge-against-clearview-ai-europe>

43 See: European Data Protection Board, ‘Facial recognition: Italian SA fines Clearview AI EUR 20 million’, 10 February 2022, https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

44 See: European Data Protection Board, ‘Facial recognition: the French SA imposes a penalty payment on CLEARVIEW AI’, 13 May 2023, https://www.edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en

45 See: Home Digitalis, ‘A big success for Homo Digitalis: The Hellenic DPA fines CLEARVIEW AI with €20 million’, 13 July 2022, <https://homodigitalis.gr/en/posts/12155/>

46 See: <https://pimeyes.com/en>

47 Liberty Investigates, ‘Met police computers access ‘dangerous’ facial recognition search engine’, 10 May 2024, <https://libertyinvestigates.org.uk/articles/met-police-computers-access-dangerous-facial-recognition-search-engine/>

48 See: Tony Diver, ‘Police raid passport photo data in ‘historic breach of privacy’’, The Telegraph, 7 August 2025, <https://www.telegraph.co.uk/politics/2025/08/07/police-raid-passport-photo-data-historic-breach-privacy/>; Daniel Boffey, ‘Police to be able to run face recognition searches on 50m driving licence holders’, The Guardian, 20 December 2023, <https://www.theguardian.com/technology/2023/dec/20/police-to-be-able-to-run-face-recognition-searches-on-50m-driving-licence-holders>

database is used for purposes other than its original intended purpose.⁴⁹

The watch lists or databases that private entities compile for FRT searches remain opaque and raise similar concerns. In the UK, Facewatch⁵⁰ is the leading FRT provider to retail companies. Facewatch describes itself as a “cloud-based facial recognition security system [that] has helped leading retail stores... reduce in-store theft, staff violence and abuse.”⁵¹ Facewatch has built a database of facial images stemming from the thousands of cameras operated by Facewatch’s customers.⁵²

The use of FRT in educational settings

In an educational setting students cannot meaningfully consent to the use of FRT due to the inherent power dynamic.⁵³ Furthermore, FRT use in educational settings for administrative purposes can be achieved through less invasive means and therefore remains disproportionate and unnecessary.⁵⁴ Within educational settings there is also a greater chance that FRT will be used on children, and the processing of children’s sensitive data should raise even more concerns. For this reason, FRT should not be used in educational settings under any circumstance.⁵⁵

What can make the use of FRT authoritarian?

While there are inherent issues with FRT, including how and when it is deployed and by who, as outlined above, specific legislation or regulation could be used to ensure prohibitions or restrictions on FRT, or to enable safeguards to mitigate harms, to ensure it is in compliance with human rights law.

However, for the purpose of this report we seek to evidence instances where FRT is being deployed in an arbitrary manner that goes beyond these harms to infringe on rights in such a grave and systemic way that it has serious consequences for a democratic society. To this end we are seeing FRT being deployed in an increasingly hostile manner either to enable mass surveillance or with the intention to target specific communities to stifle dissent.

Below we provide examples related to the deployment of FRT that we classify as authoritarian, including the use of FRT at protests, and the banning of face coverings to facilitate FRT at protests. As well as how FRT has been implemented in countries, such as the UK, Israel and the Occupied Palestinian Territories, and Brazil. We discuss these examples below.

49 Privacy International, ‘The rise of the Surveillance Databases’, 2024, <https://privacyinternational.org/long-read/5455/rise-surveillance-databases>

50 See: <https://www.facewatch.co.uk/>

51 Ibid.

52 Privacy International, ‘Facewatch: The Reality Behind the Marketing Discourse’, 15 October 2020, <https://privacyinternational.org/long-read/4216/facewatch-reality-behind-marketing-discourse>

53 Privacy International, PI’s briefing: A critical examination of facial recognition implementation in educational spaces, 2024, <https://privacyinternational.org/advocacy/5469/pis-briefing-critical-examination-facial-recognition-implementation-educational>

54 Privacy International, ‘Why you should be worried about facial recognition in educational spaces: PI’s briefing’, October 2024, <https://privacyinternational.org/sites/default/files/2024-11/Briefing%20with%20graphic.pdf>

55 Ibid.

Examples of the authoritarian use of FRT

The use of FRT at protests

A trend we are observing globally is governments and law enforcement deploying FRT at protests to identify, monitor and track protesters either openly or surreptitiously. We believe constitutes an authoritarian use of FRT. In some cases, FRT is even used to aid the arrest, or detention of those participating in protests, or to build watch lists of protesters for intelligence purposes.

Using FRT at protests involves the deployment of FRT-enabled cameras by law enforcement to take pictures or videos of people attending the protest to identify them in real-time (live FRT) or at a later point (retrospective FRT).⁵⁶ However, even if a digital image of a protester is captured but a match is not found, these images could be used to create a new database or watch list of people who attend protests for future matching and identification purposes. Furthermore, police might use face-tracking technology to follow an unidentified protester from a rally to their home or car, to identify them with an address or license plate database. Police may also use face clustering technology to create a multi-photo array of a particular unidentified protester and manually identify the protester by comparing that array to a database, where such manual identification would have been impossible based on a single photo of the protester.⁵⁷

There are increasing examples of the deployment of FRT by governments and law enforcement at protests to monitor, intimidate and essentially stifle dissent, and penalise communities. We outline some examples below.

In Hungary, in September 2025 the parliament passed amendments to the Assembly Act, the Infraction Act, and the Facial Recognition Technology Act⁵⁸ to ban LGBTQI+ pride events and protests.⁵⁹ These amendments directly threaten and enable the deployment of FRT at such events to enforce the ban to identify and penalise those who attend.⁶⁰ The Hungarian parliament took these measures despite it being a direct breach of Article 5 of the newly adopted EU AI Act which prohibits and restricts uses of FRT across Europe.⁶¹ Not only does it infringe on the right to protest and freedom of expression but explicitly is being used to target and penalise the LGBTQI+ community.

56 Privacy International, 'How facial recognition can be used at a protest', 2021 <https://privacyinternational.org/explainer/4495/how-facial-recognition-technology-can-be-used-protest>

57 Giulia Gabrielli, 'The Use of Facial Recognition Technologies in the Context of Peaceful Protest: The Risk of Mass Surveillance Practices and the Implications for the Protection of Human Rights', The European Journal of Risk Regulation, 2025, <https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/use-of-facial-recognition-technologies-in-the-context-of-peaceful-protest-the-risk-of-mass-surveillance-practices-and-the-implications-for-the-protection-of-human-rights/A4B2FABA8F32DDBC0217C86837CDBAC6#fn101>

58 EDRI, 'The Commission Must Uphold the AI Act and Fundamental Freedoms in Hungary', 16 October 2025, <https://edri.org/our-work/the-commission-must-uphold-the-ai-act-and-fundamental-freedoms-in-hungary/>

59 Ashifa Kassam, 'Hungary bans Pride events and plans to use facial recognition to target attendees', The Guardian, 18 March 2024, <https://www.theguardian.com/world/2025/mar/18/hungary-bans-pride-events-and-plans-to-use-facial-recognition-to-target-attendees>

60 EDRI, 'The Commission Must Uphold the AI Act and Fundamental Freedoms in Hungary', 16 October 2025, <https://edri.org/our-work/the-commission-must-uphold-the-ai-act-and-fundamental-freedoms-in-hungary/>

61 European Centre for Not-for-Profit Law, 'Hungary's new biometric surveillance laws violate the AI Act', 2025,

In Russia, FRT was used to identify and track down a protester who held an individual demonstration in the Moscow underground, eventually leading to his arrest, which was taken to the European Court of Human Rights (ECtHR).⁶² The police took screenshots of photos and a video of the protester's demonstration from social media, as well as collecting footage from CCTV installed in the stations of the Moscow underground,⁶³ and several days later, used live FRT to locate and arrest him while he was traveling in the underground. The Court concluded that the processing of his personal data in the context of his peaceful demonstration, which had not caused any danger to public order or safety, had been particularly intrusive, and therefore incompatible with the ideals and values of a democratic society governed by the rule of law, in violation of both his privacy and protest rights.⁶⁴

In Austria, FRT was used by police to later identify and prosecute someone who had attended a climate related protest in Vienna in March 2023.⁶⁵ Although the prosecution was later dropped due to police overreach at the protest.

Another authoritarian strategy pursued by governments to enable the use of FRT at protests is the introduction of bans around people wearing face coverings at protests.

FRT was used during Hong Kong's pro-democracy demonstrations in 2019 to suppress dissent and deter people from protesting around fears that participating could result in arrests or other consequences, like being barred from future work or school opportunities.⁶⁶ As a result protesters used counter measures such as wearing masks, goggles and using face paint to frustrate detection. This led to Chinese authorities using legislation called the Emergency Regulations Ordinance to enact a ban on face coverings in October 2019.⁶⁷

In the UK, the Crime and Policing Act 2026⁶⁸ made it a criminal offense to wear a face covering that conceals the wearers or another person's identity when in an area where a protest is taking place. The offense will carry a maximum penalty of one month imprisonment, a £1000 fine, or both. Although the Act does not explicitly state that the purpose of this provision is to enable FRT it is widely implied.⁶⁹

A similar approach has been taken in Kazakhstan. In 2025 an amendment to the country's prevention of offenses law bans face coverings in public spaces, which is reported to

62 Glukhin v. Russia, Application no. 11519/20, 4 July 2023, <https://hudoc.echr.coe.int/#%22itemid%22:%22001-225655%22>

63 Glukhin v. Russia, Application no. 11519/20, 4 July 2023, <https://hudoc.echr.coe.int/#%22itemid%22:%22001-225655%22> para. 7.

64 Ibid, para. 90.

65 Vol.at, 'Data Protection Advocates Criticize Use of Facial Recognition at Climate Demonstration in Vienna', 25 June 2025, <https://www.vol.at/data-protection-advocates-criticize-use-of-facial-recognition-at-climate-demonstration-in-vienna/9504071>

66 Catherine Rhodes, 'The Abuse of Facial Recognition Technology in the Hong Kong Protests', UAB Institute for Human Rights Blog, 13 February 2025, <https://sites.uab.edu/humanrights/2025/02/13/the-abuse-of-facial-recognition-technology-in-the-hong-kong-protests/>

67 BBC News, 'Hong Kong protests: Authorities to announce face mask ban', 3 October 2019, <https://www.bbc.co.uk/news/world-asia-china-49918889>

68 See: <https://www.gov.uk/government/publications/crime-and-policing-act-2026-factsheets/crime-and-policing-act-2026-public-order-offences-factsheet>

69 The Conversation, 'Banning face coverings, expanding facial recognition – how the UK government and police are eroding protest rights', 28 March 2025, <https://theconversation.com/banning-face-coverings-expanding-facial-recognition-how-the-uk-government-and-police-are-eroding-protest-rights-252976>

explicitly state “it is prohibited to wear clothing items in public places that impede facial recognition”.⁷⁰

Overall, the deployment of FRT at protests including further measures to ban face coverings represent a crackdown on ordinary citizens exercise of their rights to express themselves and their dissent via an authoritarian use of technology.⁷¹

Brazil

FRT is increasingly implemented and normalised across all aspects of Brazilian society from football stadiums to large carnival gatherings as well as on public transport and in schools. It's reported that more than a third of Brazil's 212 million people are potentially being monitored with FRT through 376 projects implemented by cities across Brazil.⁷²

Brazil is an extremely diverse country with persistent problems with racism. Therefore, this indiscriminate and mass implementation of FRT across Brazilian cities can only serve to exacerbate existing problems with racism and inequality,⁷³ while also posing risks to privacy and other rights.

Smart Sampa

The Smart Sampa⁷⁴ project in São Paulo is one of the most significant FRT surveillance initiatives which are increasingly being deployed by Brazilian states. It is significant due to the sheer size of the population it impacts - 12 million people - and the number of cameras involved, 25,000, some of which are hidden.⁷⁵

The Smart Sampa system was introduced by the São Paulo Mayor in 2023, aiming to combat crime and manage public safety.⁷⁶ Although the tendering process was suspended on two occasions due to concerns regarding discrimination and racial bias, it was allowed to progress after the Court of Justice granted permission to proceed claiming there was no evidence to support these claims.⁷⁷

The project has a single video surveillance platform that integrates and supports the operations of emergency and traffic services, the city's public transport network, and police forces. The project also integrates several third-party and private cameras into the network.

70 [Galiya Khassenkhanova, 'Kazakhstan bans face coverings in public places', Euro News, 2 July 2025, https://www.euronews.com/2025/07/02/kazakhstan-bans-face-coverings-in-public-places](https://www.euronews.com/2025/07/02/kazakhstan-bans-face-coverings-in-public-places)

71 Marquise Francis, 'Mask bans are growing in popularity. Critics call the trend a 'dog whistle' to quell protest' NBC News, 8 July 2024, <https://www.nbcnews.com/news/us-news/mask-bans-are-growing-popularity-critics-call-trend-dog-whistle-quell-rcna160218>

72 Naiara Galarraga Gortazar, 'In São Paulo, 'Big Brother' is watching, with 25,000 cameras and facial recognition technology', El Pais, 10 May 2025, <https://english.elpais.com/international/2025-05-10/in-sao-paulo-big-brother-is-watching-with-25000-cameras-and-facial-recognition-technology.html>

73 Angelica Mari, 'Facial recognition surveillance in São Paulo could worsen racism', 13 July 2023 <https://www.aljazeera.com/economy/2023/7/13/facial-recognition-surveillance-in-sao-paulo-could-worsen-racism>

74 See: <https://smartsampa.prefeitura.sp.gov.br/>

75 Naiara Galarraga Gortázar, 'In São Paulo, 'Big Brother' is watching, with 25,000 cameras and facial recognition technology', El Pais, 10 May 2025, <https://english.elpais.com/international/2025-05-10/in-sao-paulo-big-brother-is-watching-with-25000-cameras-and-facial-recognition-technology.html>

76 Ibid.

77 Angelica Mari, 'Facial recognition surveillance in São Paulo could worsen racism', Al Jazeera, 13 July 2023, <https://www.aljazeera.com/economy/2023/7/13/facial-recognition-surveillance-in-sao-paulo-could-worsen-racism>

For example, the mayor claimed in an interview that the Supermarket Association, with 7300 units in the city, has offered to collaborate with the project.⁷⁸ The mayor has reportedly expressed plans to have 100,000 cameras by the end of his term in 2028.⁷⁹

The system is managed by a consortium of Brazilian companies that utilise AI-powered software called FindFace, from the Russian-based company Ntechlab⁸⁰. The project and vast network of FRT cameras is overseen by the Smart Sampa Centre, the headquarters of the project which is based in São Paulo.⁸¹ It works by essentially scanning everyone's face who comes within the vicinity of these thousands of cameras comparing their images to a database of wanted individuals to identify a match. The mayor's team emphasises that, to avoid errors, they've adopted a strict protocol whereby the alarm is only triggered when the match rate exceeds 92%.⁸² If there is a match, an alert is triggered at the headquarters, and the police confirm that the arrest warrant is valid, and if valid sends officer or patrol cars who are closest to the suspect to make an arrest. Each arrest is recorded on the "prisonometer," an electronic panel at the Smart Sampa Centre.⁸³

One of the key issues highlighted by civil society and other experts regarding the Smart Sampa system pertains to the negative consequences against the Black community due to inherent bias and accuracy with the technology.⁸⁴ Al Jazeera reported that a study conducted by the Center for Studies on Public Security and Citizenship, which monitors the impact of FRT use by police in Brazil, revealed that more than 90 percent of the individuals arrested through decisions based on FRT in Brazil are Black.⁸⁵ Furthermore, in Rio de Janeiro, it was reported that "the percentage of unjust arrests based on photographic recognition and involving Black individuals reached 81 percent in 2021, according to data from the Public Defenders Chamber of Rio de Janeiro".⁸⁶ Brazil's criminal justice system is also reported to be discriminatory with a high representation of Black people accounting for over 67 percent of the imprisoned population.⁸⁷ Therefore, there are fears that the use of FRT can only exacerbate the risks and harms to this population.

78 Naiara Galarraga Gortázar, 'In São Paulo, 'Big Brother' is watching, with 25,000 cameras and facial recognition technology', El Pais, 10 May 2025, <https://english.elpais.com/international/2025-05-10/in-sao-paulo-big-brother-is-watching-with-25000-cameras-and-facial-recognition-technology.html>

79 Ibid.

80 See: <https://ntechlab.com/>

81 Naiara Galarraga Gortázar, 'In São Paulo, 'Big Brother' is watching, with 25,000 cameras and facial recognition technology', El Pais, 10 May 2025, <https://english.elpais.com/international/2025-05-10/in-sao-paulo-big-brother-is-watching-with-25000-cameras-and-facial-recognition-technology.html>

82 Ibid.

83 Ibid.

84 Connectas Human Rights, 'Lack of regulation and inequality exacerbate flaws in facial recognition in Brazil, says Nina da Hora', October 2025, <https://conectas.org/en/noticias/lack-of-regulation-and-inequality-exacerbate-flaws-in-facial-recognition-in-brazil-says-nina-da-hora/>

85 Angelica Mari, 'Facial recognition surveillance in São Paulo could worsen racism', Al Jazeera, 13 July 2023, <https://www.aljazeera.com/economy/2023/7/13/facial-recognition-surveillance-in-sao-paulo-could-worsen-racism>

86 Ibid.

87 Ibid.

Israel and the Occupied Palestinian Territories (OPT)

The UN Special Rapporteur on the situation of human rights in the Palestinian territories has documented that the Israeli repression of Palestinians and its expansion into the occupied Palestinian territory, and institutionalization of a regime of settler-colonial apartheid, has become progressively automated and enabled by mass data collection and biometric surveillance supporting on-the-ground military personnel.⁸⁸

In 2021, a Washington Post investigation which included testimonies from ex-Israeli soldiers and NGO Breaking the Silence, revealed a vast facial recognition program and database was being used to monitor Palestinians in the West Bank referred to as "Wolf Pack", and dubbed as "Facebook for Palestinians".⁸⁹ The FRT system is reportedly mostly deployed in Hebron, a city in the West Bank that is segregated into two areas, H1, administered by the Palestinian Authority, and H2, administered by Israel, according to the 1997 Hebron Agreement.⁹⁰ Movement between these areas is controlled via military check points.

In 2023, Amnesty International reported on their findings from further investigation into the surveillance tech being used in the West Bank, which exposed details of Israel's "Red Wolf" programme linked to similar, earlier programmes known as Blue Wolf and Wolf Pack.⁹¹ Amnesty reported that there is strong evidence to suggest that Red Wolf is linked with two other military-run surveillance systems, Wolf Pack and Blue Wolf. Wolf Pack is a vast database containing all available information on Palestinians from the OPT, including where they live, who their family members are, and whether they are wanted for questioning by Israeli authorities. Whereas Blue Wolf is an app which Israeli forces can access via smartphones and tablets, and which can instantly pull up the information stored in the Wolf Pack database.

According to Amnesty when a Palestinian goes through a checkpoint where Red Wolf is operating, their face is scanned, without their knowledge or consent, and compared with biometric entries in databases which exclusively contain information about Palestinians. Red Wolf uses this data to determine whether an individual can pass a checkpoint, and automatically biometrically enrolls any new face it scans. If no entry exists for an individual, they will be denied passage. Red Wolf could also deny entry based on other information stored on Palestinian profiles, for example if an individual is wanted for questioning or arrest.

Commenting on the surveillance system Palestinian writer Jalal Abukhater, who at the time was based in East Jerusalem, said, "people feel this chilling effect, where they do not socialise or move as freely as they would – they do not live normally as they would," and that "this form of surveillance system is used specifically to entrench the occupation...to maintain apartheid."⁹²

88 A/HRC/59/23, 'From economy of occupation to economy of genocide, report of the special rapporteur on the situation of human rights in the Palestinian territories occupied since 1967', Francesca Albanese, 2 July 2025, <https://docs.un.org/en/A/HRC/59/23>

89 The Washington Post, 'Israel Escalates Surveillance of Palestinians with Facial Recognition', 8 November 2021, https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html

90 Amnesty International, 'Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians in the OPT', 2023, <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>

91 Ibid.

92 Usaid Siddiqui, 'Chilling effect': Israel's ongoing surveillance of Palestinians', Al Jazeera, 7 May 2023, <https://www.aljazeera.com/news/2023/5/7/chilling-effect-israels-ongoing-surveillance-of-palestinians>

The United Kingdom (UK)

The use of FRT in UK has drastically increased in the past few years by both the police and private actors, at times directly supported by the government. The current use of FRT in the UK is resulting in the normalisation of surveillance across all societal levels and accordingly casting a “chilling effect” on the exercise of fundamental rights. This authoritarian use of FRT is enabled by the absence of appropriate democratic oversight, as no specific legislation exists that would curtail and restrict abusive uses of the tech. Instead, the police and private actors are left to their own devices with their deployment across UK society as the Government proceeds with its deployment without letting Parliament determine whether and how this unprecedented technology is used. Instead, the current deployment of FRT is seeing the UK become a dystopian biometric surveillance state, where everyone is identified and tracked everywhere they go, in real time, as they move through public spaces and get on with their everyday lives.

Lack of dedicated legislation

The use of FRT in the UK was subject to a legal challenge brought by campaigner Ed Bridges, who had his biometric facial data scanned by the FRT on a Cardiff high street in December 2017, and again when he was at a protest in March 2018.⁹³ The Court of Appeal found that the police’s use of FRT breached Article 8 ECHR and that the Police had not conducted appropriate Data Protection and Equality Impact Assessments in accordance with the Data Protection Act 2018 and Equality Act 2010.⁹⁴ Since the judgment, the police have claimed they have sought to address the Court’s findings through developing internal guidance and impact assessments.⁹⁵ But both the police and government continue to rely on a patchwork of legislation that is inadequate to protect people from FRT being deployed in a way that we consider to be authoritarian.

A report compiled by the House of Lords directly acknowledges the myriad of issues surrounding the use of FRT in the UK, stemming from the absence of specific legislation to ensure safeguards.⁹⁶ Furthermore, the police use of FRT was debated in Parliament for the first time in November 2024 during which the then Minister for Policing confirmed that “no one specific law gives the police the power to use live facial recognition”.⁹⁷

Yet successive UK governments continue to pursue the authoritarian use of FRT through further funding for new initiatives. For example, in the April 2024 Spring Budget the government announced £4m for bespoke mobile units to be deployed to local high streets and in November 2024, the government advertised a £20million tender for live FRT systems

93 See: Liberty, ‘Legal Challenge: Ed Bridges v South Wales Police’, <https://www.libertyhumanrights.org.uk/issue/legal-challenge-ed-bridges-v-south-wales-police/>

94 R (Bridges) v The Chief Constable of South Wales Police [2020] EWCA Civ 1058. See: <https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf>

95 See: College of Policing, Live facial recognition technology guidance published, 22 March 2022, <https://www.college.police.uk/article/live-facial-recognition-technology-guidance-published>; Metropolitan Police, Facial Recognition Technology, <https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology/>

96 House of Commons, ‘Debate Pack: Police use of live facial recognition technology’, 11 November 2024, <https://researchbriefings.files.parliament.uk/documents/CDP-2024-0144/CDP-2024-0144.pdf>

97 See: UK Parliament, House of Commons, Facial Recognition: Police Use, Volume 756: debated on Wednesday 13 November 2024, <https://hansard.parliament.uk/commons/2024-11-13/debates/E334DF95-2313-4AAC-AA25-D34F8F7C8DD5/FacialRecognitionPoliceUse>

for police forces across the country.⁹⁸ In August 2025, the UK Home Office also announced the rollout of 10 new Live FRT vans to be used by seven police forces in England.⁹⁹ In 2026, the government's White Paper on police reforms provided that the current number of 10 vans will rise to 50.¹⁰⁰

Its continued reliance on an inadequate patchwork of legislation demonstrates the UK Government's unwillingness to acknowledge the dangers of FRT and the threats it poses to human rights.

In December 2025, following campaigning from civil society, and after years of UK police forces using unregulated FRT, the Home Office announced a long-awaited public consultation which is an opportunity to bring forth robust legislation.¹⁰¹ However, the consultation already sets out plans to expand this technology before the public have had their say.¹⁰²

The use of FRT by UK Police

Police forces across the UK have been using FRT in public spaces as far back as 2016.¹⁰³ A report shows the use of retrospective facial searches conducted by UK police has increased significantly over the past 5 years.¹⁰⁴ In 2021, 19,827 searches were conducted which jumped to 85,158 searches in 2022.¹⁰⁵ UK police officers also are gaining access to operator-initiated facial recognition directly on their smartphones, providing them with excessive power to instantly identify people on the spot.¹⁰⁶ However, what is most concerning is police mass deployment of live FRT in public spaces.

The Metropolitan Police (The Met) have been at the forefront of rolling out live FRT across London, at large scale events including the King's Coronation¹⁰⁷ and Notting Hill Carnival,¹⁰⁸ an annual festival that takes place on the streets of Notting Hill, West London to celebrate

98 Lindsay Clark, 'Smile! UK cops spend tens of millions on live facial recognition tech', The Register, 25 November 2024, https://www.theregister.com/2024/11/25/uk_police_lfr_tender/

99 Home Office, 'News story: Live Facial Recognition technology to catch high-harm offenders', 13 August 2025, <https://www.gov.uk/government/news/live-facial-recognition-technology-to-catch-high-harm-offenders>

100 Home Office, From Local to National: A New Model for Policing, January 2026, https://assets.publishing.service.gov.uk/media/69779267276692606c013862/260125_White_Paper.pdf

101 See: Home Office, Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies (accessible), published on 4 December 2025, <https://www.gov.uk/government/consultations/legal-framework-for-using-facial-recognition-in-law-enforcement/consultation-on-a-new-legal-framework-for-law-enforcement-use-of-biometrics-facial-recognition-and-similar-technologies-accessible>

102 Home Office, 'News Story: Government pledges to ramp up facial recognition and biometrics', 4 December 2025, <https://www.gov.uk/government/news/government-pledges-to-ramp-up-facial-recognition-and-biometrics>

103 Privacy International, 'UK MPs Asleep at the Wheel as Facial Recognition Technology Spells the End of Privacy in Public', 7 November 2023, <https://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public>

104 Ibid.

105 Ibid.

106 See: <https://www.south-wales.police.uk/police-forces/south-wales-police/areas/about-us/about-us/facial-recognition-technology/faqs-for-operator-initiated-facial-recognition-app/>

107 Vikram Dodd, 'Police accused over use of facial recognition at King Charles's coronation', The Guardian, 3 May 2023, <https://www.theguardian.com/uk-news/2023/may/03/metropolitan-police-live-facial-recognition-in-crowds-at-king-charles-coronation>

108 Rajeed Syal, 'Met chief rejects calls to scrap live facial recognition at Notting Hill carnival', The Guardian, 19 August 2025, <https://www.theguardian.com/culture/2025/aug/19/met-chief-rejects-calls-scrap-live-facial-recognition-notting-hill-carnival>

Caribbean culture. In 2023, the Met reportedly scanned 4.7 million faces across the year.¹⁰⁹

Increasingly, the Met are also holding live FRT deployments around the city in so called "crime hotspots", defined as a geographical area of approximately 300-500m, where the Met's "crime data", "intelligence reporting" and/or "operational experience as to future criminality" indicates the crime rate is in the upper quartile.¹¹⁰ In practice, this includes areas with large numbers of people and heavy footfall, usually London Underground stations such as Oxford Circus, Bond Street, Paddington, and Kings Cross, which are subject to repeated deployments.¹¹¹ To this end London is turning into one of the most heavily surveilled cities in the world. These deployments can scan up to 50,000 faces per deployment. On 25 August 2025, 51,221 faces were scanned over a period of nine hours and 39 minutes in one single session.¹¹² Similarly, in the Met's 2026 deployment statistics on 7 April 2026, during a 6-hour deployment at Piccadilly Circus, over 45,000 faces were scanned.¹¹³

Other police forces are following in their footsteps. In Cardiff, South Wales Police have continuously used LFRT at sporting¹¹⁴ and music events.¹¹⁵ Northamptonshire Police used live facial recognition at the 2023 British Grand Prix over two days, which saw 450,000 people attend.¹¹⁶

In October 2025, Croydon, in South London installed the first permanent live FRT camera.¹¹⁷ The Met police also plan to roll out more static live FRT cameras across central London by summer 2027.¹¹⁸

These temporary but sweeping deployments of live FRT are taking place in crowded public areas, with limited warning, without the consent of individuals whose facial data is being processed. Although these deployments do lead to arrests, some of which for reportedly serious offenses, the arrests also relate to breaches of bail and tag conditions, and other

109 Daniel Boffey and Mark Wilding, 'Live facial recognition cameras may become 'commonplace' as police use soars', The Guardian, 24 May 2025, <https://www.theguardian.com/technology/2025/may/24/police-live-facial-recognition-cameras-england-and-wales>

110 the Metropolitan Police Force, MPS OVERT LFR POLICY DOCUMENT, pg. 23, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/policy-documents/lfr-policy-document2.pdf>

111 Bill Curtis and Charles Hyman, 'Met recognition cameras catch 50,000 faces a day', The Telegraph, 24 September 2025, <https://www.telegraph.co.uk/news/2025/09/24/met-police-recognition-cameras-catch-50000-faces-day-london/>

112 Ibid.

113 See: MPS LFR Deployments 2026, <https://www.met.police.uk/SysSiteAssets/media/downloads/force-content/met/advice/lfr/deployment-records/live-facial-recognition-deployment-record-2026>

114 Niamh Campbell, 'Six Nations: Extra 'live facial recognition' cameras to be deployed by police across Cardiff ahead of Wales v Ireland', Belfast Telegraph, 19 February 2025, <https://www.belfasttelegraph.co.uk/sport/rugby/six-nations-extra-live-facial-recognition-cameras-to-be-deployed-by-police-across-cardiff-ahead-of-wales-v-ireland/a1267098689.html>

115 Geneva Abdul, 'Police to use live facial recognition in Cardiff during Beyoncé concert', The Guardian, 17 May 2023, <https://www.theguardian.com/technology/2023/may/17/police-to-use-facial-recognition-technology-in-cardiff-during-beyonce-concert>

116 Tom Percival and Pete Cooper, 'F1 British Grand Prix: Facial recognition at Silverstone being used', BBC News, 6 July 2023, <https://www.bbc.co.uk/news/uk-england-northamptonshire-66120010>

117 See: Video posted by Jason Perry, Mayor of Croydon, on Facebook on 1 October 2025, <https://www.facebook.com/JasonForCroydon/videos/watch-live-facial-recognition-cameras-have-arrived-in-croydon-making-our-town-ce/25353569887615650/>

118 Metropolitan Police, News: The Commissioner's full speech on the Met's use of technology, 24 June 2026, <https://news.met.police.uk/news/the-commissioners-full-speech-on-the-mets-use-of-technology-510746>

minor offenses. It is unclear whether any of the arrests led to any further action.¹¹⁹ The fact remains that thousands of people have their highly sensitive facial data processed unknowingly to conduct these arrests which strongly undermines police claims of FRT being a “targeted” measure.

UK Local authorities and FRT

Local authorities are taking steps to introduce permanent facial recognition cameras in public spaces, either via upgrading CCTV with FRT capabilities or installing new static FRT cameras. Hammersmith and Fulham Council in West London have unveiled plans for an extensive expansion of FRT across the West London borough.¹²⁰ The Council’s Cabinet White Paper sets out details to introduce live FRT cameras in 10 locations, with two cameras initially trialled at each of the 10 locations.¹²¹ They also include plans to upgrade 500 existing CCTV cameras with retrospective FRT and AI capabilities.

Inaccuracies, misidentification and discrimination

There have been several cases of misidentifications because of UK police deployments of FRT which expose inaccuracies in the system. In 2024, Shaun Thompson, a Black anti-knife-crime activist, was wrongly flagged by LFRT, detained and questioned by police at a London Bridge deployment.¹²² In February 2026, an Asian man was wrongfully arrested and detained for several hours after Thames Valley police used FRT which matched him with footage of a suspect of the same race for a burglary that took place 100 miles away in Milton Keynes, despite clear differences including that the suspect was much younger.¹²³ The police had retained the image of the man wrongfully arrested from when he was a victim of an attack 5 years prior, which also raises concerns that victims’ images remain on police databases, potentially triggering future ‘matches’.

As a result of these issues Essex Police commissioned the University of Cambridge to conduct a study which involved actors walking past FRT cameras being actively deployed from marked police vans in Chelmsford.¹²⁴ The results showed it was more likely to correctly identify men than women, and that overall, the technology identifies some demographic groups more successfully than others which they believe raises questions about fairness that

119 Privacy International, ‘Latest Developments with facial recognition technology in the UK’, 15 May 2024, <https://privacyinternational.org/long-read/5322/latest-developments-facial-recognition-technology-uk>

120 Ben Lynch, ‘London borough with most CCTV in UK to see new AI and facial recognition cameras in £3.2m upgrade, London Update, 17 September 2025, <https://www.mylondon.news/news/west-london-news/london-borough-most-cctv-uk-32487781>

121 See: London Borough of Hammersmith & Fulham report to Cabinet on CCTV and Artificial Intelligence – new innovations and improved infrastructure to help combat crime and anti-social behaviour, 15 September 2025, <https://democracy.lbhf.gov.uk/documents/s132480/CCTV%20and%20Artificial%20Intelligence.pdf>

122 Sonja Jessop, ‘Facial recognition tech mistook me for wanted man’, BBC News, 6 August 2025, <https://www.bbc.co.uk/news/articles/cqxcg8v74d8jo>

123 Robert Booth and Mark Wilding, ‘Facial recognition error prompts police to arrest Asian man for burglary 100 miles away’, The Guardian, 25 February 2026, <https://www.theguardian.com/technology/2026/feb/25/facial-recognition-error-prompts-police-to-arrest-asian-man-for-burglary-100-miles-away>

124 Dr Matt Bland & Jacob Verrey, ‘Live Facial Recognition: Accuracy, Watchlists, and Deterrence’, University of Cambridge, 12 March 2026, <https://www.essex.police.uk/SysSiteAssets/media/downloads/essex/about-us/live-facial-recognition/2026-03-12-lfr-accuracy-watchlists-deterrence-cambs-uni.pdf>

require continued monitoring.¹²⁵ As a result of potential risk of bias, Essex police paused deploying FRT.¹²⁶

It is also important to reflect on how the police are using this invasive technology in the context of existing concerns around policing in the UK. The Met has been found to be institutionally racist, misogynist and homophobic¹²⁷, and they are deploying a technology which has also been reported to have inherent bias that can lead to discrimination against minorities.¹²⁸ Therefore, the use of FRT potentially compounds existing discrimination against people of colour and other minorities.¹²⁹

Watch lists and databases

There are also issues concerning how UK police watch lists are compiled for live FRT deployments, as well as police accessing public and private databases for FRT searches which we outline below. Watch lists are the lists of people the police, or other FRT users, are trying to identify through an FRT search.

Comparing data from 2020 to 2022, the number of people on The Met's watch list has gone from about 6,500 to more than 16,000 in 2025.¹³⁰ Issues surrounding how the Police compile watch lists was also raised in the 2020 Court of Appeal judgement *Bridges v South Wales Police*, which concluded police had employed too broad a discretion when deciding who should be on the watch lists for the deployment of FRT.¹³¹ An investigation by The Times and Liberty Investigates revealed that children had also been included on police FRT watchlists, yet the police forces who provided the figures had not recorded the reason for their inclusion.¹³²

Regarding the use of databases, UK Police and the Home Office were exposed as having accessed both the UK passport database and immigration databases with over 150 million photos of the public without a clear legal basis, and without informing the public or parliament.¹³³ Statistics showed the searches jumped from 2 in 2020 to 417 in 2023, and an

125 Dr Matt Bland & Jacob Verrey, 'Live Facial Recognition: Accuracy, Watchlists, and Deterrence', University of Cambridge, 12 March 2026, <https://www.essex.police.uk/SysSiteAssets/media/downloads/essex/about-us/live-facial-recognition/2026-03-12-lfr-accuracy-watchlists-deterrence-cambs-uni.pdf>

126 Robert Booth and Mark Wilding, Essex police pause facial recognition camera use after study finds racial bias, The Guardian, 20 March 2026, www.theguardian.com/technology/2026/mar/19/essex-police-pause-facial-recognition-camera-use-study-racial-bias

127 Vikram Dodd, 'Met police found to be institutionally racist, misogynistic and homophobic', The Guardian, 21 March 2023, <https://www.theguardian.com/uk-news/2023/mar/21/metropolitan-police-institutionally-racist-misogynistic-homophobic-louise-casey-report>

128 Mark Wilding and Daniel Boffey, UK police forces lobbied to use biased facial recognition technology, 10 December 2025, <https://www.theguardian.com/technology/2025/dec/10/police-facial-recognition-technology-bias>

129 Privacy International, 'Live facial recognition cameras may become 'commonplace' as police use soars', 7 November 2023, <https://privacyinternational.org/long-read/5155/uk-mps-asleep-wheel-facial-recognition-technology-spells-end-privacy-public>

130 Bill Curtis and Charles Hyman, 'Met recognition cameras catch 50,000 faces a day', The Telegraph, 24 September 2025, <https://www.telegraph.co.uk/news/2025/09/24/met-police-recognition-cameras-catch-50000-faces-day-london/>

131 *R (Bridges) v The Chief Constable of South Wales Police* [2020] EWCA Civ 1058. See: <https://www.libertyhumanrights.org.uk/wp-content/uploads/2020/02/Bridges-Court-of-Appeal-judgment.pdf>

132 Liberty Investigates, 'Police forces use facial recognition to track children as young as 12', 1 December 2025, <https://libertyinvestigates.org.uk/articles/police-facial-recognition-children-met-government-consultation/>

133 Privacy International, 'Revealed: "Skyrocketing" scale of UK police's Secret Facial Recognition Searches of Passport and Immigration Databases', 7 August 2025, <https://privacyinternational.org/news-analysis/5635/revealed-skyrocketing-scale-uk-polices-secret-facial-recognition-searches>

almost sevenfold increase from 16 searches of the immigration database in 2023, to 102 in 2024.¹³⁴

An investigation by Liberty also found that the Met accessed the mass facial recognition search engine PimEyes 2,337 times from its computers during a three-month period,¹³⁵ which soon after resulted in the Met taking action to block access to the PimEyes website on the Met's devices.¹³⁶

Private entities deploying FRT in the UK

Many private companies in the UK have also been using FRT in a variety of settings including in retail spaces, bars, and public transport, with little to no public consent or oversight.¹³⁷

Fraser's Group, who own the retail shops House of Fraser, Sports Direct and Flannels, were reported to be using live FRT in 27 of their stores.¹³⁸ The Co-op supermarket chain also reportedly has 34 branches using FRT provided by Facewatch.¹³⁹ Sainsbury's has also recently announced a trial of FRT in their stores.¹⁴⁰

In 2025, several cases of misidentification from FRT in retail stores were reported. In June 2025, retailer Home Bargains, wrongly accused a woman of shoplifting and asked her to leave two of their stores after being incorrectly flagged by FRT.¹⁴¹

In July 2023, it was reported that the Minister for Policing and senior Home Office officials held a closed-door meeting with Facewatch, a company responsible for providing FRT throughout the private sector in the UK, particularly in retail spaces.¹⁴² Minutes of the meeting made the concerning revelation that the government minister appeared to have put pressure on the Information Commissioner's Office (ICO), an independent oversight body, by writing to them to ensure they consider the so-called benefits of FRT in fighting retail crime.¹⁴³

The private sector use of FRT in the UK remains almost completely unchecked.

134 Ibid.

135 Liberty Investigates, 'Met police computers access 'dangerous' facial recognition search engine', 10 May 2024, <https://libertyinvestigates.org.uk/articles/met-police-computers-access-dangerous-facial-recognition-search-engine/>

136 See: London Assembly, Question to the Mayor, MPS use of PimEyes <https://www.london.gov.uk/who-we-are/what-london-assembly-does/questions-mayor/find-an-answer/mps-use-pimeyes>

137 Privacy International, 'Toward Regulation: Addressing the Legal Void in Facial Recognition Technology', 1 October 2025, <https://privacyinternational.org/long-read/5682/toward-regulation-addressing-legal-void-facial-recognition-technology>

138 Alex Hern, 'MPs condemn Frasers Group's use of facial recognition cameras in stores', The Guardian, 23 April 2023, <https://www.theguardian.com/business/2023/apr/23/mps-condemn-frasers-groups-use-of-facial-recognition-cameras-in-stores>

139 Shanti Das, 'Facial recognition cameras in supermarkets 'targeted at poor areas' in England', The Guardian, 27 January 2024, <https://www.theguardian.com/uk-news/2024/jan/27/facial-recognition-cameras-in-supermarkets-targeted-at-poor-areas-in-england>

140 Pritti Mistry, 'Sainsbury's to trial facial recognition to catch shoplifters', BBC News, 2 September 2025, <https://www.bbc.co.uk/news/articles/c15l5p4zwdqo>

141 Kelly Foran & Rumeana Jahangir, 'Woman mistaken for thief after shop face scan alert', BBC News, 14 June 2025, <https://www.bbc.co.uk/news/articles/cdr510p7kymo>

142 Marks Townsend, 'Revealed: Home Office secretly lobbied for facial recognition 'spy' company', The Guardian, 2 September 2025, <https://www.theguardian.com/technology/2023/sep/02/home-office-accused-of-secret-lobbying-for-facial-recognition-spy-company>

143 Ibid.

Human Rights and Data Protection Implications

As we have discussed, the use of FRT at protests interferes with the right to privacy and other rights such as freedom of assembly, association and expression. FRT can also be discriminatory as we sometimes see cases of misidentification caused by inherent biases embedded within the technology itself, or if it is used to target specific groups. The UN Special Rapporteur on freedom of assembly and of association has raised concerns about how FRT has affected the ability to remain anonymous in public, enabling the rapid, precise identification and tracking of individuals participating in public assemblies and in associations' activities.¹⁴⁴ Activists from all regions consulted for this report documented how real-time monitoring of crowds and retrospective identification of individuals from captured images heightened chilling effects, depleted anonymity, led to arbitrary, preventive and mass arrests, and reduced public participation at assemblies.¹⁴⁵

While the first question should be whether FRT should be deployed at all, any deployment of FRT should only occur if it is demonstrated to comply with existing human rights law and standards. This includes being subject to the overarching human rights principles of legality, necessity and proportionality. These restrictions and safeguards must be clearly defined in primary national legislation before FRT is deployed to prevent abuse and prevent it from being used in an authoritarian way.

PI believes that certain types or uses of FRT pose such significant risks to human rights that cannot be adequately mitigated due to their indiscriminate nature. Live FRT falls in this category and should be prohibited in public spaces, including at protests to identify protesters. Retrospective FRT use must be subject to safeguards such as prior judicial authorisation and pre-deployment impact assessments. FRT by the private sector should also be controlled and restricted. Furthermore, without a legal framework for regulating FRT in the UK, there are no clear avenues for redress for people wrongfully flagged by FRT.

Various UN bodies and mechanisms have made statements and provided guidance on measures that States should take to ensure FRT is used in a way that complies with international human rights law. Furthermore, some States and jurisdictions have taken steps to introduce safeguards and restrictions to limit human rights abuses, some of which we outline below.¹⁴⁶

In 2021, the UN High Commissioner for Human Rights stated that "[g]iven that it can take time before risks can be assessed and addressed, States should also impose moratoriums on the use of potentially high-risk technology, such as remote real-time facial recognition, until it is ensured that their use cannot violate human rights."¹⁴⁷ The report reiterates calls for a moratorium on the use [of biometric technologies] in public spaces, at least until authorities

144 A/HRC/62/45, 'Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', Gina Romero, 21 April 2026, at 41, <https://docs.un.org/en/A/HRC/62/45>

145 Ibid.

146 Privacy International, 'Toward Regulation: Addressing the Legal Void in Facial Recognition Technology', 1 October 2025, <https://privacyinternational.org/long-read/5682/toward-regulation-addressing-legal-void-facial-recognition-technology>

147 Office of the High Commissioner for Human Rights, 'Press Release: Artificial intelligence risks to privacy demand urgent action – Bachelet', 15 September 2021, <https://www.ohchr.org/en/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469>

can demonstrate that there are no significant issues with accuracy or discriminatory impacts and that these AI systems comply with robust privacy and data protection standards.¹⁴⁸

The UN High Commissioner for Human Rights also called on States and businesses to ensure that new technologies, including facial recognition...are developed and used in ways that do not disrupt and prevent people's ability to exercise their fundamental rights to peaceful assembly and expression, and their right to participate in public affairs.¹⁴⁹ She stated that "[t]here should be a moratorium on the use of facial recognition technology in the context of peaceful protests, until States meet certain conditions including human rights due diligence before deploying it. These include effective, independent oversight of its use; strict privacy and data protection laws; and full transparency about the use of image recordings and facial recognition technology in the context of assemblies[...]. Facial recognition should not be deployed in the context of peaceful protests without essential safeguards regarding transparency, data protection, and oversight in place."¹⁵⁰

In 2020, the then UN Special Rapporteur on freedom of assembly and of association provided comment on the use of surveillance technologies at protests which is applicable to the use of FRT. Including that "surveillance against individuals exercising their rights of peaceful assembly and association can only be conducted on a targeted basis, where there is a reasonable suspicion that they are engaging in or planning to engage in serious criminal offences, and under the very strictest rules, operating on principles of necessity and proportionality and providing for close judicial supervision" and hence recommended that "indiscriminate and untargeted surveillance" both online and offline should be outlawed.¹⁵¹

In 2026, the same UN Special Rapporteur reiterated that states should strictly prohibit "[a]rbitrary, indiscriminate and mass surveillance used for law enforcement purposes, including biometric and AI applications, such as facial recognition technology, AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the Internet or CCTV footage."¹⁵²

The European Union Artificial Intelligence Act 2024 (AI Act)¹⁵³ introduced rules heavily restricting the use of FRT as a high-risk system. It prohibits the use of live FRT in publicly accessible spaces for the purposes of law enforcement, unless such use is "strictly necessary" to search for specific suspects, missing persons, or victims of exploitation, or to prevent threats of terrorism or physical safety of people.¹⁵⁴ A judicial authority or an

148 A/HRC/48/31, United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', 13 September 2021, <https://www.ohchr.org/en/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469>

149 Office of the High Commissioner for Human Rights, 'Press Release: New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States', 25 June 2020, <https://www.ohchr.org/en/press-releases/2020/06/new-technologies-must-serve-not-hinder-right-peaceful-protest-bachelet-tells>

150 Ibid.

151 A/HRC/44/24, 24, Report of the United Nations High Commissioner for Human Rights: Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests, June 2020, <https://www.ohchr.org/en/documents/thematic-reports/ahrc4424-impact-new-technologies-promotion-and-protection-human-rights>

152 A/HRC/62/45, 'Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', Gina Romero, 21 April 2026, at 41, <https://docs.un.org/en/A/HRC/62/45>

153 See: European Commission, AI Act, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>

154 Privacy International, 'Toward Regulation: Addressing the Legal Void in Facial Recognition Technology', 1 October 2025, <https://privacyinternational.org/long-read/5682/toward-regulation-addressing-legal-void-facial-recognition-technology>

independent administrative authority must also grant authorisation before live FRT can be deployed by the police.¹⁵⁵

It also places restrictions on retrospective FRT. Consequently, retrospective use of FRT in an investigation for the targeted search of a person suspected or convicted of having committed a criminal offence is subject to additional conditions and safeguards. These include:

- Judicial or administrative authority's binding authorisation.
- Strict necessity for a specific criminal offence.
- Prohibition of indiscriminate surveillance.
- No adverse legal effect solely based on FRT.
- Documentation of each use for reporting and analysis purposes.¹⁵⁶

Although not without its flaws, the EU AI Act stands as the most concrete example of regulation providing for restrictions and safeguards on the use of FRT.

We have also seen developments across the United States (US) with individual states introducing prohibitions or specific safeguards on FRT. In the US, cities such as San Francisco, Oakland and Boston have banned the use of FRT by public agencies, while the states of Washington, Virginia and Massachusetts have introduced legislation to regulate its use.¹⁵⁷

Conclusions

With the above concerns in mind, FRT should only be used in a manner that complies with international and national human rights law, and other relevant legislation and standards, to ensure it is not exploited and used in an authoritarian way. It should be subject to the overarching human rights principles of necessity, proportionality and legality, with restrictions and safeguards clearly defined in primary legislation to prevent abuse before any FRT is rolled out. Below is a list of essential safeguards for FRT which should be included in a legal framework for FRT:

1. **Prescribed by law:** FRT should not be used unless authorised and regulated by law. The law should be accessible, and provide the public with an adequate indication of the circumstances and conditions under which authorities can deploy and use FRT. The legal framework should also outline:
 - a. The temporal considerations which categorise FRT use as either retrospective or live.
 - b. The safeguards that guard against arbitrary and disproportionate use, as well as the process for authorisation, oversight and remedies for misuse.
 - c. The specifications for probe images for FRT to ensure a quality standard for probe images and guard against tampering. Such standards should consider the source of the image, its age, the quality of the image, whether there is anything obstructing the image, the chain of custody of the image, and whether any rights have been violated in obtaining the image.

155 Ibid.

156 Ibid.

157 Privacy International, 'Toward Regulation: Addressing the Legal Void in Facial Recognition Technology', 1 October 2025, <https://privacyinternational.org/long-read/5682/toward-regulation-addressing-legal-void-facial-recognition-technology>

- d. Details about the requirements to use a database to facilitate FRT including how to assess whether its use is necessary and proportionate, the circumstances under which it may be accessed, and the safeguards in place to limit the interference with the rights of the people in the database.
- e. Provisions regarding requirements for training and impact assessments.

2. **Prohibited uses:**

- a. Live facial recognition technology (LFRT);
- b. Inferential technologies;
- c. To Identify whistleblowers, journalists or journalistic sources;
- d. To categorise people by a protected characteristics;
- e. To Identify protesters or to collect information on people attending peaceful assemblies: and
- f. To Identify people in or around polling stations.¹⁵⁸

3. **Legal basis of use:** The use of FRT should be necessary and proportionate to legitimate aims. This means

- a. Firstly, that deploying this kind of technology would be the least intrusive means of achieving similar identification results, compared to other available investigative techniques, and proportionate to the stated purpose.
- b. Secondly, that the use of biometric technologies should be limited to the following, clearly defined purposes:
 - i. The targeted search for specific victims of abduction, trafficking in human beings, or sexual exploitation of human beings, as well as the search for missing persons;
 - ii. The prevention of a specific, substantial, and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;
 - iii. The identification of suspects or perpetrators of exhaustively listed serious crimes.¹⁵⁹

4. **Prior Judicial authorisation:** Law enforcement should not be permitted to deploy FRT unless there is prior judicial authorisation for such use, except in duly justified urgency whereby a higher-ranking officer, wholly independent of the investigation, must give prior approval.¹⁶⁰ In such exceptional cases, the judicial authorisation must still be requested without undue delay and no later than 48 hours after the use.¹⁶¹ If subsequent judicial authorisation is refused, an information obtained by the use of FRT must be deleted.

158 INCLO, Eyes on the Watchers: Challenging the Rise of Police Facial Recognition, 2025, <https://inclo.net/wp-content/uploads/2024/03/INCLO-FRT-Principles-Final.pdf>

159 See: Article 5, EU AI Act, <https://artificialintelligenceact.eu/article/5/>

160 INCLO, 'Eyes on the Watchers: Challenging the Rise of Police Facial Recognition', 2025, <https://inclo.net/wp-content/uploads/2024/03/INCLO-FRT-Principles-Final.pdf>

161 Under the EU AI Act prior authorisation or without undue delay is to take place within 48 hours and if rejected the FRT must be stopped and any data collected will be deleted.

5. **Reference databases:** The use of private databases should be prohibited. The use of any government database should be authorised by law, and its use should receive prior judicial authorisation when requested at the time of deployment. Databases may only be accessed if doing so is necessary and proportionate. The law should provide sufficient detail to the public about which databases may be used, and the circumstances and conditions under which they may be accessed.
6. **Transparency:** the law should require the publication of certain information, including:
 - a. The number of deployments, including details about where and when it FRT was deployed;
 - b. The number of FRT searches run by each law enforcement body;
 - c. The number of times a particular reference database is searched for the purposes of FRT by each law enforcement body;
 - d. The number of searches that generated leads;
 - e. The number of searches that lead to an arrest or charge;
 - f. The number of misidentifications;
 - g. The demographic breakdown of the probe images used, specifying gender, race and any other relevant protected characteristics;
 - h. Aggregated, de-identifiable information concerning the number of requests made for authorisation, including the lawful basis relied on, the outcome of the request and the databases authorised for use; and
 - i. Annual reports by the oversight body which include the number of complaints received, errors uncovered, and the outcomes.
7. **Independent oversight body:** An independent body should be established to ensure FRT is deployed in compliance with the law. Its establishment, powers, role and obligations should be regulated by law. The body should be structurally and functionally independent, sufficiently resourced and staffed with a range of subject matter and technological experts. The body should be empowered and equipped to hear and respond to complaints from members of the public and to conduct its own investigations and authorised to access the necessary information, compel disclosure and impose remedies and penalties.
8. **Disclosure to people detained, arrested and charged:** To enable the right to fair trial, any person detained, arrested and charged as a result of, or related to, the use of FRT by law enforcement should be provided all relevant information related to the deployment.¹⁶²

162 Privacy International, 'Protest Surveillance into Courts', <https://privacyinternational.org/sites/default/files/2025-01/Protest-surveillance-into-courts.pdf>



02

Mobile Phone Extraction.

INTRODUCTION

Our electronic devices, such as our mobile phones and tablets, contain huge amounts of information and sensitive data about our lives, akin to a real-time diary which constantly tracks our location. Mobile phone extraction (MPE) involves extracting data from an individual's device, or from the cloud services they use, including device information, photos, videos, audio recordings, notes, documents and apps used, as well as the messages, call logs and emails they draft, send and receive.¹⁶³

MPE is often used by police and other authorities for criminal investigations or other law enforcement purposes.¹⁶⁴ However, we are increasingly seeing MPE being used against marginalised individuals, such as migrants and asylum seekers¹⁶⁵ and to target activists and journalists.¹⁶⁶ Furthermore, due to the untargeted nature of the data collected by MPE (and technical difficulties with targeted extraction), it can include gaining access to information subject to legal privilege, journalistic material, other protected data or merely data with no relevance to the purpose of the investigation.¹⁶⁷ Therefore, MPE raises serious implications for an individual's privacy and other rights, as well as creating a chilling effect when used to target vulnerable populations, activists and journalists. Among others.

What is MPE?

Mobile Phone Extraction, also known also as mobile forensics, entails the physical connection of the mobile device that is to be analysed to a device that extracts, analyses and presents the data contained on the phone. The extracted data can include, but is not limited to:

- Device data;
- Phonebook/contact information;
- Call data – who we call, when, and for how long;
- Text messages;
- Stored files – photos, videos, audio files, documents, etc.;
- App data – what apps we use, and the data stored on them;
- Information stored on cloud-based services which are accessible through the phone;
- Location information and;
- Wi-fi network connections – which can reveal the locations of any place where we've connected to wi-fi, such as our workplace and properties we've visited.

163 Privacy International, 'Mobile Phone Extraction', <https://privacyinternational.org/learn/mobile-phone-extraction>

164 Ibid.

165 Privacy International, 'At the border, asylum seekers are "guilty until proven innocent"', 17 June 2020, <https://privacyinternational.org/long-read/3938/border-asylum-seekers-are-guilty-until-proven-innocent>

166 Amnesty International, 'Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists', December 2024, <https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/>

167 Privacy International, 'Mobile Phone Extraction', <https://privacyinternational.org/learn/mobile-phone-extraction>

How does MPE work?

Most device manufacturers seek to make their devices as secure as possible by enabling features such as security chips, encryption, PIN-protection and facial and fingerprint recognition. However, bypassing these security measures may be necessary to facilitate data extraction. A user may first be asked for their passwords to gain access. However, where a password is not provided or unknown, tools to bypass security features are required. Therefore, MPE tools are usually designed to access locked phones by exploiting security vulnerabilities and therefore may constitute a form of "hacking".¹⁶⁸ The ability to bypass security features will depend on the make and model of the phone; the phone's operating system, including whether it's the most updated version; as well as the type of extraction tool being deployed.

There are two stages to MPE, first the extraction of the data from the device itself, followed by the analysis of the data. There are four types of extraction which provide a framework to categorise extraction technologies/tools: manual, logical, file system and physical, each of which are explained below.¹⁶⁹ Some MPE tools can also access data stored remotely in the cloud, known as cloud extraction, typically from a third-party company server.¹⁷⁰

Manual extraction: Manual extraction does not involve the use of specialist tools, it involves viewing information on a user's device and documenting the information for example, by taking screenshots or photographs of what is displayed on screen.¹⁷¹ The device/phone must already be unlocked and involves manually going through the visible files, including messages, call logs, emails, photos, and content from apps. This method is often used in less serious cases.¹⁷²

Logical extraction: Logical extraction creates a copy of the user's accessible files such as their phonebook, calls, messages, and some app data which is expected to be stored from an iPhone or Android backup, or what someone would see if manually examining a user's unlocked device.¹⁷³

File system extraction: File system extraction involves extracting the entire filesystem from a device, including files not directly accessible to the user via the device interface.¹⁷⁴ File system extraction is usually done by a 'root user' so requires 'rooting the phone.' Rooting a phone is the process to attain root access.¹⁷⁵ A 'root user' is a 'superuser' who has permission to do anything to any files anywhere in the phone's system, i.e. privileged control over the phone.¹⁷⁶

168 Privacy International, 'A Technical Look at Phone Extraction', October 2019, <https://privacyinternational.org/long-read/3256/technical-look-phone-extraction>

169 Privacy International, 'A Technical Look at Phone Extraction', October 2019, <https://privacyinternational.org/long-read/3256/technical-look-phone-extraction>

170 Privacy International, 'Cloud extraction technology: the secret tech that lets government agencies collect masses of data from apps', <https://privacyinternational.org/sites/default/files/2020-03/3.12.2019%20Cloud%20Analytics%20LONG%20READ%20FINAL.pdf>

171 Holborn Adams, 'How do police extract data from phones in the UK?', June 2026, <https://www.holbornadams.com/post/how-do-police-extract-data-from-phones-uk>

172 Ibid.

173 Privacy International, 'A Technical Look at Phone Extraction', October 2019, <https://privacyinternational.org/long-read/3256/technical-look-phone-extraction>

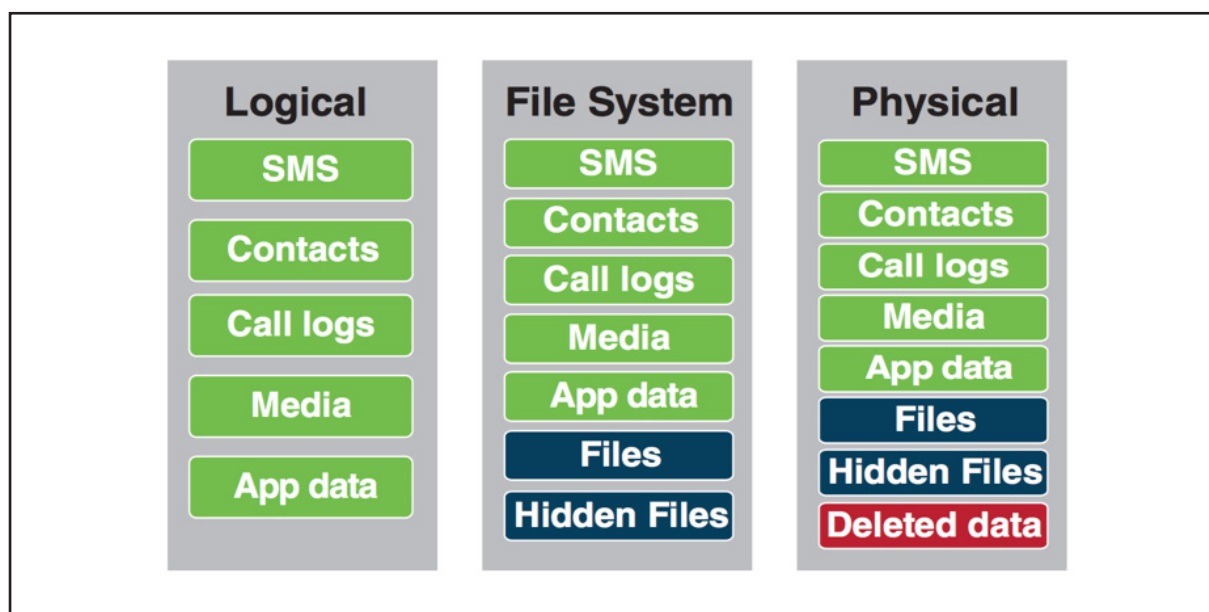
174 Ibid.

175 Ibid.

176 Ibid.

Physical extraction: This is the most advanced method of extraction. The analyst creates a complete copy of the phone's memory, including hidden and deleted information which isn't accessible through manual or logical extraction.¹⁷⁷ It can bypass some encryption and security features, but this is more difficult on the latest mobile phone devices.

Cloud data access: In certain jurisdictions police can get a warrant to access your phone data that is stored in the cloud, if your phone has been backing up your data to the cloud, including your photos/videos, messages, call logs, location data, and more.¹⁷⁸ They can request the data directly from the company that hosts your cloud data (Google, Apple, Microsoft, etc).¹⁷⁹



Data analysis: Data analysis is the next stage of the MPE process. At this stage, the data extracted is analysed to make inferences and form intelligence about an individual.¹⁸⁰ Analytics software can facilitate analysis of the data extracted in the following ways:

- **Organise the data** into different files, conduct key searches, or search by image classification;
- Use **visualisation** tools to make the data easier to read such as displaying messages exchanged as a chat, tracing a user's location or activities on a map or chronological timeline; sorting data by file type regardless of its location on the phone; or creating network graphs to infer social relationships using contact data;
- **Link analysis** to analyse phone calls, emails, text messages and location data to discover associations between individuals via different types of data. This can demonstrate the frequency of contacts between phone numbers and between IP addresses over time,

¹⁷⁷ Holborn Adams, 'How do police extract data from phones in the UK?', June 2026, <https://www.holbornadams.com/post/how-do-police-extract-data-from-phones-uk>

¹⁷⁸ Ibid.

¹⁷⁹ Ibid.

¹⁸⁰ Privacy International, 'A Technical Look at Phone Extraction', October 2019, <https://privacyinternational.org/long-read/3256/technical-look-phone-extraction>

financial transactions and chronologies of events, among other things;

- **Bring together datasets from different devices** to find links across the devices, like common contacts, call or text records, or account information.¹⁸¹

Why is it concerning?

The use of MPE by law enforcement

Many governments have confirmed they have acquired MPE tools as part of their wider arsenal of technology and surveillance tools used for investigating crime and other law enforcement purposes.¹⁸² In 2018, PI reported that 26 of 47 UK police forces confirmed they are using MPE technology with another 8 of those remaining having trialled or intended to trial MPE.¹⁸³ In 2020, it was reported that across the US, 2,000 state and local law enforcement agencies have accessed MPE tools.¹⁸⁴ In India, Delhi police force has reportedly acquired a variety of forensic tools for criminal investigation.¹⁸⁵ Likewise, MPE has been deployed by law enforcement authorities and the Public Prosecutors Office in Argentina.¹⁸⁶

However, often governments' use of MPE has not been subject to public scrutiny or democratic oversight, and is often not regulated by legal or regulatory frameworks specific to the technology.¹⁸⁷ This was the case in the UK where police officers were relying on a patchwork of laws to justify the use of MPE, which led to them conducting MPE without seeking a warrant.¹⁸⁸ PI made a complaint to the Information Commissioner's Office (ICO), the UK data protection authority, in relation to this misuse.¹⁸⁹ This complaint led to a critical report by the ICO, denouncing the considerable interference of MPE with individuals' privacy and requiring better governance and safeguards around its use.¹⁹⁰

MPE Providers: Cellebrite

Like many surveillance tools, MPE tools are rarely developed by governments themselves

181 Ibid.

182 Ibid.

183 Privacy International, 'Digital stop and search: how the UK police can secretly download everything from your mobile phone', <https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile>

184 Logan Koepke et. al., 'Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones, Upturn', 20 October 2020, <https://www.upturn.org/work/mass-extraction/>

185 Aditya Agrawal, 'Exclusive: Delhi Police has tools to extract data from smartphones, including iPhones', MediaNama, 22 December 2020, <https://www.medianama.com/2020/12/223-exclusive-delhi-police-has-tools-extract-data-from-smartphones-iphones/>; Astha Savyasachi, 'Looking Back at the Camera: How Controversial AI Firms Shaped Delhi's Predictive Policing', The Wire: Story, 3 July 2025, <https://pulitzercenter.org/stories/looking-back-camera-how-controversial-ai-firms-shaped-delhis-predictive-policing>

186 Privacy International, 'Use of mobile phone extraction tools by law enforcement in Argentina', <https://privacyinternational.org/news-analysis/5031/use-mobile-phone-extraction-tools-law-enforcement-argentina>

187 Privacy International, 'Mobile Phone Extraction', <https://privacyinternational.org/learn/mobile-phone-extraction>

188 Privacy International, 'Digital stop and search: how the UK police can secretly download everything from your mobile phone', March 2018, pp 2, <https://privacyinternational.org/sites/default/files/2018-03/Digital%20Stop%20and%20Search%20Report.pdf>

189 See: <https://privacyinternational.org/sites/default/files/2018-04/Complaint%20to%20ICO%20about%20Mobile%20Phone%20Extraction%2026th%20April%202018.pdf>

190 Informational Commissioner's Office, 'Mobile phone data extraction by police forces in England and Wales, Investigation report', June 2020, https://ico.org.uk/media/2/migrated/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

and instead procured from various companies including Cellebrite, Oxygen Forensic Detective, and MSAB.¹⁹¹ Israeli company Cellebrite is one of the most prominent companies providing MPE tools.¹⁹² The Universal Forensic Extraction Device (UFED) is one of Cellebrite's MPE tools.¹⁹³ In 2020, Upturn reported that Cellebrite's tools can extract and interpret data from at least 181 apps on the Android operating system and at least 148 apps on Apple iPhones.¹⁹⁴ They also reported that Google apps like Google Maps, Gmail, and Google Photos, dating apps like Tinder, Grindr and OkCupid, Nike+ Run Club, social networks like Facebook, Instagram, Twitter, and Snapchat, web browsers like Chrome and Firefox, and even encrypted messaging apps like Signal and Telegram, can be mined with Cellebrite hardware.¹⁹⁵

The MPE business has amassed millions of US dollars in public and private contracts in more than a hundred countries, including the US, by providing hardware and software for use by law enforcement agencies in criminal investigations.¹⁹⁶ Cellebrite has also been known to provide its tools to governments with poor human rights records including Botswana, Nigeria, Myanmar, Venezuela, Saudi Arabia and Bahrain.¹⁹⁷ Indeed, Cellebrite clients are also reported to include specific national law enforcement agencies which are associated with serious human rights violations, such as the Rapid Action Battalion in Bangladesh.¹⁹⁸ The company has themselves acknowledged that "some of our solutions may be used by customers in a way that is, or that is perceived to be, incompatible with human rights."¹⁹⁹

What can make the use of MPE authoritarian?

MPE is increasingly being used by States for purposes beyond legitimate criminal investigation, including to target human rights defenders (HRDs), political dissidents and journalists, as well as migrants and asylum seekers.²⁰⁰ Furthermore, MPE can be deployed covertly, meaning that governments may have used MPE on a person's device without them even knowing.²⁰¹

Use of MPE against HRDs, activists and political dissidents is often designed to uncover

191 Privacy International, 'A Technical Look at Phone Extraction', October 2019, <https://privacyinternational.org/long-read/3256/technical-look-phone-extraction>

192 Privacy International, Cellebrite, <https://privacyinternational.org/taxonomy/term/584>

193 Cellebrite, "Cellebrite UFED", <https://cellebrite.com/en/products/cellebrite-inseyets/ufed/>

194 Logan Koepke et. al., 'Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones', Upturn, October 2020, <https://www.upturn.org/work/mass-extraction/>

195 Ibid.

196 Diarmaid Harkin et. al., 'Should 'Moral Taint' Be a Factor in Police Technology Procurement? The Case of Cellebrite Open Access', The British Journal of Criminology, 2 August 2025, <https://academic.oup.com/bjc/advance-article/doi/10.1093/bjc/azaf073/8221209>

197 Infogram, 'Cellebrite's abuses around the world', <https://infogram.com/cellebrite-abuses-graph-1h7k2303rwnlv2x>

198 Ode Yaron, 'Israeli Cellebrite Sold Spy-tech to Bangladesh 'Death Squad' ', Haaretz, 9 March 2021, <https://www.haaretz.com/israel-news/tech-news/2021-03-09/ty-article/.highlight/israeli-cellebrite-sold-spy-tech-to-bangladesh-death-squad/0000017f-e592-da9b-a1ff-edff29cf0000>

199 Registration Statement filed with the Securities and Exchange Commission on 17 May 2021 by Cellebrite DI Ltd, pg. 25, https://www.sec.gov/Archives/edgar/data/1854587/000121390021026630/ff42021_cellebriedi.htm

200 A/HRC/48/76, 'Racial and xenophobic discrimination and the use of digital technologies in border and immigration enforcement report of the special Rapporteur on racism', E. Tendayi

Achiume, October 2021, <https://documents.un.org/doc/undoc/gen/g21/379/61/pdf/g2137961.pdf>; Citizenlab, 'Not Safe for Politics: Cellebrite Used on Kenyan Activist and Politician Boniface Mwangi', February 2026, <https://citizenlab.ca/research/cellebrite-used-on-kenyan-activist-and-politician-boniface-mwangi/>

201 Privacy International, 'Mobile Phone Extraction', <https://privacyinternational.org/learn/mobile-phone-extraction>

information and intelligence about them to prosecute them for a variety of crimes associated with dissenting against or opposing the government.²⁰²

In the case of its use against journalists, we are seeing a concerning trend of journalists being arrested and their devices seized and searched, even if they end up not being charged with a crime.²⁰³ This has a chilling effect on journalists' ability to safely and effectively undertake their work and serve their "public watchdog" function, with implications for the free press at a societal level and the right to freedom of expression.²⁰⁴ Such practises may result in self-censorship, and may also lead to fewer sources wanting to speak out to journalists at the risk of being identified.²⁰⁵

Regarding migrants and asylum seekers who have had their device or phone seized for MPE, the technology can isolate them from contact with family and friends when they are already in a vulnerable situation, as well as hinder their access to legal assistance and other support.²⁰⁶ The deployment of such invasive surveillance tools in the context of immigration is extremely problematic and reinforces the hostile environment where those arriving at the border for international protection to exercise their human right to seek asylum are instead treated as having committed a crime.²⁰⁷

The authoritarian ways in which MPE has been used thus extend beyond impacts on privacy. The deployment of this intrusive surveillance technology can undermine a broader range of fundamental rights and freedoms, including freedom of expression, and the freedoms of peaceful assembly and association. Moreover, where its use is targeted against journalists, human rights defenders, political opponents and civil society actors, it risks eroding the rule of law and the democratic values of a free press and meaningful civic participation which we believe may constitute an authoritarian use of the technology.²⁰⁸

Below we outline some of what we believe constitute authoritarian uses of MPE reported by individuals and groups who have been directly affected. However, it is important to note that as governments often have not been completely transparent or forthcoming about the acquisition and use of MPE tools, the examples only reflect what is publicly available and are unlikely to be a true reflection of the extent of this practice by states around the world.

202 Stephanie Kirchgaessner, 'Jordan used Israeli firm's phone-cracking tool to surveil pro-Gaza activists, report finds', The Guardian, 22 January 2026, <https://www.theguardian.com/world/2026/jan/22/jordan-israeli-spyware-gaza-activists>

203 See: Sibylla Brodzinsky, 'Venezuela detains journalists and seizes communication devices after Maduro's removal', The Guardian, 6 January 2026, <https://www.theguardian.com/world/2026/jan/06/venezuela-detains-journalists-after-nicolas-maduros-captured>; National Union of Journalists, NUJ alarmed at ongoing police crackdown of journalists, 28 Oct 2024, <https://www.nuj.org.uk/resource/nuj-alarmed-at-ongoing-police-crackdown-of-journalists.html>

204 A/HRC/62/45, A/HRC/62/45, 'Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', Gina Romero, 21 April 2026, <https://docs.un.org/en/A/HRC/62/45>

205 Ibid.

206 Moha Ennaji, 'Mobile phones: An indispensable tool for migrants', The UNESCO Courier, 21 September 2021, <https://courier.unesco.org/en/articles/mobile-phones-indispensable-tool-migrants>

207 Privacy International, Migrants, <https://privacyinternational.org/learn/migrants>

208 A/HRC/62/45, 'Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', Gina Romero, 21 April 2026, <https://docs.un.org/en/A/HRC/62/45>

Examples of the authoritarian use of MPE

The use of MPE against human rights defenders and activists

In 2016, The Intercept reported that Cellebrite's UFED was used against political activist Mohammed al-Singace who had worked to bring attention to the Bahraini government's mishandling of poverty and inflation.²⁰⁹ Mohammed al-Singace was arrested on 15 May 2013 in **Bahrain** and placed in police custody at which point his phone was seized.²¹⁰ A report on the contents of Singace's phone, prepared by Bahrain's General Directorate of Anti-Corruption and Economic and Electronic Security and generated by Cellebrite's software, was entered as evidence against him during his trial.²¹¹ It contains nearly 20 pages his private WhatsApp conversations. Other court documents show that photos were taken from Singace's phone as well, including several images that were specifically cited during his sentencing as evidence of criminal association.²¹²

In July 2025, prominent **Kenyan** political opposition figure, Boniface Mwangi, was arrested by Kenya's Directorate of Criminal Investigations, which raided his home and office and seized several of his devices, leading to widespread condemnation.²¹³ Authorities only returned the seized devices to him in September, at which point Mwangi noticed his phone's password protection had been removed, despite never having shared the password with authorities.²¹⁴ Forensic analysis by Citizen Lab found signs that Cellebrite's forensic extraction tool was used on the phone around 20–21 of July 2025, while it was in police custody, and attributed this with "high confidence" to Cellebrite's MPE technology, stating that the findings "add to the growing body of evidence that Cellebrite's technology is being abused by its government clients, and the company is failing to prevent those abuses from happening".²¹⁵ The report further called on Cellebrite to suspend services to the relevant Kenyan agencies and conduct an investigation into its technology's implications in rights abuses in Kenya.²¹⁶

An MPE tool provided by Cellebrite was also reportedly used by **Hong Kong** police against Joshua Wong, a pro-democracy activist.²¹⁷ Wong wrote a Facebook post saying the software was used by the Hong Kong Police Forces to hack into his phone.²¹⁸ Wong also shared an online petition started previously by another activist, Kwun Chung Law, with over 36,000 signatories, titled "calling upon Cellebrite to terminate phone hacking cooperations with Hong Kong Police."²¹⁹

209 Sam Biddle and Fahad Desmukh, 'Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident', The Intercept, 8 December 2016, <https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/>

210 Ibid.

211 Ibid.

212 Ibid.

213 CitizenLab, 'Not Safe for Politics Cellebrite Used on Kenyan Activist and Politician Boniface Mwangi', February 2026 <https://citizenlab.ca/research/cellebrite-used-on-kenyan-activist-and-politician-boniface-mwangi/>

214 Ibid.

215 Ibid.

216 Ibid.

217 Mary Hui, 'Hong Kong's mass arrests are giving police crucial intelligence: people's phones', Quartz, 21 July 2022, <https://qz.com/1844937/hong-kongs-mass-arrests-give-police-access-to-phones>

218 Lahav Harkov, 'Hong Kong democracy activists to Israel: Stop exporting tech to police', The Jerusalem Post, 31 July 2020, <https://www.jpost.com/israel-news/hong-kong-democracy-activists-to-israel-stop-exporting-tech-to-police-636918>

219 Ibid.

In 2021, the **Venezuelan** Military Counterintelligence Directorate (DGCIM) broadcast on a state television programme that they would be using Cellebrite's UFED "for the fight against crime," which immediately raised concerns for HRDs due to allegations of DGCIM's involvement in espionage and repression.²²⁰

In 2025, it was reported that Chinese authorities had started using a mobile phone extraction malware named Massistant in order to extract data from seized phones — including texts from apps like Signal, images, location histories, audio recordings, and contacts.²²¹ Massistant required physical access to a device to perform extraction.²²² As of at least 2024, it has been legal in **China** for police conducting a criminal investigation to search individuals' phones and computers without a warrant.²²³

In June 2026, an investigation by Citizen Lab at the Munk School of Global Affairs at the University of Toronto confirmed that **Russian** authorities used Cellebrite's UFED to hack into an iPhone of Andrey Pivovarov, a prominent Russian activist and former political prisoner.²²⁴ Citizen Lab also described a forensic report provided to Pivovarov by the Russian government which states that authorities used UFED to infiltrate several of his devices. This use occurred three months after the company said it was ending sales to Russia "immediately."²²⁵

There are additional concerns of MPE being used against HRDs in the context of protests.²²⁶ For example, in **Lebanon**, CSO SMEX has documented device seizures by security agencies across several protests between 2015 and 2019 as part of a wider crackdown on freedom of expression and assembly.²²⁷

The use of MPE against journalists

Amnesty's Security Lab confirmed that Cellebrite's UFED was used against Slaviša Milanov, a **Serbian** independent investigative journalist.²²⁸ In February 2024, Serbian Slaviša Milanov was arrested and detained by police. While in detention, Slaviša was questioned by officers about his journalism work.²²⁹ Slaviša's Android phone was turned off when he surrendered it to police, and at no point was he asked for, nor did he provide the passcode. After his release, Slaviša noticed that his phone, which he had left at the police station reception

220 Proyecto ITEM, 'Behind the Resale of Cellebrite Technology That Can Hack Your Phone', 20 February 2022, <https://www.itempnews.org/2022/02/20/cellebrite-hacking/>

221 Lorenzo Franceschi-Bicchieri, 'Chinese authorities are using a new tool to hack seized phones and extract data', Tech Crunch, July 2025 <https://techcrunch.com/2025/07/16/chinese-authorities-are-using-a-new-tool-to-hack-seized-phones-and-extract-data/>

222 Ibid.

223 Ibid.

224 John Scott-Railton et. al., 'Russia Breaks into Human Rights Activist's Phone with Cellebrite', Citizen Lab, 25 June 2026, <https://citizenlab.ca/research/russia-breaks-into-human-rights-activists-phone-with-cellebrite/>

225 Ibid.

226 Privacy International, 'How mobile phone extraction can be used at a protest', <https://privacyinternational.org/explainer/4484/how-mobile-phone-extraction-can-be-used-protest>

227 SMEX, 'Device Seizures in Lebanon - Assessing the Legal Framework concerning device seizures in Lebanon', January 2021, <https://smex.org/wp-content/uploads/2021/02/SMEX-Device-Seizures-Report-2021-eng.pdf>

228 Amnesty International, 'Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists', 16 December 2024, <https://www.amnesty.org/en/latest/news/2024/12/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/>

229 Ibid.

during his interrogation, appeared to have been tampered with, and his phone data was turned off. He requested Amnesty to conduct a forensic analysis of his phone. The analysis revealed that Cellebrite's UFED product was used to secretly unlock Slaviša's phone during his detention.²³⁰ Additional forensic evidence showed that NoviSpy was then used by Serbian authorities to infect Slaviša's phone, as use of spyware which we cover in more detail in the following chapter.²³¹

The Committee on the Protection of Journalists (CPJ) has reported many instances of journalists being targeted using MPE²³² including in **Botswana**,²³³ **Nigeria**,²³⁴ and **Ghana**.²³⁵ In these cases, MPE was used to extract information including documents journalists held to identify their sources. Similarly, the Washington Post reported in 2019 that Cellebrite was used against two journalists in **Myanmar**.²³⁶

Seizure and search of mobile devices of two photojournalists in Poland being challenged before the ECtHR

In November 2021, PI and Article 19 intervened in a case before the European Court of Human Rights (ECtHR) which concerned the apprehension of journalists and searches of their phones and cameras close to the Polish Belarusian border.²³⁷ The applicants, Mr Maciej Nabrdalik and Mr Maciej Moskwa, two photojournalists, were apprehended by **Polish** military officers, and their car, phones and cameras were searched.²³⁸ They were later released without charge. The two applicants submitted complaints under the following articles of the European Convention on Human Rights (ECHR):²³⁹

- Article 8 "arguing that the intervention of the military officers and search of their clothes and car as well as their phones and cameras amounted to a violation of their private life and of the right to respect for their correspondence".
- Article 10 of the Convention, "submitting that they were arrested when they were collecting journalistic materials. The military officers checked the contents of their phones and cameras, took photos of their correspondence and pictures, which might

230 Ibid.

231 Ibid.; For more on spyware, see Chapter 3.

232 Committee to Protect Journalists, 'Digital Forensics', <https://cpj.org/tags/digitalforensics/>

233 Jonathan Rozen, 'Botswana police use Israeli Cellebrite tech to search another journalist's phone', Committee to Protect Journalists, 14 July 2021, <https://cpj.org/2021/07/botswana-cellebrite-search-journalists-phone/>

234 Jonathan Rozen, 'Nigerian military targeted journalists' phones, computers with "forensic search" for source', Committee to Protect Journalists, 22 October 2019, <https://cpj.org/2019/10/nigerian-military-target-journalists-phones-forensic-search/>

235 Jonathan Rozen, 'US, UK, Interpol give Ghana phone hacking tools, raising journalist concerns on safety and confidentiality', Committee to Protect Journalists, 14 July 2020, <https://cpj.org/2020/07/us-uk-interpol-give-ghana-phone-hacking-tools-raising-journalist-concerns-on-safety-and-confidentiality/>

236 Timothy McLaughlin, 'Security-tech companies once flocked to Myanmar. One firm's tools were used against two journalists', The Washington Post, 4 May 2019, https://www.washingtonpost.com/world/asia_pacific/security-tech-companies-once-flocked-to-myanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html

237 Privacy International, 'Nabrdalik v Poland', <https://privacyinternational.org/legal-action/nabrdalik-v-poland>; NABRDALIK v. POLAND and 1 other application, 30614/22 30848/22, <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%22001-223550%22%7D>

238 Mapping Media Freedom, 'Three photojournalists detained and handcuffed near Belarusian border, 16 November 2021, <https://www.mapmf.org/alert/24390>

239 NABRDALIK v. POLAND and 1 other application, 30614/22 30848/22, <https://hudoc.echr.coe.int/eng#%7B%22itemid%22%3A%22001-223550%22%7D>

lead to disclosure of confidential sources of information. The officers had also access to potentially fragile data contained in the phones."

It has not yet been confirmed whether the Polish military officers used forensic extraction tools in order to search the applicants' devices, or if they obtained access through other "soft" methods (such as demanding and obtaining the applicants' PIN codes) and copied contents to another device. Whatever method was used, the potential level of intrusion into the applicants' private lives is similarly grave. The case is still pending before the ECtHR at the time of writing.

The use of MPE against migrants

The use of MPE against migrants and asylum seekers as part of immigration enforcement and border management operations is evident in concerning policies and practices.²⁴⁰

In the **US**, Immigration and Customs Enforcement (ICE) have reportedly had contracts with Cellebrite for several years,²⁴¹ and the use of MPE has been alleged as a core tactic deployed by ICE under the Trump administration, as part of wider plans to crackdown on irregular migrants.²⁴² The 2026 report *The Tech behind ICE*, detailed that the Swedish forensic company, MSAB, "supplies ICE with its XRY mobile extraction tools", and collaborated with another private company called Berla whose Berla iVe vehicle forensics system accesses and analyses vehicle information, to create a unified platform "for extracting and analysing data from both vehicles and mobile devices."²⁴³ In 2025, U.S. Customs and Border Patrol renewed its commitment to the MPE technology with three separate contract awards.²⁴⁴

The seizure, confiscation and search of electronic devices of migrants arriving by small boats to the United Kingdom

A legal case was brought against the **UK** Home Office's for their secret and blanket practice of seizing and searching devices of migrants arriving in the UK by small boats between April and November 2020.²⁴⁵ The case revealed that migrants were searched on arrival at Tug Haven in Dover and compelled to hand over their mobile phones and provide their PIN numbers.

240 D.G. Niruka Sanjeevani, 'The Use of Mobile Data in the European Asylum System', *Borders Criminologies*, 7 November 2025, <https://blogs.law.ox.ac.uk/border-criminologies-blog/blog-post/2025/11/use-mobile-data-european-asylum-system> ; Stephan Scheel, 'Epistemic domination by data extraction: questioning the use of biometrics and mobile phone data analysis in asylum procedures', *Journal of Ethnic and Migration Studies* (2024), <https://pmc.ncbi.nlm.nih.gov/articles/PMC11034547/>

241 Marcus Gilmer, 'Hacking firm Cellebrite's newest agreement is with ICE', *Mashable*, 12 September 2019, <https://mashable.com/article/cellebrite-hack-tools-ice-border>

242 Center for Constitutional Rights, 'Legal Groups Sue Trump Administration to Uncover Use of Israeli Spyware Tools on U.S. Communities', 30 October 2025, <https://ccrjustice.org/home/press-center/press-releases/legal-groups-sue-trump-administration-uncover-use-israeli-spyware>

243 Mijente, Just Futures Law, and Surveillance Resistance Lab, 'The Tech Behind ICE: Oligarchs, Immigration Enforcement, and the Threat to Democracy', June 2026 <https://notechforice.com/wp-content/uploads/2026/06/Tech-Behind-ICE-Oligarchs-Immigration-Enforcement-and-the-Threat-to-Democracy.pdf>

244 Mijente, Just Futures Law, and Surveillance Resistance Lab, 'The Tech Behind ICE: Oligarchs, Immigration Enforcement, and the Threat to Democracy', June 2026 <https://notechforice.com/wp-content/uploads/2026/06/Tech-Behind-ICE-Oligarchs-Immigration-Enforcement-and-the-Threat-to-Democracy.pdf>

245 Gold Jennings Solicitors, 'High Court to hear asylum seekers' challenge to Home Secretary's policy of seizing mobile phones from boat arrivals and extracting data', 25 January 2022, <https://goldjennings.co.uk/high-court-to-hear-asylum-seekers-challenge-to-policy-of-seizing-mobile-phones-from-boat-arrivals-and-extracting-data/>

The Home Office justified the seizure under section 48 of the Immigration Act (IA) 2016, noting that the phones were “believed to contain evidence in relation to immigration offences”.²⁴⁶ However, the High Court confirmed that this provision does not authorise a search of individuals and is confined to the search of premises. The Court concluded that it was for Parliament to provide the power for seizing and searching mobile devices, and not a power the Home Office could assume.²⁴⁷

The substantive judgment was handed down on 25 March 2022, in which the High Court found that the secret and blanket policy of the **UK** Home Office to seize and search migrants’ phones breached Article 8 of the ECHR and UK data protection laws.²⁴⁸ In a judgment of 14 October 2022²⁴⁹, the UK High Court ordered the UK Home Office to provide remedy to the thousands of migrants affected by its unlawful policy and practice of seizing mobile phones from people arriving by small boats to UK shores.²⁵⁰

Despite this positive outcome, there remain concerns that such a practice is ongoing. These concerns are substantiated by the empowerment of immigration officers to seize and extract information from electronic devices under the Police, Crime, Sentencing and Courts Act 2022²⁵¹ and more recently the inclusion of similar powers in the Border Security, Asylum and Immigration Act 2025.²⁵²

Attempt by German government to use MPE to gather data to verify identity of asylum seekers deemed unlawful

In **Germany**, legal action was brought against the Federal Office for Migration and Refugees (“BAMF”), to challenge the extraction and analysis of asylum seekers’ phones in order to verify their identity.²⁵³ Such extraction became authorised in July 2017 under Section 5 of the Asylum Act (Asylgesetz, AsylG), requiring asylum seekers to surrender all data carriers if they are unable to produce a valid passport.²⁵⁴ The Berlin Administrative Court, affirmed on appeal by the Federal Administrative Court, held that BAMF is not allowed to access

246 HM & Ors, R. (On the Application Of) [2022] EWHC 2729 (Admin) (14 October 2022), <https://www.bailii.org/ew/cases/EWHC/Admin/2022/2729.html>, para. 15.

247 Privacy International, ‘UK High Court rules blanket seizure of asylum seekers’ phones breached article 8 ECHR’ <https://privacyinternational.org/news-analysis/4810/uk-high-court-rules-blanket-seizure-asylum-seekers-phones-breached-article-8>

248 HM, R (On the Application Of) v Secretary of State for the Home Department [2022] EWHC 695 (Admin) (25 March 2022) <https://www.bailii.org/ew/cases/EWHC/Admin/2022/695.html>

249 HM & Ors, R. (On the Application Of) [2022] EWHC 2729 (Admin) (14 October 2022), <https://www.bailii.org/ew/cases/EWHC/Admin/2022/2729.html>

250 Privacy International, ‘UK High Court orders groundbreaking redress for thousands of migrants affected by unlawful phone seizures and data extraction’, 18 November 2022, <https://privacyinternational.org/news-analysis/4987/uk-high-court-orders-groundbreaking-redress-thousands-migrants-affected-unlawful>

251 Police, Crime, Sentencing and Courts Act 2022, <https://www.legislation.gov.uk/ukpga/2022/32/part/2/chapter/3>

252 Border Security, Asylum and Immigration Act 2025, <https://www.legislation.gov.uk/ukpga/2025/31/contents>, sections 23 and 24.

253 Francesca Palmiotto and Derya Ozkul, ‘Like Handing My Whole Life Over’ The German Federal Administrative Court’s Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures’, 28 February 2023, <https://verfassungsblog.de/like-handing-my-whole-life-over/>

254 Gesellschaft für Freiheitsrechte e.V., ‘Race, Borders, and Digital Technology: Submission to the Office of the United Nations High Commissioner for Human Rights on the Reinforcing, Reproductive and Compounding Effects of the Deployment of Digital Technologies in the context of Border Enforcement and Administration’, May 2020, https://www.ohchr.org/sites/default/files/Documents/Issues/Racism/SR/RaceBordersDigitalTechnologies/Gesellschaft_fur_Freiheitsrechte.pdf

information on a mobile phone unless they have a good reason, and that authorities must first examine whether less intrusive means of establishing identity are available.²⁵⁵ Despite the existence of a purpose-made legal framework to authorise the search and analysis of asylum seekers' phones, the national courts found that searching asylum seekers' phones required a "good reason to do so", and that in this case it was disproportionate and therefore unlawful.²⁵⁶

Human rights and data protection implications

The use of MPE is highly intrusive and raises a host of human rights and data protection concerns. When coupled with contexts such as those laid out above, including individuals' heightened vulnerability, pre-existing abusive state practises, or the absence of effective legal safeguards or regulation, the technology's use is at serious risk of being authoritarian. The use cases presented in this chapter illustrate the impact that MPE can have on individuals and exemplify serious concerns that this technology is being used in a targeted manner against specific minority groups and those who dissent. Some courts and regulators have highlighted that MPE is an intrusive tool, and that it must be effectively regulated to ensure people's rights are protected.

In 2020, the ICO published a report on MPE use in England and Wales highlighting that MPE constitutes a considerable interference with individuals' privacy "through excessive processing of data held or accessed through the phone".²⁵⁷ This was followed by a similar report on Northern Ireland²⁵⁸ and Scotland²⁵⁹, and an updated report on England and Wales in 2021²⁶⁰. The findings revealed a widespread use of MPE by police forces in the UK, including that not all had undertaken DPIAs, and that data retention policies were unclear. The ICO then undertook a project to assess the extent to which police forces had implemented the recommendations from their previous reports and to ascertain whether they had adopted them into operational practice.²⁶¹ The efforts of the ICO to sustain its scrutiny of the use of MPE is an important indication of its concerns regarding the use of this technology.

In line with such concerns raised by regulators, decisions of courts in the UK and Germany have recognised that certain uses of MPE in the context of asylum are disproportionate

255 InfoMigrants, 'German court rejects phone searches of asylum seekers', 16 February 2023, <https://www.infomigrants.net/en/post/46897/german-court-rejects-phone-searches-of-asylum-seekers>

256 Ibid.

257 Informational Commissioner's Office, 'Mobile phone data extraction by police forces in England and Wales, Investigation report', June 2020, https://ico.org.uk/media2/migrated/2617838/ico-report-on-mpe-in-england-and-wales-v1_1.pdf

258 Informational Commissioner's Office, 'Mobile phone data extraction by police in Northern Ireland, Investigation report', June 2021, <https://ico.org.uk/media2/migrated/2620094/ico-investigation-mpe-northern-ireland-202106.pdf>

259 Informational Commissioner's Office, 'Mobile phone data extraction by police in Scotland, Investigation report', June 2021, <https://ico.org.uk/media2/migrated/2620095/ico-investigation-mpe-scotland-202106.pdf>

260 Informational Commissioner's Office, 'Mobile phone data extraction by police forces in England and Wales, An update on our findings', June 2021, <https://ico.org.uk/media2/migrated/2620093/ico-investigation-mpe-england-wales-202106.pdf>

261 Informational Commissioner's Office, 'Findings from ICO reviews of mobile phone data extraction by police forces in the United Kingdom', May 2024, <https://ico.org.uk/media2/migrated/4029444/mpe-outcomes-report.pdf>

interferences with the right to privacy.²⁶² At a regional level, it is notable that in 2024, the Court of Justice of the European Union recognised that police access to the data contained on a mobile phone is liable to constitute a “serious, or even particularly serious” interference with the rights to privacy and the protection of personal data.²⁶³

In the US, the Supreme Court in the case of *Riley v California*²⁶⁴ one of the first cases worldwide to explore the use of MPE evidence in law enforcement, observed how mobile phones “differ in both a quantitative and a qualitative sense from other objects”, in particular given that: information is collected in one place, it provides the capacity to convey more, and the timeframe that it would cover which could date as far back as the moment of purchase of the device.²⁶⁵ When delivering his opinion to the Court, Chief Justice Roberts commented on the vast volumes of data that can be extracted as well as the sensitive nature of it:

*“The term “cell phone” is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.”*²⁶⁶

*“...a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form— unless the phone is.”*²⁶⁷

Concerns over the human rights implications of MPE use have also been raised by international bodies, including the UN. The UN Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, has highlighted that the practice of seizing “mobile phones from asylum or migration applicants, from which data are then extracted and used as part of asylum procedures.... constitute a serious, disproportionate interference with migrants’ and refugees’ right to privacy, on the basis of immigration status and, in effect, national origin.”²⁶⁸

More broadly, the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association noted that the use of digital technologies should comply with international human rights law and would require “an assessment of all human rights implications, including less visible impacts, such as the creation of any chilling effects that affect the free participation and exercise of fundamental freedoms in online and offline spaces, as

262 InfoMigrants, ‘German court rejects phone searches of asylum seekers’, 16 February 2023, <https://www.infomigrants.net/en/post/46897/german-court-rejects-phone-searches-of-asylum-seekers> ; See also: HM, R (On the Application Of) v Secretary of State for the Home Department [2022] EWHC 695 (Admin) (25 March 2022) <https://www.bailii.org/ew/cases/EWHC/Admin/2022/695.html>

263 Court of Justice of the European Union (CJEU), Case C-548/21, CG v Bezirkshauptmannschaft Landeck, 2024, <https://eur-lex.europa.eu/legal-content/EN/SUM/?uri=celex%253A62021CJ0548>

264 573 US 373 (2014), <https://supreme.justia.com/cases/federal/us/573/373/>

265 See: *Riley v. California*, 573 U.S. 373 (2014). <https://supreme.justia.com/cases/federal/us/573/373/>

266 See: *Riley v. California*, 573 U.S. 373 (2014), p 17

267 Ibid, p 21

268 A/75/590, Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance prepared pursuant to General Assembly resolution 74/137, E. Tendayi Achiume, 10 November 2020, para. 27, <https://docs.un.org/en/A/75/590>

well as any actions that are discriminatory or bear an adverse psychological impact on individuals.”²⁶⁹

With respect to data protection implications of MPE use, the data subject rights of all individuals, not just the owner or user, whose data is contained within a target device could potentially be put at risk by this technology’s use. This is due to the fact that MPE technology is often unable to discern between data types within a device and instead carries out blanket mass data collection of large quantities of personal data that the device contains.²⁷⁰ Such blanket collection risks undermining the data protection principle of proportionality, since not all data in a device will always be necessary to collect in order to investigate a particular crime. This data could also be subject to legal privilege or be special category sensitive data regarding an individuals’ health, political or religious opinion, sexuality, biometric information, race or ethnic origin – making it much more liable to cause harm if that data were to be exploited – and thus should normally be subject to additional robust safeguards to allow it to be processed safely.²⁷¹

Conclusion

As this chapter outlines, MPE is increasingly being used for purposes other than lawful criminal investigations. Instead, we are seeing a trend in MPE being deployed as a tool to gather information and intelligence about activists, journalists, political dissidents, and migrants, which we believe to constitute an authoritarian use of the technology.

Below we outline the necessary safeguards and restrictions that we recommend should be followed when using MPE, to enable it to be legitimately deployed in a way that complies with human rights law and data protection law and standards.

- MPE should only ever be used to investigate individuals who have been lawfully arrested for serious crimes, not including purported political crimes related to peaceful dissent, that have been or are suspected as having been committed;
- MPE should never be used:
 - As a blanket policy, especially against a vulnerable group such as migrants;
 - To identify whistleblowers, journalists or journalistic sources;
 - To categorise people by protected characteristics;
 - To identify protesters or to collect information on people attending peaceful assemblies; and
 - To intentionally suppress the rights to expression or assembly.
- The use of MPE should be explicitly regulated and overseen by a **robust legal and regulatory framework** which ensures:
 - Its use must be based on reasonable suspicion that a serious offence has been committed;
 - Its use must be both necessary and proportionate to the aim pursued;
 - Its use must be subject to prior judicial authorisation (e.g. a warrant);

269 A/HRC/55/60, Model Protocol for Law Enforcement Officials to Promote and Protect Human Rights in the Context of Peaceful Protests, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Clément Nyaletsossi Voule, 31 January 2024, para. 61, <https://docs.un.org/en/A/HRC/55/60>

270 See “How does MPE work?” above.

271 Privacy International, ‘A Guide for Policy Engagement on Data Protection: Data Protection Principles’, <https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf>

- Its use must be in accordance with a pre-established national legislative and regulatory framework designed to protect privacy and ensure data protection;
 - Individuals whose devices are subject to MPE have the right to be informed of circumstances in which their mobile phones may be seized and searched, and provided information as to how that will be done, what the information will be used for, and who it will be shared with; and
 - Regular and published independent audits of MPE use.
- More broadly, the use of MPE should be overseen by an independent national oversight body (e.g. data protection authority, inspector general, parliamentary committee) with the power to hear and respond to complaints from members of the public, to conduct its own investigations with authorised to access the necessary information, to compel disclosure and to impose remedies and penalties;
- The **safe procurement** of MPE tools by state authorities must be subject to the following:
 - Open and transparent processes, which include the *prior* and systematic conduct of human rights and data protection due diligence both regarding the MPE technology and the vendor;
 - Procurement contracts include binding human rights clauses (not just aspirational language) with audit and termination rights if misuse is suspected;
 - Budget and contract value disclosed through normal public procurement transparency channels; and
 - Consultation with civil society representatives of potentially affected communities *prior* to large scale procurement.
- Export laws should require private companies that export MPE to undertake impact assessments of their potential clients to assess the human rights and data protection risks of supplying their products and services to a given client, and should prevent exportation if high risks of misuse are found in these assessments.



03 Spyware.

Introduction

Spyware can fall clearly within this report's definition of the "authoritarian use of technology" owing to how it can be used to exert control, erode democratic norms, and unjustifiably infringe upon human rights. While typically marketed as a counterterrorism and crimefighting tool, spyware has been repeatedly deployed by both authoritarian and democratic governments to conduct secret, intrusive surveillance of journalists, human rights defenders, opposition politicians, their family members and other individuals already at risk of state repression.²⁷² By covertly invading personal devices and collecting large quantities of private personal information without knowledge, consent or oversight, spyware use is extremely intrusive and severely limits the safe exercise of fundamental rights such as privacy, freedom of expression, and freedom of association among others.

The impact of spyware extends far beyond its individual targets - it creates a broader climate of fear and self-censorship, producing a "chilling effect" on entire communities and civic spaces.²⁷³ People become less willing to speak out, organise, or participate in democratic processes when they know their communications may be secretly monitored. This in turn has a corrosive effect on democratic institutions and human rights protections, not only silencing dissenting voices but also undermining trust in the rule of law and accountability mechanisms. The fact that spyware's use is often incompatible with human rights law reinforces its role as a tool of authoritarian control.²⁷⁴ Instead of serving public safety, spyware technologies are too often used to target, persecute, or ostracise - making them a clear and urgent example of the authoritarian use of technology as defined in this report.

What is spyware?

Spying software which relies on vulnerabilities in systems to access them, known as spyware, is a type of malware. Malware (short for "malicious software") describes any form software or code that exists to cause damage, disruption or compromise data confidentiality, integrity, or availability.

Spyware is secretly installed on an internet-connected device, such as a mobile phone, tablet, smartwatch or laptop, without the user's knowledge or consent. Once installed, the spyware facilitates remote unauthorised access for the purposes of surveillance, or covert collection and extraction of data. Spyware can transfer (often for profit) the collected data to a third party and may also enable remote monitoring or control of the targeted device, including covertly turning on cameras and microphones.

272 A/HRC/51/17, The right to privacy in the digital age report of the Office of the United Nations High Commissioner for Human Rights, 4 August 2022, para. 24–39, <https://docs.un.org/A/HRC/51/17>

273 Ibid., para. 10 and 24–30.

274 See "What makes the use of spyware authoritarian?" and "Human Rights and Data Protection Concerns" in this Chapter. See also: European Data Protection Supervisor, 'Preliminary Remarks on Modern Spyware', February 2022, https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

Council of Europe Commissioner for Human Rights, 'Highly intrusive spyware threatens the essence of human rights', The Council of Europe, 27 January 2023 https://www.coe.int/en/web/commissioner/blog/2023/-/asset_publisher/aa3hyf8wKBn/content/highly-intrusive-spyware-threatens-the-essence-of-human-rights

How does spyware work?

The use of spyware can enable extraordinarily intrusive surveillance. Spyware can access a vast range of sensitive personal data that a target device contains, including text and other messages (including those sent through encrypted apps like Signal and WhatsApp), contact lists, emails, photographs, videos, audio messages and recording, stored notes and documents, as well as passwords, browsing history, browsing habits, login credentials, user keyboard strokes, geolocation information and financial information such as credit card details, bank account details and personal identification number (PIN) codes.²⁷⁵

Beyond merely being able to access and obtain massive quantities of personal data from an infected device, spyware's unique and pernicious nature is further characterised by its ability to exercise control, effectively transforming target device into a 24/7 surveillance tool.²⁷⁶ For example, spyware may be able to secretly:²⁷⁷

- Control a device's microphone to take recordings;
- Control a device's camera to take photographs or videos;
- Track geolocation using the device's internal global positioning system (GPS) trackers; and
- Access a device's list of contacts and modify them.²⁷⁸

Spyware works by infiltrating and then infecting devices remotely (with no physical access required) and without any detection. There are a broad range of ways that spyware may succeed in this infiltration, some of which are prompted by an action from the device's unwitting user, such as clicking on a link, accepting a cookie request or pop up, or downloading content such as apps, games or videos.²⁷⁹ Usually the malicious software is hidden within, or masquerading as, benign content.

However, it is also possible for spyware to infect a device completely unprompted and without any interaction from the device user. This type of spyware was made notorious by the Pegasus scandal and is famously known to gain access via zero-click exploits. The receipt of an iMessage, for example, is enough.²⁸⁰ Often, spyware infiltrates by combining zero-click exploits with zero-day exploits,²⁸¹ which are vulnerabilities in a device previously unknown to the developer, vendor or the public at large. Use of zero-day exploits has security as well as privacy implications as the failure to disclose and patch these vulnerabilities leaves all users of the affected systems at risk.

275 Privacy International, "Hacking Necessary Safeguards", n.d., <https://privacyinternational.org/demand/government-hacking-safeguards>

National Institute of Standards and Technology, Computer Security Resource Centre, 'Spyware', <https://csrc.nist.gov/glossary/term/spyware>; Fortinet, 'What is Spyware?', <https://www.fortinet.com/uk/resources/cyberglossary/spyware>; RSI Security, 'How to detect Pegasus spyware', 1 April 2025, <https://blog.rsisecurity.com/how-to-detect-pegasus-spyware/>

276 Stephanie Kirchgaessner, 'Ice obtains access to Israeli-made spyware that can hack phones and encrypted apps', The Guardian, September 2025 <https://www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware>

277 Fortinet, 'What is Spyware?', <https://www.fortinet.com/uk/resources/cyberglossary/spyware>

278 McAfee, 'Mobile Spyware: How Hackers Can Turn Your Phone Into a Stalking Machine', 19 July 2023, <https://www.mcafee.com/blogs/mobile-security/mobile-spyware/>

279 Fortinet, 'What is Spyware?', <https://www.fortinet.com/uk/resources/cyberglossary/spyware>

280 Ibid.

281 Privacy International, "Exploiting Privacy: Surveillance Companies Pushing Zero-Day Exploits", February 2018, <https://privacyinternational.org/blog/1245/exploiting-privacy-surveillance-companies-pushing-zero-day-exploits>

Usually, it is extremely difficult to know whether a device has been infected with spyware. Most victims remain unaware, unless their device undergoes forensic or other specialised analysis. In recent years, self-help online tools have been developed to assist individuals in attempts to ascertain whether or not they have been targeted, such as Amnesty International's Mobile Verification Toolkit.²⁸² Solutions that have been recommended for spyware-infected devices include to stop using the device, buy a new device and change all passwords for all connected accounts, indicating that the level of damage and penetration by the malware amounts to rendering the device effectively unusable.²⁸³

What makes the use of spyware authoritarian?

Spyware is a highly intrusive form of surveillance and its human rights implications are severe. They attain such a level of seriousness that the European Data Protection Supervisor stated that spyware tools constitute "a level of intrusiveness that is incomparable with what we have seen before, with features capable to render many of the existing legal and technical safeguards ineffective and meaningless."²⁸⁴ The Council of Europe's (CoE) Commissioner for Human Rights stated that the technology posed such an existential threat to the "fundamental right to privacy [...] that it risks obliteration".²⁸⁵ Equally, UN Special Procedures called for a global moratorium on the sale and transfer of "life threatening" spyware technology.²⁸⁶

Examples of the authoritarian use of spyware

The global spyware market is vast, opaque and complex. Spyware can be developed in-house, for example by a government, or more commonly it is purchased. An Atlantic Council 2024 report that mapped the spyware market across 42 countries, found that at least 80 of the 195 countries in the world are known to have procured commercial spyware, and another report found that commercial spyware vendors (CSVs) accounted for 64% of the exploitation of mobile and browser vulnerabilities in 2023.²⁸⁷

The Atlantic Council report found a high concentration of global spyware companies in Israel, India and Italy, with Israel hosting by far most of the CSVs analysed, in line with its

282 Amnesty International, 'GitHub, "mvt-project/mvtL MVT (Mobile Verification Toolkit)', <https://github.com/mvt-project/mvt>

283 Reporters Sans Frontières, 'RSF's recommendations for those who could be spied on by Pegasus, 23 July 2021, <https://rsf.org/en/rsf-s-recommendations-those-who-could-be-spied-pegasus>

284 European Data Protection Supervisor, 'Preliminary Remarks on Modern Spyware', February 2022 https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

285 Council of Europe Commissioner for Human Rights, 'Highly intrusive spyware threatens the essence of human rights', The Council of Europe, 27 January 2023, <https://www.coe.int/en/web/commissioner/blog/2023/-/asset-publisher/aa3hyyf8wKBn/content/highly-intrusive-spyware-threatens-the-essence-of-human-rights>

286 UN Special Procedures Joint Mandates, 'Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech', August 2021, <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening>

287 Jen Roberts, Trey Herr, Nitansha Bansal, and Nancy Messieh, with Emma Taylor, Jean Le Roux, and Sopo Gelava, 'Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights', Atlantic Council, 4 September 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/#executive-summary>; Google, 'We're all in this together: A year in review of zero-days exploited in-the-wild in 2023', pg. 15, March 2024, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Year_in_Review_of_ZeroDays.pdf

reputation as the world's largest global spyware exporter.²⁸⁸ In the European Union, 14 of the 27 countries purchased spyware from just one company - NSO Group.²⁸⁹

NSO Group and The Pegasus Scandal

The Israeli firm, NSO Group, rose to international notoriety in the wake of the Pegasus scandal when they were implicated in a plethora of human rights violations worldwide.²⁹⁰ The Pegasus Project, an investigation published in 2021 by an international consortium of media outlets, exposed the widespread misuse of military-grade²⁹¹ spyware named "Pegasus", developed by NSO Group.²⁹²

The revelations consisted of the publication of a leaked database of more than 50,000 phone numbers allegedly selected as potential surveillance targets by governments using NSO Group's Pegasus spyware.²⁹³ Whilst NSO Group has stated the spyware is intended for uses of counterterrorism and crime fighting,²⁹⁴ the Pegasus software was found to have been subject to mission creep and had been reportedly used by governments to secretly surveil "persons of interest" including journalists, activists, opposition politicians, lawyers, civil society actors and even world leaders, sparking concerns over widescale human rights violations and unchecked use of the surveillance technology.²⁹⁵ A leaked list of potential targets included 14 heads of state, such as Imran Khan of Pakistan and Emmanuel Macron of France.²⁹⁶

288 Ibid; Mariav Zonszein, 'Review: Why Israel tests its spyware on Palestinians', Chatham House, 22 November 2023 <https://www.chathamhouse.org/publications/the-world-today/2023-06/review-why-israel-tests-its-spyware-palestinians>

289 Jen Roberts, Trey Herr, Nitansha Bansal, and Nancy Messieh, with Emma Taylor, Jean Le Roux, and Sopo Gelava, 'Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights', Atlantic Council, 4 September 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/#executive-summary>

290 This research has uncovered widespread, persistent and ongoing unlawful surveillance and human rights abuses perpetrated using NSO Group's Pegasus spyware in a report covering 10 countries, see: Amnesty International, 'Forensic Methodology Report: How to catch NSO Group's Pegasus', July 2021 <https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/>

291 Federico Guerrini, 'Pegasus Spyware Scandals Highlight Global Dangers as Activists Demand Action', Forbes, September 2023, <https://www.forbes.com/sites/federicoguerrini/2023/09/14/pegasus-spyware-scandals-highlight-global-dangers-as-activists-demand-action/>

292 Stephanie Kirchgaessner, Paul Lewis, David Pegg, Sam Cutler, Nina Lakhani and Michael Safi, 'Revealed: leak uncovers global abuse of cyber-surveillance weapon', The Guardian, 18 July 2021, <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>

293 Ibid.

294 Shalev Hulio NSO Technologies CSO, Letter to UN Special Rapporteur Mr David Kaye, December 2019, <https://www.documentcloud.org/documents/24766245-downloadfile/>

295 Amnesty International, 'Pegasus Project: Macron among world leaders selected as potential targets of NSO spyware', 20 July 2021, <https://www.amnesty.org/en/latest/press-release/2021/07/world-leaders-potential-targets-of-nso-group-pegasus-spyware/>; Council of Europe's Parliamentary Assembly (PACE) report, 'Pegasus and similar spyware and secret state surveillance', September 2023, <https://pace.coe.int/en/files/33018/html>; UN Special Procedures Mandates, 'Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech', August 2021 <https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening>; European Parliament, 'Draft Recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware', May 2023 https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html

296 Amnesty International, 'Pegasus Project: Macron among world leaders selected as potential targets of NSO spyware', 20 July 2021, <https://www.amnesty.org/en/latest/press-release/2021/07/world-leaders-potential-targets-of-nso-group-pegasus-spyware/>

Legal cases were initiated in jurisdictions around the world in light of the revelations, as well as official inquiries ordered by the Supreme Court in India²⁹⁷ and in France.²⁹⁸ The revelations included targets in over 50 countries and over 200 journalists, including from CNN, the New York Times, Reuters, AP, France 24, the Financial Times and Al Jazeera.²⁹⁹ Clients included Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda and Saudi Arabia.³⁰⁰

In 2020, PI co-joined as amici curiae in the lawsuit brought in the USA by WhatsApp against NSO Group for using its servers to target individuals.³⁰¹ The case culminated in a 2025 decision that NSO Group had unlawfully targeted WhatsApp's users with its spyware.³⁰² The six-year-long case revealed that NSO Group (rather than its clients) was directly responsible for operating the spyware, including installing it on target devices and using it to extract data.³⁰³ In May 2025 at the culmination of the case, a jury imposed \$167,254,000 in punitive damages and close to half a million dollars in compensatory damages on NSO Group;³⁰⁴ however in October a federal judge significantly reduced the punitive damages to just \$4 million.³⁰⁵

NSO Group, however, is just one of many hundreds if not thousands of corporate entities worldwide that develop, vend and market this highly invasive technology,³⁰⁶ which is too often used for autocratic purposes.

297 Amrit Dillon and Michael Safi, 'Indian supreme court orders inquiry into state's use of Pegasus spyware', The Guardian, 27 October 2021, <https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware> ;

Reporters Sans Frontières, 'Pegasus judicial proceedings in France offer only possibility of justice', 18 July 2022 <https://rsf.org/en/pegasus-judicial-proceedings-france-offer-only-possibility-justice>

298 Reporters without Borders, 'Pegasus judicial proceedings in France offer only possibility of justice', 18 July 2022, <https://rsf.org/en/pegasus-judicial-proceedings-france-offer-only-possibility-justice>

299 BBC, 'Pegasus: Spyware sold to governments 'targets activists'', 19 July 2021, <https://www.bbc.co.uk/news/technology-57881364>; Reporters Sans Frontières, "Pegasus judicial proceedings in France offer only possibility of justice", 18 July 2022 <https://rsf.org/en/pegasus-judicial-proceedings-france-offer-only-possibility-justice>

300 Kali Robinson, 'How Israel's Pegasus Spyware Stoked the Surveillance Debate', Council on Foreign Relations, 8 March 2022, <https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate>

301 Brief of Access Now, Amnesty International, Committee to Protect Journalists, Internet Freedom Foundation, Paradigm Initiative, Privacy International, Red En Defensa De Los Derechos Digitales, and Reporters Without Borders As Amici Curiae in support of Appellees' Request for Affirmance, December 2020, <https://www.accessnow.org/wp-content/uploads/2020/12/2020-12-22-AccessNow-Amicus-Brief13845453.1.pdf>

302 Amnesty International, 'Global: Ruling against NSO Group in Whatsapp case a "momentous win in fight against spyware abuse"', 7 May 2025, <https://www.amnesty.org/en/latest/news/2025/05/ruling-against-nso-group-in-whatsapp-case-a-momentous-win/>

303 Stephanie Kirchgaessner, 'NSO – not government clients – operates its spyware, legal documents reveal', The Guardian, 15 November 2024, <https://www.theguardian.com/technology/2024/nov/14/nso-pegasus-spyware-whatsapp>

304 Lorenzo Franceschi-Bicchieri, 'NSO Group must pay more than \$167 million in damages to WhatsApp for spyware campaign', TechCrunch, 6 May 2025 <https://techcrunch.com/2025/05/06/nso-group-must-pay-more-than-167-million-in-damages-to-whatsapp-for-spyware-campaign/>

305 Anton Mous, 'Federal judge reduces fine for spyware company NSO Group from \$167M to \$4M', Cybernews, 21 October 2025 <https://cybernews.com/news/nso-group-whatsapp-fine-reduced/>

306 Jen Roberts, Trey Herr, Nitansha Bansal, and Nancy Messieh, with Emma Taylor, Jean Le Roux, and Sopo Gelava, 'Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights', Atlantic Council, 4 September 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/#executive-summary>

2.b. Country Examples

Europe: Poland, Greece, Serbia and the EU Parliament PEGA Inquiry

In Europe, spyware has been deployed not as a narrow crime-fighting tool but as a mechanism of control, targeting journalists, political opponents, and civil society.³⁰⁷ Indeed, in 2023 the European Parliament's PEGA inquiry (launched in response to the Pegasus Project) condemned **Poland** and **Hungary** for "major violations of EU law", for dismantling oversight institutions and deploying spyware as part of a systemic strategy to surveil and intimidate political opposition, silence critical media and manipulate elections.³⁰⁸ In Poland alone, prosecutors revealed that between 2017 and 2022, Pegasus spyware had been used against 578 people across three state agencies, revealing "enormous knowledge" of the private and professional lives of those targeted.³⁰⁹

In **Greece**, the Predator spyware scandal exposed attempts to compromise devices belonging to government ministers, senior military officers, and critics, whereby the devices of at least 87 individuals were flagged by the Hellenic Data Protection Authority, and in 27 of those cases the same people were also under conventional surveillance by Greece's National Intelligence Service; overlaps which strongly suggest coordination or shared targeting between spyware actors and the state security apparatus.³¹⁰ The political fallout included resignations of intelligence heads and new legislation expanding state surveillance powers.³¹¹ The case has since gone to Greek courts with two Israeli and two Greek former executives of Intellexa, the Greek company that marketed Predator spyware, being criminally charged in Athens for the "violation of telephone communication secrecy".³¹²

In Serbia, authorities have employed spyware to surveil journalists, activists, and civil society actors in ways that breach procedural norms and human rights standards. Amnesty International documented how mobile forensic products, as discussed in the previous chapter on MPE, were used to unlock phones without proper legal process, and then domestic spyware named NoviSpy was allegedly installed while the devices were in police custody or during questioning.³¹³

307 European Parliament, 'Draft Recommendation to the Council and the Commission following the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware', May 2023 https://www.europarl.europa.eu/doceo/document/B-9-2023-0260_EN.html;

308 European Parliament, 'Spyware: MEPs sound alarm on threat to democracy and demand reforms', Press release, 8 May 2023 <https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democracy-and-demand-reforms>

309 AP and Euronews, 'Shocking and depressing': Polish minister says government used spyware against hundreds of people', 25 April 2024, <https://www.euronews.com/next/2024/04/25/shocking-and-depressing-polish-minister-says-government-used-spyware-against-hundreds-of-p>

310 Emre Çitak, 'Greece used Predator spyware on ministers and military', Dataconomy, 24 September 2025, <https://dataconomy.com/2025/09/24/greece-used-predator-spyware-on-ministers-and-military/>

311 Ibid.

312 Hurriyet Daily News, 'Wiretapping scandal goes to court in Greece', 24 September 2025, <https://www.hurriyetdailynews.com/wiretapping-scandal-goes-to-court-in-greece-213959>

313 Amnesty International, 'Serbia: Authorities using spyware and Cellebrite forensic extraction tools to hack journalists and activists', 16 December 2024, <https://securitylab.amnesty.org/latest/2024/12/serbia-a-digital-prison-spyware-and-cellebrite-used-on-journalists-and-activists/>

The PEGA inquiry, to which PI made a submission,³¹⁴ revealed the wide abuse of spyware across EU Member States, often without legal justification or adequate oversight. It found serious human rights violations, including breaches of privacy, data protection, and freedom of expression, alongside a lack of transparency, judicial control, and effective remedies for victims.³¹⁵ The report warned that vague national security justifications and weak EU export controls have enabled spyware to become a systemic threat to democracy and the rule of law in Europe.³¹⁶ In September 2025, new findings showed that millions of euros in EU taxpayer money, allocated by the EU's European Commission (EC) (partly through the EU's Defence Fund) have gone directly to finance the spyware industry, with corporate beneficiaries including Intellexa Alliance, Cy4Gate, Verint Systems and Cognyte.³¹⁷ The revelation prompted MEPs to demand answers from the EC, stating "[t]his raises serious questions about the governance, transparency, and accountability of the Union's funding mechanisms".³¹⁸

Egypt

In 2023, Ahmed Eltantawy, a former Egyptian MP, was systematically targeted with Predator spyware³¹⁹ produced by Cytox, a company from North Macedonia (reportedly part of Intellexa)³²⁰, after publicly announcing his intention to run for president in the 2024 Egyptian elections.³²¹ CitizenLab attributed his targeting with Predator spyware to the Egyptian government with "high confidence".³²² The targeting included SMS and WhatsApp links designed to deliver the spyware, as well as network injection when he used Vodafone Egypt mobile data to visit certain websites.³²³ Earlier, in 2021, the same individual had also been infected via text links containing Predator spyware, including over WhatsApp from

314 Privacy International, 'Statement before the European Parliament hearing on "Spyware used in third countries and implications for EU foreign relations"', December 2022, <https://privacyinternational.org/advocacy/5002/statement-european-parliament-hearing-spyware-used-third-countries-and-implications>

315 European Parliament PEGA Committee, 'Report of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware', May 2023, https://www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html

316 Ibid.

317 Suzanne Smalley, 'European parliamentarians implore EU leadership to stop funding spyware', The Record, October 2025, <https://therecord.media/european-parliament-stop-funding-spyware>; See also:

Vas Pangiotopoulos, 'Spyware industry pockets EU subsidies while snooping on its citizens', Follow the Money, 16 September 2025, <https://www.ftm.eu/articles/spyware-industry-eu-subsidies-surveillance-concerns?share=JHFsd1Fi6UUTf4Cgic8juJMJeC7kpl9O1%2Bjc%2FwYH5nBTe%2FhCTCe%2B0heiPISH740%3D>

318 Connor Jones, 'EU funds are flowing into spyware companies, and politicians are demanding answers', The Register, 2 October 2025, https://www.theregister.com/2025/10/02/eu_spyware_funding/

319 Bill Marczak, John Scott-Railton, Daniel Roethlisberger, Bahr Abdul Razzak, Siena Anstis, Ron Deibert, 'PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions', Citizenlab, 22 September 2023, <https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/>

320 Patrick Howell O'Neil, 'The Lucrative Government Spyware Industry Has a New 'One-Stop-Shop' for Hacking Everything', Gizmodo, 15 February 2019, <https://gizmodo.com/the-lucrative-government-spyware-industry-has-a-new-one-1832568791>

321 Bill Marczak, John Scott-Railton, Daniel Roethlisberger, Bahr Abdul Razzak, Siena Anstis, Ron Deibert, 'PREDATOR IN THE WIRES: Ahmed Eltantawy Targeted with Predator Spyware After Announcing Presidential Ambitions', Citizenlab, 22 September 2023, <https://citizenlab.ca/2023/09/predator-in-the-wires-ahmed-eltantawy-targeted-with-predator-spyware-after-announcing-presidential-ambitions/>

322 Ibid.

323 Ibid.

an individual purporting to be from a well-known human rights organisation.³²⁴ Egyptian opposition leader and vocal critic of President Abdel Fattah El-Sisi, Ayman Nour, was also subjected to targeting with spyware whilst living in exile in Turkey, both with Pegasus and Predator spyware separately, and an anonymous exiled dissident Egyptian journalist also having had their device hacked by Cyrox's Predator spyware.³²⁵

Legislative changes in Egypt since have reinforced the surveillance framework but leave open potential for abuse. As of early 2025, Egypt's draft Criminal Procedure Law grants the Public Prosecution (with investigating-judge approval) sweeping powers to intercept and monitor communications: social media accounts, emails, messages on phones or other devices; to seize devices; to record private conversations; and generally surveil on the basis of misdemeanours punishable by three months or more in prison.³²⁶ These powers are indefinitely renewable in 30-day increments, raising concerns about arbitrary or extended use.³²⁷ Civil society organisations have warned that the vague wording of the provisions, weak safeguards and the historic pattern of targeting of journalists, dissidents, and political opposition, in conjunction with Egypt's "long history of using spyware", increase the risk that these laws may be used for repression rather than purely law enforcement.³²⁸

El Salvador

In El Salvador between mid-2020 and late 2021, at least **35 journalists and civil society figures** were confirmed to have had their mobile phones hacked with NSO Group's **Pegasus spyware**, in many cases exfiltrating large volumes of private data.³²⁹ The targets included staff of independent national media outlets such as *El Faro*, *GatoEncerrado*, *La Prensa Gráfica*, and others, as well as NGO staff. The spyware hacks reportedly coincided with targets' sensitive investigations of the government of President Nayib Bukele – including *El Faro*'s revelations that Bukele's government had been in covert negotiations for a pact with the street gang Mara Salvatrucha 13 (MS-13) in order to reduce violence or to increase political support.³³⁰

Although the El Salvadorean government has denied purchasing or using Pegasus,³³¹ the Citizen Lab and Access Now investigation found that one Pegasus customer allegedly

324 Ibid.

325 Ibid.

326 Rasha Ammar, 'Egyptians Fear Privacy Invasion as New Law Permits Digital Surveillance', *Zawia3*, 11 February 2025, <https://zawia3.com/en/snooping/>

327 Egyptian Initiative for Personal Rights, 'Privacy under attack: Egypt must reform its draft Criminal Procedure Code', 12 February 2025, <https://eipr.org/en/press/2025/02/privacy-under-attack-egypt-must-reform-its-draft-criminal-procedure-code>

328 Ibid.

329 John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Aljizawi, Salvatore Solimano, Ron Deibert, 'Project Torogoz Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware', *CitizenLab*, 12 January 2022, <https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/>

330 Carlos Martínez, Óscar Martínez, Sergio Arauz y Efrén Lemus, 'Gobierno de Bukele lleva un año negociando con la MS-13 reducción de homicidios y apoyo electoral', *El Faro*, 3 September 2020, <https://elfaro.net/es/202009/el-salvador/24781/Gobierno-de-Bukele-lleva-un-año-negociando-con-la-MS-13-reducción-de-homicidios-y-apoyo-electoral.htm>

331 Merlin Delcid, 'El Salvador denies responsibility for hacking journalists after report finds Pegasus spyware on their phones', *CNN*, 13 January 2022, <https://edition.cnn.com/2022/01/13/americas/el-salvador-pegasus-spyware-intl>

operated almost exclusively on El Salvador since 2019, and stated there was a “range of circumstantial evidence pointing to a strong El Salvador government nexus”,³³² concerning overlap with the interests of Bukele’s administration. Women made up just half of those confirmed to have been targeted with Pegasus, several of whom testified to use of the spyware being linked to gendered impacts of persecution they faced as a consequence of targeting, including vulnerability to defamation and doxxing.³³³

Compounding these concerns over the use of spyware in El Salvador is that they have taken place in a broader national context of deteriorating human rights and intensifying authoritarianism: the same year of the revelations of spyware in El Salvador, the popular Nayib Bukele, who termed himself the “world’s coolest dictator”³³⁴, was granted permission by a Constitutional Chamber (whose magistrates and attorney general his own party had replaced) to stand for immediate re-election despite an explicit constitutional provision forbidding this; and in July 2025 the constitution was again altered to consolidate his power by ending presidential term limits altogether, further to a general erosion of the nation’s democratic institutions.³³⁵

For over three and a half years and up to the time of writing, El Salvador has been under a “state of exception” in which fundamental rights are suspended.³³⁶ A context of weakened legal rights protections exacerbates the potential rights implications of the use of surveillance technology. 2025 saw a “great exodus” of Salvadorean journalists, lawyers and human rights activists fleeing the country and entering into exile around the world.³³⁷ In 2026, Amnesty International reported that mass arbitrary detention, denial of due process and “systematic allegations of torture” have occurred in El Salvador with more than 90,000 people detained during the state of exception, of which at least 470 died in state custody, in what the organisation has proclaimed “could amount to crimes against humanity under international criminal law”.³³⁸

332 John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Aljizawi, Salvatore Solimano, Ron Deibert, “Project Torogoz Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware”, CitizenLab, 12 January 2022, <https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/>

Carlos Martínez, Óscar Martínez, Sergio Arauz y Efrén Lemus, ‘Gobierno de Bukele lleva un año negociando con la MS-13 reducción de homicidios y apoyo electoral’, El Faro, 3 September 2020, <https://elfaro.net/es/202009/el-salvador/24781/Gobierno-de-Bukele-lleva-un-año-negociando-con-la-MS-13-reducción-de-homicidios-y-apoyo-electoral.htm>; Sam Jones, ‘Pegasus spyware used in ‘jaw-dropping’ phone hacks on El Salvador journalists’, The Guardian, 13 January 2022, <https://www.theguardian.com/news/2022/jan/13/pegasus-spyware-target-journalists-activists-el-salvador>

333 Access Now, ‘Mujeres resistiendo a Pegasus: Testimonios desde El Salvador’, 17 March 2023 (last updated), <https://www.accessnow.org/testimonios-mujeres-pegasus-el-salvador/>

334 El Tiempo, ‘Presidente Bukele dice en Twitter que es “el dictador más cool del mundo”’, 21 September 2021, <https://www.eltiempo.com/mundo/latinoamerica/presidente-bukele-dice-que-es-el-dictador-mas-cool-del-mundo-619795>

335 Juanita Goebertus Estrada, ‘El Salvador’s Democracy Is Dying’, Human Rights Watch, 2 September 2025, <https://www.hrw.org/news/2025/09/02/el-salvadors-democracy-is-dying>; WOLA, “El Salvador’s Constitutional Court Paves Way for President Bukele to Seek Reelection Following Purge of Country’s Judiciary”, September 2021 <https://www.wola.org/2021/09/el-salvador-president-reelection-judiciary/>

336 Tom Lantos Human Rights Commission, ‘The State of Exception in El Salvador: Taking Stock’, Event, 12 October 2024, <https://humanrightscommission.house.gov/events/hearings/state-exception-el-salvador-taking-stock>

337 Óscar Martínez y Carlos Martínez, ‘El exilio nos alcanza’, El Faro, 1 June 2025, <https://beta.elfaro.net/titulares/el-exilio-nos-alcanza>

338 <https://www.amnesty.org/en/latest/news/2026/07/el-salvador-el-costo-humano-del-regimen-de-excepcion-podria-constituir-crmenes-de-lesa-humanidad/>

US (Immigration and Customs Enforcement – ICE)

In August 2025, the Trump administration reactivated a \$2 million contract with Israeli spyware firm Paragon Solutions to provide its Immigration and Customs Enforcement (ICE) agency with access to Graphite spyware, giving ICE authority to deploy the tool.³³⁹ Graphite spyware has been documented to have been used against journalists, migration advocates, and civil society actors in Italy, raising alarms about the risk of misuse in the U.S. context, particularly in the hands of an agency that has been condemned for human rights abuses.³⁴⁰ In response, U.S. lawmakers formally requested transparency from ICE concerning the possible deployment of **Paragon Solution's Graphite** spyware in a 6 October 2025 letter to the Department of Homeland Security, including asking for "[a] comprehensive list of data surveillance targets and ICE's strategy for deploying spyware or mass data surveillance within the United States".³⁴¹ In 2026, in response to 404 media's FOIA request for documents relative to the Paragon purchase, ICE stated that it had found 673 potentially responsive pages of records relevant to this, then began to release them subject to heavy redactions obscuring almost all of the information in them.³⁴²

Critically, ICE's apparent procurement of spyware technology occurred in the context of the US government's mass deportation campaign, during which the ICE Director proclaimed his intention to digitise and accelerate deportation to make it "like [Amazon] Prime, but with human beings".³⁴³ Mass detentions, raids (with powers to conduct them in schools, places of worship and hospitals) and deportations have taken place,³⁴⁴ with ICE non-criminal arrests reportedly rising by **800 %** since April 2025 amidst widespread reports of human rights violations.³⁴⁵

Mexico

In 2019, the Inter American Commission on Human Rights (IACHR) and the Office of the United Nations Special Rapporteur on Freedom of Expression urged the Mexican

339 Jack Poulson, 'Exclusive: ICE reactivated its \$2 million contract with Israeli spyware firm Paragon, following its acquisition by U.S. capital', 1 September 2025, <https://jackpoulson.substack.com/p/exclusive-ice-has-reactivated-its>

340 Stephanie Kirchgaessner, 'Ice obtains access to Israeli-made spyware that can hack phones and encrypted apps', The Guardian, 2 September 2025, <https://www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware>

341 Elizabeth Weill-Greenberg, 'Lawmakers Demand Information About Potential Use of Paragon Spyware by ICE', truthout, 6 October 2025, <https://truthout.org/articles/lawmakers-demand-information-about-potential-use-of-paragon-spyware-by-ice/>; Letter to Kristi Noem, Department of Homeland Security, 6 October 2025, https://drive.google.com/file/d/1hepcrk651kcQaTzGvJJSouPjbizr5e_g/view

342 Joseph Cox, 'We Sued ICE to Get Its Spyware Contract. The Agency Is Redacting Essentially Everything', 404 Media, June 2026 <https://www.404media.co/we-sued-ice-to-get-its-spyware-contract-the-agency-is-redacting-essentially-everything/>

343 Marina Dunbar, 'Ice director wants to run deportations like 'Amazon Prime for human beings'', The Guardian, 9 April 2025 <https://www.theguardian.com/us-news/2025/apr/09/ice-todd-lyons-deporation-amazon>

344 Rebecca Santana, 'Trump administration throws out policies limiting migrant arrests at sensitive spots like churches', Associated Press, 22 January 2025 <https://apnews.com/article/immigration-enforcement-sensitive-locations-trump-ab0d2d2652e9df696f14410ebb52a1fc>

345 Human Rights Watch, ' "You Feel Like Your Life Is Over": Abusive Practices at Three Florida Immigration Detention Centers Since January 2025', 21 July 2025, <https://www.hrw.org/report/2025/07/21/you-feel-like-your-life-is-over/abusive-practices-at-three-florida-immigration>; Visa Verge, "DHS Brags of Massive Deportations as Democrats Condemn ICE Tactics", 16 August 2025, <https://www.visaverge.com/news/dhs-brags-of-massive-deportations-as-democrats-condemn-ice-tactics/>

government to “step up its efforts [to investigate] the illegal use of Pegasus spyware to target journalists and defenders,” the uses of which the IACHR stated “violate the right to privacy enshrined in the American Convention”.³⁴⁶ Documents that emerged from the WhatsApp vs NSO Group US litigation revealed that in Mexico, in a period of merely two months in 2019, at least **456 people** were allegedly surveilled with Pegasus spyware by the state (or state-contracted actors) during the presidency of Andrés Manuel López Obrador, as highlighted by Mexican civil society organisation Red en Defensa de los Derechos Digitales (R3D).³⁴⁷ During litigation, NSO Group’s representative confirmed that the Mexican government was one of their clients.³⁴⁸

Sudan

In 2022, Lighthouse Reports reported that a clandestine network involving an Israeli Intellexa spyware magnate and the Rapid Support Forces (RSF) militia in Sudan were delivering surveillance technology to the junta.³⁴⁹ In May 2022, a private jet linked to Intellexa delivered advanced surveillance equipment from Cyprus to Khartoum, Sudan, where it was swiftly transferred to the RSF.³⁵⁰ Intellexa sells Predator spyware. The RSF militia, notorious for its role in Darfur’s atrocities,³⁵¹ thus received technology capabilities allowing the transformation of smartphones into covert surveillance tools. The equipment’s arrival was so perilous that RSF commanders reportedly relocated it to Darfur to prevent seizure by Sudanese military forces.³⁵² The investigation uncovered a broader European supply chain, with Intellexa operating through entities in Cyprus, Ireland, and the British Virgin Islands, raising serious concerns about the export of EU-made spyware to authoritarian regimes and armed groups.³⁵³ A year after the investigation was published, a devastating war broke out in Sudan between the RSF and the Sudanese army that continues at the time of writing.³⁵⁴

346 Inter-American Commission on Human Rights, ‘IACHR Expresses Concern Over the Increase in Cases Concerning the Use of Pegasus Spyware in Mexico’, June 2023, https://www.oas.org/en/iachr/jsForm/?File=/en/iachr/media_center/preleases/2023/109.asp

347 Red en Defensa de los Derechos Digitales, ‘Gobierno mexicano usó Pegasus para espiar al menos a 456 personas en 2019’, 14 April 2025 <https://r3d.mx/2025/04/14/gobierno-mexicano-uso-pegasus-para-espiar-al-menos-a-456-personas-en-2019/>

348 Ibid.

349 Tasos Telloglou, Eliza Triantafillou, Crofton Black, Omer Benjakob, Avi Scharf, Tomas Statius, Gabriel Geiger, Klaas van Dijken, Bashar Deeb, Jack Sapoch, Daniel Howden, Margot Gibbs, Lionel Faull, ‘Flight of the Predator co-published with Haaretz and Inside Story’, 30 November 2022, <https://www.lighthousereports.com/investigation/flight-of-the-predator/>

350 Ibid.

351 Amnesty International, “Sudan: RSF atrocities in El Fasher ‘a stain on the conscience of humanity’ – new report”, 1 July 2026, <https://www.amnesty.org/en/latest/news/2026/07/sudan-rsf-atrocities-in-el-fasher-a-stain-on-the-conscience-of-humanity-new-report/>
Human Rights Watch, “Sudan: Mass Atrocities in Captured Darfur City”, 29 October 2025, <https://www.hrw.org/news/2025/10/29/sudan-mass-atrocities-in-captured-darfur-city>

352 Tasos Telloglou, Eliza Triantafillou, Crofton Black, Omer Benjakob, Avi Scharf, Tomas Statius, Gabriel Geiger, Klaas van Dijken, Bashar Deeb, Jack Sapoch, Daniel Howden, Margot Gibbs, Lionel Faull, ‘Flight of the Predator co-published with Haaretz and Inside Story’, 30 November 2022, <https://www.lighthousereports.com/investigation/flight-of-the-predator/>

353 Ibid.

354 Centre for Preventative Action, ‘Civil War in Sudan’, July 2026 <https://www.cfr.org/global-conflict-tracker/conflict/power-struggle-sudan>

Armenia

The first documented deployment of commercial spyware during an international war took place in Armenia.³⁵⁵ In May 2023, a joint-investigation reported twelve cases of Armenian public figures whose devices forensic analysis confirmed to have been targeted with NSO Group's Pegasus spyware amid a 44-day conflict in the Nagorno-Karabakh (also referred to as the Republic of Artsakh in Armenia) with Azerbaijan, between 2020 and 2022.³⁵⁶ Citizen Lab further confirmed that Azerbaijan had at least two Pegasus command centres operating by 2018.³⁵⁷ Moreover, **hundreds of Armenian officials, journalists, and civil society figures** received Apple threat notifications between 2020 and 2023 which indicated the possibility they had been targeted with spyware, including high profile figures such as the President, Prime Minister, and National Assembly Speaker, as well as some of their family members.³⁵⁸ This case exemplifies the use of spyware not only as a tool for civil society repression but as a weapon to be deployed in conflict settings and in wartime.

The use of Spyware in the Gulf countries of Bahrain, United Arab Emirates and Saudi Arabia

Privacy International acknowledges and credits the valuable contributions of the Bahrain Institute for Rights and Democracy (BIRD) whose provision of research and information allowed for the compilation of this case study.

Many countries in the Gulf are noted for their repressive forms of governance and widespread curtailments of the human rights and fundamental freedoms of their populations. All six Gulf Cooperation Council (GCC) states – the Kingdom of Saudi Arabia, the United Arab Emirates (UAE), Bahrain, Kuwait, Qatar and Oman - are ranked as and termed “**authoritarian**” countries in an index on global democracy published in 2025 by the Economist Intelligence.³⁵⁹

Of the GCC states, Saudi Arabia, Bahrain and the UAE all have documented authoritarian

355 AccessNow, 'Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict', 25 May 2023, <https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/>; Sargis Harutynyan, 'Pegasus. Targeting Armenia', 2024, https://mdi.am/wp-content/uploads/2024/07/PEGASUS-TARGETING-ARMENIA_2024_Eng.pdf

356 Amnesty International, 'Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict', 25 May 2023, <https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/#:~:text=A%C2%A0joint%20investigation%C2%A0has%20revealed%20that%20at,the%20reason%20for%20the%20targeting>; Sargis Harutynyan, 'Pegasus. Targeting Armenia', 2024, https://mdi.am/wp-content/uploads/2024/07/PEGASUS-TARGETING-ARMENIA_2024_Eng.pdf

357 John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Nicola Lawford, and Ron Deiber, 'Armenia-Azerbaijan conflict: Pegasus infections - Technical Brief [1]', The Citizen Lab, 25 May 2023, <https://citizenlab.ca/research/cr1-armenia-pegasus/>

358 Sargis Harutynyan, 'Pegasus. Targeting Armenia', 2024, https://mdi.am/wp-content/uploads/2024/07/PEGASUS-TARGETING-ARMENIA_2024_Eng.pdf; Amnesty International, 'Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict', 25 May 2023, <https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/#:~:text=A%C2%A0joint%20investigation%C2%A0has%20revealed%20that%20at,the%20reason%20for%20the%20targeting>; AccessNow, 'Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict', 25 May 2023, <https://www.accessnow.org/press-release/spyware-warfare-pegasus-in-azerbaijan-armenia-conflict/>

359 Economist Intelligence, 'The Democracy Index 2024', February 2025, <https://www.eiu.com/n/global-themes/democracy-index/>

practises and are routinely condemned for human rights violations including arbitrary executions and imposition of the death penalty, torture, mass trials and lack of due process, the stifling of free expression and serious religious, gendered and political repression.³⁶⁰ These three nations repeatedly receive amongst the lowest scores on international rights and freedoms rankings. Indeed, in Freedom House's 2025 freedom in the world rankings, Saudi Arabia scored just 9/100, Bahrain scored only 12/100 and the UAE 18/100.³⁶¹ Equally, on the Reporters Sans Frontières index on press freedom around the world, out of 180 countries, the UAE, Saudi Arabia and Bahrain were ranked 164, 162 and 157 respectively in 2025.³⁶² Prominently featuring amongst these states' toolkits of digital repression for over a decade is spyware.

Spyware against Gulf diaspora living in the UK: Litigation as an avenue of resistance

Moosa Mohammed and Dr Saeed Shehabi

Following the violent crackdown against protesters during Bahrain's Arab Spring uprising in 2011,³⁶³ those who came to the UK to flee persecution in Bahrain and its neighbouring countries may have still been subject to state-sanctioned interferences with their human rights, including the right to privacy.³⁶⁴

The use of spyware against Gulf dissidents, including pro-democracy Bahraini activists living in the Bahrain, the UK and the USA, was documented by Citizen Lab in 2012.³⁶⁵ They

360 Human Rights Watch, 'Bahrain, Events of 2024 - World Report 2025', 2025, <https://www.hrw.org/world-report/2025/country-chapters/bahrain>; Human Rights Watch, Saudi Arabia, Events of 2024 - World Report 2025', 2025, <https://www.hrw.org/world-report/2025/country-chapters/saudi-arabia>; Human Rights Watch, UAE, Events of 2024 - World Report 2025, 2025, <https://www.hrw.org/world-report/2025/country-chapters/united-arab-emirates>; Reprieve and the Bahrain Institute for Rights and Democracy (BIRD), 'From uprisings to executions: The death penalty in Bahrain, ten years on from the Arab Spring', 27 July 2021, <https://reprieve.org/uk/2021/07/27/death-penalty-in-bahrain/>

361 "Saudi Arabia's absolute monarchy restricts almost all political rights and civil liberties". See: Freedom House, "'Saudi Arabia" - Freedom in the World 2025', <https://freedomhouse.org/country/saudi-arabia>; "Bahrain's Sunni-led monarchy dominates state institutions, and elections for the lower house of parliament are neither competitive nor inclusive. Since violently crushing a popular prodemocracy protest movement in 2011, the authorities have systematically eliminated a broad range of political rights and civil liberties, dismantled the political opposition, and cracked down on persistent dissent concentrated among the Shiite population". See: Freedom House, "'Bahrain" - Freedom in the World 2025', <https://freedomhouse.org/country/bahrain>; "[...] political parties are banned, and all executive, legislative, and judicial authority ultimately rests with the seven hereditary rulers. The civil liberties of both citizens and noncitizens are subject to significant restrictions". See: Freedom House, "'United Arab Emirates" - Freedom in the World 2025, <https://freedomhouse.org/country/united-arab-emirates.rsf-ranking-2025>

362 Reporters Sans Frontières, 'World Press Freedom Index 2025', <https://rsf.org/en/index?year=2025>

363 Amnesty International, 'Bahrain: "Disturbing, Damning Evidence" of Bahrain's Excessive Force Against Peaceful Protestors Including Live Ammunition Fired at Close Range', 27 March 2011, <https://www.amnestyusa.org/press-releases/bahrain-disturbing-damning-evidence-of-bahrains-excessive-force-against-peaceful-protestors-including-live-ammunition-fired-at-close-range-2/>

364 See: Bindmans, 'Prominent blogger launches lawsuit against Bahrain and NSO Group over spyware', 6 December 2022, <https://www.bindmans.com/news-insights/news/blogger-launches-lawsuit-against-bahrain-and-nso/>; Diane Taylor, 'UK home secretary apologises over unlawful detention of Bahraini activist', The Guardian, 8 February 2024, <https://www.theguardian.com/politics/2024/feb/08/james-cleverly-apology-unlawful-detention-bahraini-activist-sayed-ahmed-alwadaei>; Dan Sabbagh, David Pegg, Paul Lewis and Stephanie Kirchgaessner, 'UAE linked to listing of hundreds of UK phones in Pegasus project leak', The Guardian, 21 July 2021, <https://www.theguardian.com/world/2021/jul/21/uae-linked-to-listing-of-hundreds-of-uk-phones-in-pegasus-project-leak>

365 Morgan Marquis-Boire, Bill Marczak, 'From Bahrain With Love: FinFisher's Spy Kit Exposed?', 25 July 2012, <https://citizenlab.ca/research/from-bahrain-with-love-finfishers-spy-kit-exposed/>

were targeted by FinFisher spyware (a signature product of UK-based company Gamma International).³⁶⁶ The spyware purportedly could record communications, intercept voice-over-Internet calls, and record every keystroke of the targeted devices.³⁶⁷ The spyware was found to be connecting to a computer located in Bahrain.³⁶⁸

Almost a decade later, two of the activists identified by Citizen Lab, Dr Saeed Shehabi and Moosa Mohammed took their case to the UK courts, alleging "that the Bahraini government used German-made FinFisher surveillance software to infiltrate their computers whilst they were living in London in 2011."³⁶⁹ In response, the Bahraini government argued that it had state immunity and was not subject to the powers of the British judicial system.³⁷⁰ In June 2026, the Supreme Court ruled in favour of Dr Shehabi and Mr Mohammed, dismissing the Bahraini government's appeal, and holding that, assuming the claimants' computers had been hacked in the UK by Bahrain, that act "involved an interference with the territorial sovereignty of the United Kingdom".³⁷¹ Thus the Bahraini was not immune from the suit, but the underlying allegations regarding the use of spyware are still being litigated.

This case speaks to the question of technology-enabled transnational repression and the possibility of remedies for cross-border authoritarian use of technology. Commenting on the judgment, Dr Shehabi said: "This is not just a victory for us, but for everyone targeted by authoritarian states beyond their own borders".³⁷²

Ghanem Almasarir and others

In the Pegasus Project revelations, further use of spyware against Gulf individuals, including diaspora living abroad in the UK, was revealed. Ghanem Almasarir, a Saudi comedian and prominent dissident launched a civil case against the Saudi government in 2019, alleging that he had been targeted by the government with Pegasus spyware whilst on UK soil.³⁷³ He brought a "civil legal claim for misuse of private information, harassment, and trespass to goods" and personal injury against Saudi Arabia which was issued in the High Court.³⁷⁴ In 2022, the case became the first one in UK courts to find an exception for sovereign immunity regarding the use of spyware technology, since the High Court ruled that Saudi Arabia did not have immunity under the UK State Immunity Act, contrary to the defendant's

366 Ibid.

367 Ibid.

368 Ibid.

369 Leigh Day, 'Dissidents win in Supreme Court as it rejects Kingdom of Bahrain's appeal over sovereign immunity from spyware claims', 27 July 2026, <https://www.leighday.co.uk/news/press-releases/2026-news/dissidents-win-in-supreme-court-as-it-rejects-kingdom-of-bahrain-s-appeal-over-sovereign-immunity-from-spyware-claims/>

370 Ibid.

371 UK Supreme Court, 'The Kingdom of Bahrain (Appellant) v Shehabi and another (Respondents)', 27 July 2026 https://supremecourt.uk/uploads/uksc_2024_0152_judgment_a1ae6cd3a5.pdf

372 Dr Saeed Shehabi in a quotation contained in a press release, shared internally by the Bahrain Institute for Rights and Democracy (BIRD) via email with Privacy International on 27 June 2026.

373 Leigh Day, 'Legal case launched against Kingdom of Saudi Arabia for alleged use of spyware to target dissident', 28 May 2019, <https://www.leighday.co.uk/news/press-releases/2019-news/legal-case-launched-against-kingdom-of-saudi-arabia-for-alleged-use-of-spyware-to-target-dissident/>; Leigh Day, 'Human rights activist issues case against the Kingdom of Saudi Arabia for alleged use of NSO spyware', 4 November 2019, <https://www.leighday.co.uk/news/press-releases/2019-news/human-rights-activist-issues-case-against-the-kingdom-of-saudi-arabia-for-alleged-use-of-nso-spyware/>

374 Ibid.

application, providing precedent for the success of the above case against Bahrain.³⁷⁵ In 2026, Saudi Arabia was “found responsible for infecting his phone with Pegasus spyware and later directing an assault on him” and ordered to pay over 3 million pounds in damages, stating that Al-Masariir’s high-profile activism “made him an obvious target for the KSA,” which had “a well-documented history of use of various forms of spyware”.³⁷⁶

The High Court has also ruled that another UK-based Saudi Arabian dissident and human rights defender, Yahya Assiri, could bring a spyware case against KSA for use of the technology against him on British soil.³⁷⁷

Further lawsuits from UK-based activists, journalists and dissidents, some of whom live in exile having been granted asylum due to persecution by their governments, have emerged in recent years on the basis of the alleged use of spyware against them.³⁷⁸ These include claims from Anas Altikriti, Azzam Tamimi, Mohammed Kozbar, Rania Dridi and Yusuf Al-Jamri who allege Gulf state-sponsored hacking on their devices by Bahrain, Saudi Arabia and the UAE.³⁷⁹

Bahrain

In 2014, leaked documents revealed that German surveillance company FinFisher had allegedly helped the Bahraini government to infect 77 devices with spyware between 2010 and 2012; a critical period leading to the Arab Spring uprising and Bahrain’s ensuing bloody crackdown on pro-democracy protesters.³⁸⁰ Targets of the spyware included those living in Bahrain, such as human rights lawyers, and the leader of the political opposition, Hassan

375 Stephanie Kirchgaessner, ‘British judge rules dissident can sue Saudi Arabia for Pegasus hacking’, The Guardian, 19 August 2022, <https://www.theguardian.com/world/2022/aug/19/british-judge-rules-dissident-ghanem-almasarir-can-sue-saudi-arabia-for-pegasus-hacking>; Leigh Day, ‘High Court gives green light to a Pegasus spyware case being brought in London against the Kingdom of Saudi Arabia by a UK based dissident’, 19 August 2022, <https://www.leighday.co.uk/news/press-releases/2022-news/high-court-gives-green-light-to-a-pegasus-spyware-case-being-brought-in-london-against-the-kingdom-of-saudi-arabia-by-a-uk-based-dissident/>

376 Columbia University Global Freedom of Expression, ‘“Al-Masariir v. Saudi Arabia” Case Analysis’, 2026 <https://globalfreedomofexpression.columbia.edu/cases/al-masariir-v-saudi-arabia>; Freedom House, ‘TNR Watch: Delivering Accountability for Spyware Abuse’, February 2026 <https://freedomhouse.org/article/tnr-watch-delivering-accountability-spyware-abuse>; Haroon Siddique and Stephanie Kirchgaessner, ‘Saudi Arabia ordered to pay £3m to London dissident over Pegasus spying’, The Guardian, January 2026, <https://www.theguardian.com/world/2026/jan/26/saudi-arabia-ordered-pay-london-dissident-pegasus-spying-ghanem-al-masariir>

377 Amnesty International, ‘UK court says activist can pursue spyware case against Saudi Arabia’, 21 October 2024, <https://securitylab.amnesty.org/latest/2024/10/uk-court-says-activist-can-pursue-spyware-case-against-saudi-arabia/>

378 Global Legal Action Network, ‘New Criminal Complaint Over Pegasus Spyware Hacking of journalists and activists in the UK’, 19 September 2024, <https://glanlaw.org/news/new-criminal-complaint-over-pegasus-spyware-hacking-of-journalists-and-activists-in-the-uk/>

379 Ibid.; Bindmans, ‘High Court grants permission to Yusuf AlJamri to bring a spyware based legal claim against the Kingdom of Bahrain over Pegasus cyberattacks’, 4 December 2024, <https://www.bindmans.com/news-insights/news/press-release-high-court-grants-permission-to-yusuf-aljamri-to-bring-a-spyware-based-legal-claim-against-the-kingdom-of-bahrain-over-pegasus-cyberattacks/>; Bindmans, ‘Bindmans launches legal action in the United Kingdom on misuse of Pegasus spyware’, 19 April 2022, <https://www.bindmans.com/news-insights/news/bindmans-launches-legal-action-in-the-united-kingdom-on-misuse-of-pegasus-spyware/>; Leigh Day, ‘High Court grants permission to British journalist to bring a spyware based legal case against the United Arab Emirates’, 20 March 2024, <https://www.leighday.co.uk/news/news/2024-news/high-court-grants-permission-to-british-journalist-to-bring-a-spyware-based-legal-case-against-the-united-arab-emirates/>

380 Morgan Marquis-Boire and Cora Currier, ‘Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters’, The Intercept, 7 August 2014, <https://theintercept.com/2014/08/07/leaked-files-german-spy-company-helped-bahrain-track-arab-spring-protesters/>

Mushaima, who was later imprisoned and remains arbitrarily detained in Bahrain at the time of writing, over a decade later.³⁸¹

Mushaima was sentenced to prison months after leaked installation logs showed that the spyware infiltrated his computer.³⁸² The company Nokia Siemens was also reported to have sold spyware to Bahrain in 2011.³⁸³ Bahraini interrogators are reported to have shown detainees transcripts of the text messages and phone conversations whilst they were being tortured, raising serious concerns that data obtained through the use of spyware was being used to fuel human rights violations and widespread political repression.³⁸⁴

UAE

A high profile political prisoner in the UAE - award winning Emirati human rights defender and blogger, Ahmed Mansoor – was reportedly repeatedly targeted with spyware by the UAE government, whose persecution of him is well-documented,³⁸⁵ including one incident of spyware targeting against him in 2016.³⁸⁶ In 2017, Mansoor was imprisoned in the UAE where he has remained in prison under arbitrary detention ever since and up to the time of writing, whilst being subject to a host of human rights violations.³⁸⁷ The basis of his 15 year criminal conviction includes using email and WhatsApp to communicate with human rights organisations.³⁸⁸

Far afield from the UAE in the UK, computer systems in the British Prime Minister's executive office at number 10 Downing Street and in the Foreign Office were suspected to have been infiltrated with spyware, which Citizen Lab reportedly linked in 2021 to operators based in the UAE.³⁸⁹ The year beforehand, a UK High Court found that the ruler of Dubai and UAE Prime Minister, Sheikh Mohamed bin-Rashid al-Maktoum, hacked his wife's phone whilst she

381 Ibid.; United Nations Working Group on Arbitrary Detention, Opinions adopted by the Working Group on Arbitrary Detention at its 98th session, 13-17 November 2023: Opinion No. 74 /2023 concerning Hasan Mushaima, Abdullah Isa Abdulla Mahroos, Abdulwahab Husain Ali Ahmed Ismaeel and Abduljalil Radhi Mansoor Makki (Bahrain), November 2023, <https://digitallibrary.un.org/record/4043219?ln=en&v=pdf>

382 Morgan Marquis-Boire and Cora Currier, 'Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters', The Intercept, 7 August 2014 <https://theintercept.com/2014/08/07/leaked-files-german-spy-company-helped-bahrain-track-arab-spring-protesters/>

383 Ibid.

384 Ibid.; Kim Zetter, 'Nokia-Siemens Spy Tools Aid Police Torture in Bahrain', Wired, 23 August 2011 <https://www.wired.com/2011/08/nokia-siemens-spy-systems/>

385 Human Rights Watch, 'The Persecution of Ahmed Mansoor', 27 January 2021, <https://www.hrw.org/report/2021/01/27/persecution-ahmed-mansoor/how-united-arab-emirates-silenced-its-most-famous-human>; Human Rights Watch, 'UAE: Ahmed Mansoor's 15-Year Sentence Upheld', 7 March 2025, <https://www.hrw.org/news/2025/03/07/uae-ahmed-mansoor-15-year-sentence-upheld>

386 Bill Marczak and John Scott-Railton, 'The Million Dollar Dissident NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender', Citizenlab, 24 August 2016 <https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/>

387 Human Rights Watch, 'UAE: Ahmed Mansoor's 15-Year Sentence Upheld', 7 March 2025, <https://www.hrw.org/news/2025/03/07/uae-ahmed-mansoor-15-year-sentence-upheld>; A/HRC/WGAD/2011/64, 'United Nations Working Group on Arbitrary Detention - Ahmed Mansoor v. United Arab Emirates', 2011, University of Minnesota Human Rights Library, <https://hrlibrary.umn.edu/wgad/64-2011.html>

388 Ibid.

389 Ron Deibert, 'UK Government Officials Infected with Pegasus', CitizenLab, 18 April 2022, <https://citizenlab.ca/2022/04/uk-government-officials-targeted-pegasus/>

was in London using Pegasus spyware from NSO Group in what was termed an abuse of power.³⁹⁰

Saudi Arabia

Amongst the most notable cases of suspected spyware targeting by Saudi Arabia includes the emergence of evidence to suggest that those in the close circle of Jamal Khashoggi were targeted with Pegasus spyware by Saudi Arabia and the UAE.³⁹¹ Khashoggi was a journalist whose brutal murder and dismemberment in the Saudi Arabian Embassy in Istanbul, Turkey, on 2 October 2018 caused international outcry, and which according to the Central Intelligence Agency (CIA) and US Senators was allegedly ordered by Saudi Crown Prince Mohammed Bin Salman.³⁹² Those targeted with spyware included Khashoggi's widow, Hanan Elatr, who has since filed a lawsuit in Virginia, US, against NSO Group, after forensics showed her phone had been infected by spyware allegedly from an agency in the UAE.³⁹³

Human rights and Data Protection Implications

The use of spyware can violate the right to privacy of a targeted individual. Beyond this, it also puts the right to privacy of people in their circles at risk. Whilst the right to privacy is not an absolute right, any interference must satisfy requirements of legality, necessity and proportionality. In this regard, the technical capabilities of many forms of spyware, particularly their capacity to access extensive information on a device and to exploit previously unknown vulnerabilities, raises serious concerns about whether such tools can ever be deployed in a way that is compatible with these requirements.³⁹⁴ Further, these characteristics create significant tension with core data protection principles, such as purpose limitation and data minimisation, insofar as the means and scope of the data

390 Haroon Siddique, 'Dubai ruler hacked ex-wife using NSO Pegasus spyware, high court judge finds', The Guardian, 6 October 2021 <https://www.theguardian.com/world/2021/oct/06/dubai-ruler-hacked-ex-wife-using-nso-pegasus-spyware-high-court-judge-finds-sheikh-mohammed-princess-haya>

391 Stephanie Kirchgaessner, 'Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests', The Guardian, 18 July 2019 <https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus>

392 Joyce Lee and Dalton Bennett, 'The assassination of Jamal Khashoggi', The Washington Post, 1 April 2019 <https://www.washingtonpost.com/graphics/2019/world/assassination-of-jamal-khashoggi-documentary/>; Shane Harris, Greg Miller and Josh Dawsey, 'CIA concludes Saudi crown prince ordered Jamal Khashoggi's assassination', The Washington Post, 16 November 2018, https://www.washingtonpost.com/world/national-security/cia-concludes-saudi-crown-prince-ordered-jamal-khashoggis-assassination/2018/11/16/98c89fe6-e9b2-11e8-a939-9469f1166f9d_story.html; Shane Harris and Karoun Demirjian, 'Senators accuse Saudi crown prince of complicity in Khashoggi's killing', The Washington Post, 4 December 2018, https://www.washingtonpost.com/world/national-security/cia-director-briefs-senators-on-saudi-role-in-khashoggi-killing/2018/12/04/e6d6498c-f7d5-11e8-8d64-4e79db33382f_story.html

393 Raphael Satter, 'Khashoggi's widow sues Israeli spyware company NSO over phone hacking', Reuters, 16 June 2023, <https://www.reuters.com/world/middle-east/khashoggis-widow-sues-israeli-spyware-company-nso-over-phone-hacking-2023-06-16/>; Dana Priest, 'A UAE agency put Pegasus spyware on phone of Jamal Khashoggi's wife months before his murder, new forensics show', The Washington Post, 21 December 2021, <https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/>; Hanan Elatr Khashoggi vs NSO Group Technologies Limited and Q Cyber Technologies Limited, Civil Action No. 1:23-cv-779, <https://www.courtsenews.com/wp-content/uploads/2023/06/khashoggi.pdf>;

Dana Priest, 'A UAE agency put Pegasus spyware on phone of Jamal Khashoggi's wife months before his murder, new forensics show', The Washington Post, December 2021, <https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/>

394 Privacy International, 'Aynur Ganbarova v. Azerbaijan and 24 other applications & Mustafayev and Others v. Azerbaijan', n.d., <https://privacyinternational.org/legal-action/aynur-ganbarova-v-azerbaijan-and-24-other-applications-mustafayev-and-others-v>

accessed will likely exceed what is strictly necessary, and may incidentally affect the data of people in the circles of the person targeted.

Beyond the right to privacy, spyware use could also endanger the full spectrum of human rights. The Council of Europe Commissioner for Human Rights has highlighted with respect to Pegasus and equivalent spyware that “it is difficult to imagine a scenario in which the use of such powerful and invasive spyware would ever be proportionate to the aim and thus human rights compliant”, making its compliance with CoE law and safeguards “virtually unimaginable”.³⁹⁵

Equally, the Office of the United Nations High Commissioner for Human Rights reported that spyware such as Pegasus “effectively turn[s] most smartphones into 24-hour surveillance devices” and raised the alarm over its misuse against civil society rather than for crime fighting purposes, and calling for a qualified moratorium on the domestic and transnational sale and use of such hacking technologies.³⁹⁶

It must be recalled that the data extracted by spyware use may include special categories of personal data (which should be subject to additional safeguards), such as biometric data, and data revealing information about an individual’s health, sexuality, religion, political opinion, and racial or ethnic origin, and will often implicate the personal data of children who require further safeguards to protect their best interests.³⁹⁷

The use of spyware may have a chilling effect on society. The covert nature of the malware – often difficult to detect without specialist forensic analysis – could create a pervasive sense of uncertainty amongst targeted populations, making it nearly impossible for individuals to ascertain whether they are under surveillance. This uncertainty could fuel self-censorship and alters behaviours, as individuals pre-emptively restrict their expression or association to avoid potential repercussions. Such an environment of fear may deter civic engagement and weaken democratic accountability.

Cases outlined earlier in this chapter allege the use of spyware against individuals the world over and assert fundamental human rights beyond privacy were violated, including the right to freedom from torture,³⁹⁸ the right to due process³⁹⁹ and the rights to freedom of expression, peaceful assembly and opinion.⁴⁰⁰ The targeting of voices of political dissent,

395 Ibid.

396 A/HRC/51/17, The right to privacy in the digital age report of the Office of the United Nations High Commissioner for Human Rights, 4 August 2022, <https://docs.un.org/A/HRC/51/17>

397 Privacy International, ‘Data Protection Principles’, September 2018, <https://privacyinternational.org/sites/default/files/2018-09/Part%203%20-%20Data%20Protection%20Principles.pdf>

398 “In August 2017, Yusuf was summoned, detained, and tortured three times by the Bahraini National Security Agency”, in Bindmans, “Prominent blogger launches lawsuit against Bahrain and NSO Group over spyware”, December 2022, <https://www.bindmans.com/news-insights/news/blogger-launches-lawsuit-against-bahrain-and-nso/>; Alex MacDonald, ‘UK Supreme Court says no state immunity for Bahrain in surveillance case’, Middle East Eye, July 2026, <https://www.middleeasteye.net/news/supreme-court-says-no-state-immunity-bahrain-uk-surveillance-case>; UK Supreme Court, The Kingdom of Bahrain (Appellant) v Shehabi and another (Respondents), July 2026, https://supremecourt.uk/uploads/uksc_2024_0152_judgment_a1ae6cd3a5.pdf

399 Human Rights Watch, ‘NO JUSTICE IN BAHRAIN: Unfair Trials in Military and Civilian Courts’ 28 February 2012, <https://www.hrw.org/report/2012/02/28/no-justice-bahrain/unfair-trials-military-and-civilian-courts>; Human Rights Watch, ‘Bahrain: Hundreds Railroaded in Unjust Trials’, 28 February 2012, <https://www.hrw.org/news/2012/02/28/bahrain-hundreds-railroaded-unjust-trials>

400 Columbia University Global Freedom of Expression, ‘“Al-Masariir v. Saudi Arabia” Case Analysis’, 2026 <https://globalfreedomofexpression.columbia.edu/cases/al-masariir-v-saudi-arabia/>;

including journalists, activists and opposition figures, has pushed people around the world into exile and underground. These examples speak to the extent of the implications of individual and collective societal civic freedoms that the use of this technology use can have.

Given the covert and highly sophisticated nature of these technologies, infection by spyware is notoriously difficult to detect and prove. Even when it can be conclusively proven, it remains very difficult to attribute the infection to the actor who carried out the infiltration.⁴⁰¹ As a consequence, the victim's right to an effective remedy becomes elusive, and effective redress and accountability may be undermined.

As outlined in the GCC case study of this chapter, litigation from spyware victims to force accountability on the part of certain Gulf states has opened potential, albeit slow and arduous, avenues for a solution. Nonetheless, redress remains well out of reach of most people who are subject to the use of spyware.

The plethora of risks associated with spyware use include what has been termed "vertical" use (by governments against their own populations) and "diagonal" use (against the population of other governments, including diaspora).⁴⁰² These terms speak to the emerging trend of spyware as a key tool for the conduct of transnational repression, as identified by Freedom House, which stated in 2026 that: "[a]t least 19 of the 48 state perpetrators of transnational repression identified by Freedom House have used spyware to monitor the communications and movements of dissidents living abroad".⁴⁰³

The transnational nature of the use of spyware, whose remote installation and operation is a characteristic feature of the technology, further raises questions over interference with state sovereignty and nations' ability to defend their populations against this type of attack. Furthermore, the fundamental right to seek asylum can also be undermined by the use of spyware. As we have seen in the GCC cases, the granting of international protection to individuals fleeing persecution may not be effective in protecting them from ongoing persecution or abuse through the use of spyware.

As noted by the CoE Commissioner for Human Rights, there is scant evidence that spyware has effectively prevented serious crimes, while abundant proof exists of its use against ordinary citizens, activists, journalists, and opposition figures.⁴⁰⁴ This misuse is exacerbated by governmental opacity and lack of cooperation in investigations, which shields perpetrators and entrenches spyware as a tool for undermining civil liberties and suppressing dissent.⁴⁰⁵

401 See "How does spyware work?" in Chapter 3 of this report.

402 Jen Roberts et. al., 'Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights', Atlantic Council, 4 September 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/#executive-summary>

403 Freedom House, 'TNR Watch: Delivering Accountability for Spyware Abuse', February 2026 <https://freedomhouse.org/article/tnr-watch-delivering-accountability-spyware-abuse>

404 Council of Europe Commissioner for Human Rights, 'Highly intrusive spyware threatens the essence of human rights', The Council of Europe, January 2023, https://www.coe.int/en/web/commissioner/blog/2023/-/asset_publisher/aa3hyf8wKBn/content/highly-intrusive-spyware-threatens-the-essence-of-human-rights

405 Ibid.

Conclusions

With the above concerns in mind, PI recommends:

1. The banning or severe curtailment of government hacking capabilities. The use of spyware has the potential to be incredibly intrusive, permitting a government remotely and in secret to access personal devices and all the intimate information they store. As such it is difficult to foresee a circumstance where spyware would meet the standards and requirements set under international human rights law.
2. If spyware use is to be permitted, it should only be under the strict safeguards we propose,⁴⁰⁶ including meeting the requirements of: (1) legality, (2) maintaining the security and integrity of systems, (3) necessity and proportionality, (4) prior judicial authorisation, (5) preserving the integrity of information, (6) notification, (7) destruction and return of data, (8) sufficient oversight and transparency, (9) compliance with international legal requirements for extraterritorial use, and (10) effective remedy. Further information on these safeguards is available in the paper identified in the footnote.
3. The export and transfer of certain spyware technologies should be prohibited due to their highly intrusive nature and the unique threats they pose to privacy and security. States should implement a global moratorium on the export, sale, transfer and use of certain spyware.⁴⁰⁷
4. If spyware is to be exported, its transfer should be made conditional on an appropriate legal framework and effective safeguards – including independent authorisation and oversight procedures, as well as appropriate remedial mechanisms. Furthermore, support of surveillance technologies should only be provided to countries with adequate data protection frameworks. And any transfer of surveillance capabilities should occur only after adequate human rights impact and risk assessments are carried out.
5. States should mandate and enforce know-your-vendor requirements for all those from whom they have acquired spyware, including CSVs, subsidiaries, suppliers and investors; since “the ebb and flow of corporate relationships, constant name changes, and confusing business structures, not only makes it difficult to track what is happening behind the veil with a vendor” and presents serious obstacles for transparency, accountability and redress.⁴⁰⁸
6. States should maintain comprehensive corporate registries which are openly accessible to the public in all jurisdictions, and should regulate nationally for the minimum information required in these registries, in order to foment accountability and transparency:

406 Privacy International, 'Hacking Necessary Safeguards', <https://privacyinternational.org/demand/government-hacking-safeguards>

407 Privacy International, 'Statement before the European Parliament hearing on “Spyware used in third countries and implications for EU foreign relations”, December 2022, <https://privacyinternational.org/advocacy/5002/statement-european-parliament-hearing-spyware-used-third-countries-and-implications>; Council of Europe Commissioner for Human Rights, 'Highly intrusive spyware threatens the essence of human rights', The Council of Europe, 27 January 2023, https://www.coe.int/en/web/commissioner/blog/2023/-/asset_publisher/aa3hyf8wKBn/content/highly-intrusive-spyware-threatens-the-essence-of-human-rights

408 Jen Roberts, Trey Herr, Emma Taylor, Nitansha Bansal, 'Markets matter: A glance into the spyware industry', Atlantic Council, 22 April 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/markets-matter-a-glance-into-the-spyware-industry/#takeaways>

- a. Minimum corporate registry data should include “basic company information (name, registration number, payment ID, address, contact details, and date of registration), ownership details (senior executives, management board, and actual beneficiaries), the number of employees, financial information (balance sheet, cash flow, income statements, and investors), history of name changes, and the legal status of activity (liquidated, active, or bankrupt) [...] a history of mergers and acquisitions, legal actions against the firm, and active export licenses”.⁴⁰⁹

409 Jen Roberts et. al., 'Mythical Beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights', Atlantic Council, September 2024, <https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/#executive-summary>



04

**Social Media
Intelligence
Monitoring.**

Introduction

Social media has become a prevalent part of our lives - enabling us to share and receive information, engage in debate, connect with people and co-ordinate action. It has accordingly become an important space for the exercise of human rights and can contribute to the flourishing of democracy.

This online activity creates a large and evolving record of our lives, opinions and social connections. The ability to systematically gather and analyse this record has given rise to a form of surveillance referred to as social media monitoring or social media intelligence ("SOCMINT").

SOCMINT is increasingly used by governments and non-state actors; and when deployed without appropriate safeguards, can be a powerful tool for authoritarian control. This chapter unpacks what SOCMINT is and how it can be used to undermine fundamental human rights and exert social and political control.

What is SOCMINT?

Social media intelligence (SOCMINT) refers to the techniques and technologies that enable actors to monitor social media networking sites (SNSs), such as Facebook, Instagram, X or Reddit. This includes the collection, retention, and analysis of the vast range of social media data and interpreting that data into trends, profiles and analysis.

SOCMINT includes the monitoring of user-generated content such as posts, comments and private messages. It also includes metadata and interactions such as who someone is friends with or follows, the types of posts they share or like, the groups they are part of, who they tag in photographs, and the time and location something was shared. This information includes content on a user profile or content shared between users, or by users on groups.

For more on this see: Privacy International, 'Social Media Intelligence', <https://privacyinternational.org/explainer/55/social-media-intelligence>

See also: Maltego, 'Everything About Social Media Intelligence (SOCMINT) and Investigations', <https://www.maltego.com/blog/everything-about-social-media-intelligence-socmint-and-investigations/>

How does SOCMINT work?

The methods of analysing social media networking sites vary but it can typically be done manually or by using automated tools.⁴¹⁰

SOCMINT includes two data sources - public information and private information.⁴¹¹ This

410 Liberty & Privacy International, 'Neighbourhood Watch', February 2019, <https://privacyinternational.org/sites/default/files/2019-02/Explainers-SOCMINT.pdf>; SEON, 'SOCMINT (Social Media Intelligence)', [Dictionary entry], n.d., <https://seon.io/resources/dictionary/socmint/>

411 Szde Yu, 'Cyber Profiling: Predicting Political Orientation with SOCMINT', TIR Vol 10, June 2023, <https://www.sciencedirect.com/science/article/pii/S277250302300018X>

makes it distinct from open-source intelligence (OSINT)⁴¹² which only includes publicly available information.

Manual monitoring generally entails a person sifting through online content and analysing it. Methods may include manually reviewing content as it is posted in public or private groups or pages; reviewing the results of searches and queries about users; or reviewing the activities or types of content users' post. It can also include covert monitoring⁴¹³ - where a fake profile is created to join private groups or interact with specific individuals with the intention of gaining access to information that is not publicly visible or engaging with information anonymously.

For example the police in the U.S., in Memphis, reportedly used covert SOCMINT to collect information on Black Lives Matter Activists.⁴¹⁴ By using a fake Facebook profile of "Bob Smith", police were reported to have befriended and gathered information from activists, and access a private post, as well as the names of 58 friends who liked it.⁴¹⁵ Any such attempt by law enforcement agencies or security services to covertly add the targeted user as a validated contact, to use fake profiles, to obtain further information than what is publicly available, should be treated as undercover and covert surveillance and addressed with constraints and safeguards, similar to those in place for undercover activities taking place in physical space.⁴¹⁶

Automated monitoring entails the use of software to collect and analyse data from social media sites. Information could be collected through 'scraping' – where the content of a web page is extracted by a bot and replicated in an accessible format, or using an application programming interface (API).⁴¹⁷ It is then analysed using artificial intelligence and machine learning algorithms. The use of AI for SOCMINT was discussed by Shahbaz and Funk of Freedom House.⁴¹⁸

"Advances in artificial intelligence (AI) have opened up new possibilities for automated mass surveillance. Sophisticated monitoring systems can quickly map users' relationships through link analysis; assign a meaning or attitude to their social media posts using natural-language processing and sentiment analysis; and infer their past, present, or future locations. Machine learning enables these

412 Bipun Thapa, 'Applying SOCMINT to Extract Cyber Threat Intelligence from the Russia-Ukraine Conflict', IADIS International Journal on WWW/Internet Vol 20, https://www.researchgate.net/profile/Bipun-Thapa/publication/369830337_APPLYING_SOCMINT_TO_EXTRACT_CYBER_THREAT_INTELLIGENCE_FROM_THE_RUSSIA-UKRAINE_CONFLICT/links/642ed099ad9b6d17dc3d1b91/APPLYING-SOCMINT-TO-EXTRACT-CYBER-THREAT-INTELLIGENCE-FROM-THE-RUSSIA-UKRAINE-CONFLICT.pdf

413 Raymond James Todd, 'Using Covert Research Accounts in OSINT Investigations', UK OSINT Community, 2 September 2024, <https://www.osint.uk/content/using-covert-research-accounts-in-osint-investigations>

414 George Joseph, 'Memphis Police Collected Black Lives Matter Activists' Private Facebook Posts', 27 July 2018, <https://theappeal.org/memphis-police-collected-black-lives-matter-activists-private-facebook-posts/>

415 Ibid.

416 Privacy International, 'Social Media Monitoring in the UK: The Invisible Surveillance Tool Increasingly Deployed by Government', 2024, <https://privacyinternational.org/long-read/5337/social-media-monitoring-uk-invisible-surveillance-tool-increasingly-deployed>

417 Johanna Isabella Stegen, 'Leveraging Social Media Intelligence (SOCMINT) in the African Intelligence Context', Journal of Policing, Intelligence and Counter Terrorism Vol. 20, 17 February 2025, <https://www.tandfonline.com/doi/full/10.1080/18335330.2025.2465529#abstract>

418 Adrian Shahbaz and Allie Funk, 'Social Media Surveillance', Freedom House, 2019, <https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance>

systems to find patterns that may be invisible to humans, while deep neural networks can identify and suggest whole new categories of patterns for further investigation."

Why is it concerning?

The least regulated aspect of social media intelligence relates to the monitoring of publicly available data on social networking sites. In the context of social media, information is considered publicly available when it is accessible not only to your contacts, but to people or organisations who are not logged into a social media network, or when a person or organisation is logged in but is not a validated contact (e.g. a "friend" on Facebook or a "follower" on 'X').⁴¹⁹ Furthermore, there is a distinction between what is referred to as "overt" and "covert" social media intelligence. "Overt" surveillance relies on publicly available information, whereas "covert" surveillance involves attempts to add the targeted user as a validated contact, to use fake profiles, to obtain further information than what is publicly available.⁴²⁰

However, just because the information is public, doesn't mean it's fair game. Social media platforms, where data is posted online, engage individual privacy - the collection, retention, use, and sharing of a person's personal data is intrusive. By way of example, 'tweets' posted from a mobile phone can reveal location data, and their content can also reveal individual opinions (including political opinions) as well as information about a person's preferences, sexuality, and health status. However, law enforcement and other security agencies argue that social media intelligence has little impact on people's privacy as and when it relies "only" on publicly available information.⁴²¹ This has led to a situation where law enforcement officials and intelligence agencies may believe that everything that a given social networking website sets as publicly available is fair game for them to access, collect, and process with very limited regulation, oversight, or safeguards.⁴²² This inaccurate representation fails to account for the intrusive nature of collection, retention, use, and sharing of a person's personal data. Furthermore, PI is concerned that the safeguards designed specifically to govern the use of "overtly" collected intelligence are often lacking. Our research indicates that most public authorities in the UK who use overt social media monitoring appear to have no processes or procedures in place to audit this surveillance tactic and 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.⁴²³ Further,

419 Privacy International, 'Social Media Monitoring in the UK: the Invisible Surveillance Tool Increasingly Deployed by Government', 17 July 2024, <https://privacyinternational.org/long-read/5337/social-media-monitoring-uk-invisible-surveillance-tool-increasingly-deployed>

420 Privacy International, 'Written submission to the European Court of Human Rights *Salman BUTT v. the United Kingdom* Application no. 32946/20', 5 March 2021, <https://privacyinternational.org/sites/default/files/2021-06/PI%20Intervention%20-%20Butt%20v.%20UK-Final.pdf>

421 Ibid.

422 Ibid.

423 Privacy International, 'Social Media Monitoring in the UK: the Invisible Surveillance Tool Increasingly Deployed by Government', 17 July 2024, <https://privacyinternational.org/long-read/5337/social-media-monitoring-uk-invisible-surveillance-tool-increasingly-deployed>; Privacy International, 'Written submission to the European Court of Human Rights *Salman BUTT v. the United Kingdom* Application no. 32946/20', 5 March 2021, <https://privacyinternational.org/sites/default/files/2021-06/PI%20Intervention%20-%20Butt%20v.%20UK-Final.pdf>

there is often no requirement to obtain prior authorisation when conducting “overt” social media monitoring by public authorities and law enforcement agencies.⁴²⁴

What can make the use of SOCMINT authoritarian?

SOCMINT can be used in ways that have a grave impact on human rights and create a chilling effect on society that we consider amounts to an authoritarian use. This includes when it is used, for example, as a tool for mass surveillance, to interfere with protests and to surveil specific communities. In this section, we unpack the three major ways this happens with SOCMINT.

SOCMINT can be used to exert social and political control when used as a mass surveillance tool. Social media contains a staggering amount of data. According to the 2024 Data Never Sleeps report, 16,000 videos are uploaded to Tik Tok and 138.9 million reels are played on Facebook and Instagram every minute.⁴²⁵ By systematically collecting and analysing this data, actors can build a detailed and permanent record of individuals lives - their views, their connections and locations. This can be done for each of the 5.24 billion social media users.⁴²⁶ The availability of this data enables a shift from targeted surveillance to mass, indiscriminate surveillance. Information can be collected and digital dossiers created on an individual “before the relevance, use or the user’s role as a suspect have been determined.”⁴²⁷

This information asymmetry creates a power imbalance which makes it easier to exert political and social control. As noted by Richards:⁴²⁸

“[...] the gathering of information affects the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance. It might sound trite to say that “information is power,” but the power of personal information lies at the heart of surveillance. The power effects of surveillance illustrate three additional dangers of surveillance: blackmail, discrimination and persuasion.”

The exertion of this political control is evidenced through the use of SOCMINT to predict and deter protests, discussed below. Such use is also a distinct example of an authoritarian use of the technology.

Research by Gabriel Grill from 2021 examined the products and discourses of civil unrest predictions based on social media data. The research found that most civil unrest

424 Ibid.

425 DOMO, ‘Data Never Sleeps’, 2024, <https://www.domo.com/learn/infographic/data-never-sleeps-12>

426 Digitalnrg, ‘Top Social Media Statistic Insights for 2025: What You Need to Know’, 5 February 2025, <https://www.digitalnrg.co.uk/top-social-media-statistic-insights-for-2025/>

427 Lina Dencik, Arne Hintz, Zoe Carey, Hina Pandya, ‘Managing ‘Threats’: Uses of Social Media for Policing Domestic Extremism and Disorder in the UK’, Cardiff School of Journalism, Media and Cultural Studies, October 2015, pg. 9, <https://eprints.goldsmiths.ac.uk/id/eprint/37315/1/Managing-Threats-Project-Report.pdf>

428 Neil M. Richards, ‘The Dangers of Surveillance’, The Harvard Law Review Association vol. 126, no. 7, 2013, pg. 1934–65, <https://www.jstor.org/stable/23415062>

predictions targeted “all kinds of protests”, marking them as risky.⁴²⁹ According to Grill, this “could result in various detrimental treatments such as preemptive interventions, policing, increased surveilling, and targeting of individuals and groups”.⁴³⁰ Importantly, Grill noted that “users of civil unrest prediction are usually in positions of power, such as law enforcement officials or big companies, and seemingly aim to employ the technology to mitigate and pre-empt protest before it becomes risky or disruptive. The thresholds for when protests become too risky are unclear.”⁴³¹

Furthermore, the use of SOCMINT can have a chilling effect on the exercise of certain human rights. The right to privacy enables us to explore ideas, make mistakes and form our identities - free from observation.⁴³² Because of this, privacy is considered an enabler of other rights - “it is a necessary condition for freedom of expression, thought, religion, assembly, and association.”⁴³³ When people are aware that their conversations, likes and associations are being monitored, and may form part of a record, they may self-censor⁴³⁴ out of fear that the information may be misinterpreted or used against them.

Consequently, individuals may refrain from criticising authority, engaging in controversial debate or accessing certain information. This erodes personal autonomy and the freedom to develop as an individual. This fear and self-censorship extend to freedom of association and assembly as people may become hesitant to join an online group, sign a petition or express interest in a protest. Activists, journalists and human rights defenders who aim to hold government to account may be more inclined to censor,⁴³⁵ undermining their role in accountability. In a study on data retention, it was found that “under pervasive surveillance, individuals are inclined to make choices that conform to mainstream expectations,”⁴³⁶ demonstrating the use of surveillance to control behaviour.

Such conformity and self-censorship discourage participation in political discourse, shrinks the space for dissent and ultimately undermines the marketplace of ideas.

It warrants underlining that members of certain communities can be disproportionately harmed⁴³⁷ by SOCMINT use in violation of the prohibition against discrimination and undermining the right to equality. This includes Black and Indigenous communities, people of colour, women LGBTQ+ individuals, immigrants and people with disabilities; all groups

429 Gabriel Grill, ‘Future Protest Made Risky: Examining Social Media Based Civil Unrest Prediction Research and Products’, Computer Support Coop Work, 8 September 2021, pg. 827, <https://pmc.ncbi.nlm.nih.gov/articles/PMC8423833/>

430 Ibid.

431 Ibid.

432 United Nations Office on Drugs and Crime, ‘Privacy: What is its and why it is Important’, <https://www.unodc.org/cld/zh/education/tertiary/cybercrime/module-10/key-issues/privacy-what-it-is-and-why-it-is-important.html>

433 Ibid.

434 Neil M. Richards, ‘The Dangers of Surveillance’, The Harvard Law Review Association vol. 126, no. 7, 2013, pg. 1934–65, <https://www.jstor.org/stable/23415062>

435 Adrian Shahbaz and Allie Funk, ‘Social Media Surveillance’, 2019, <https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance>

436 Lilian Mitrou, ‘The Impact of Communications Data Retention on Fundamental Rights and Democracy — The Case of the EU Data Retention Directive’, Surveillance and Democracy, 2010, <https://www.taylorfrancis.com/chapters/edit/10.4324/9780203852156-15/impact-communications-data-retention-fundamental-rights-democracy-case-eu-data-retention-directive-lilian-mitrou>

437 Electronic Privacy Information Center, ‘Privacy and Racial Justice’, <https://epic.org/issues/democracy-free-speech/privacy-and-racial-justice/>

that have undergone longstanding and systemic discrimination.⁴³⁸ The automated tools used to analyse data collected from social media may reflect existing prejudices, meaning the algorithms may learn to associate certain racial, ethnic or religious groups with higher risk or criminality. "Even if not intentional, structural racism is embedded in the design and implementation of technology. Under representative data sets, biased training data, implicit bias of coders and designers, and a lack of transparency and accountability are some factors that affix racism in technology."⁴³⁹ These communities are often already subject to greater scrutiny from law enforcement⁴⁴⁰ and the use of SOCMINT contributes to a surveillance cycle where they are monitored more intensely, their data is interpreted more negatively and they are flagged for suspicion at a higher rate. This is evidenced by the covert monitoring conducted on Black Lives Matter activists discussed above.⁴⁴¹

Examples of the authoritarian use of SOCMINT

United States (US)

In June 2025, the US Department of State announced that it would expand the screening and vetting process of student visa applicants to include applicants' social media.⁴⁴² The announcement included an instruction for all applicants to "adjust the privacy settings on all of their social media profiles to 'public'."⁴⁴³

According to an announcement by the US Embassy in Mali, visa applicants are required to disclose all of their social media usernames and handles for every platform they have used in the last 5 years.⁴⁴⁴ Officials have reportedly⁴⁴⁵ been instructed to search for "any indications of hostility toward the citizens, culture, government, institutions, or founding principles of the United States" and any "history of political activism."⁴⁴⁶

The move is part of what some commentators have referred to as Trump's defining initiative of his second term - ideological vetting.⁴⁴⁷ Such social media surveillance has been utilised in the USA for visa and immigration for over a decade, but is reportedly becoming "more

438 Eduwik, 'How AI Bias Affects Marginalized Communities', 5 August 2025, <https://eduwik.com/how-ai-bias-affects-marginalized-communities/>

439 Electronic Privacy Information Center, 'Privacy and Racial Justice', <https://epic.org/issues/democracy-free-speech/privacy-and-racial-justice/>

440 T Jones and M Maguire, 'Crime, Community Safety and the Policing of Marginalised Populations: A Review of Research, Unpublished paper', 1999, <https://gsdrc.org/document-library/crime-community-safety-and-the-policing-of-marginalised-populations-a-review-of-research/>

441 Raymond James Todd, 'Using Covert Research Accounts in OSINT Investigations', UK OSINT Community, 2 September 2024, <https://www.osint.uk/content/using-covert-research-accounts-in-osint-investigations>

442 U.S. Department of State, 'Announcement of Expanded Screening and Vetting for Visa Applicants', 18 June 2025, <https://www.state.gov/releases/office-of-the-spokesperson/2025/06/announcement-of-expanded-screening-and-vetting-for-visa-applicants>

443 Ibid.

444 U.S. Embassy in Mali, 'Updated Social Media Disclosure Requirement for F, M, J Visa Applicants', 24 June 2025, <https://ml.usembassy.gov/u-s-requires-public-social-media-settings-for-f-m-and-j-visa-applicants/>

445 Nadine Yousif, 'US Resumes Student Visa but Orders Enhanced Social Media Vetting', BBC News, 18 June 2025, <https://www.bbc.co.uk/news/articles/cgrxyx0qr7eo>

446 Rachel Levinson-Waldman and Naz Balkam, 'The Government's Growing Trove of Social Media Data', Brennan Center for Justice, 21 July 2025, <https://www.brennancenter.org/our-work/research-reports/governments-growing-trove-social-media-data>

447 Ibid.

pervasive and ideologically driven.”⁴⁴⁸ An applicant who intends to apply for such a visa in a few years’ time will likely self-censor out of fear that their information may be misinterpreted or used to deny their entry. Consequently, they are unlikely to engage in any political activity or engage with dissenting content. These consequences have been highlighted in a recent legal challenge.

In October 2025, several trade unions launched a legal action against the United States Department of State, ICE and others contending that their surveillance program violates the First Amendment (religion, speech, press, and assembly) and the Administrative Procedure Act.⁴⁴⁹ Through the action, they seek a declaration that the program is unconstitutional and unlawful and have requested an injunction against the continued operation of the program and use of the already collected online expression.

The subject matter of the complaint concerns “the interagency federal program between the U.S. Department of Homeland Security and U.S. Department of State whereby the government (1) surveils expressive activity documented online of millions of individuals—primarily U.S. based visa holders and Lawful Permanent Residents—in order to detect disfavoured viewpoints and to take adverse immigration based on those viewpoints, and (2) coerces silence by threatening to engage in such viewpoint-targeted online surveillance and related adverse immigration action.”⁴⁵⁰ The surveillance program is allegedly targeting every visa holder in the United States, with a focus on those with campus affiliations.⁴⁵¹

Importantly, the complaint focuses on the chilling effect of the program, noting:⁴⁵²

“Taken as a whole, the Challenged Surveillance Program is having its intended effect: suppressing the speech of thousands of U.S.-based visa holders, Lawful Permanent Residents, and others with immigration status, as well as their family members, friends, and colleagues in the U.S. seeking to protect them. Noncitizens throughout the U.S. are cancelling their social media accounts, erasing past social media and online posts and interactions, and forgoing future posting and other expression that may be documented online. Citizens are similarly refraining from speaking out online for fear of making targets of their family members, friends and colleagues.”

The Plaintiffs argue that this has undermined people’s ability to engage in activities and associate with unions. This is exemplified by a ceased affiliation with unions, hesitation to attend events and a removal or change in how members engage with unions online.

As noted in the challenge, this surveillance program is allegedly conducted to identify and

448 Brennan Centre for Justice, ‘Timeline of Social Media Monitoring for Vetting by the Department of Homeland Security and the State Department’, 25 June 2025, <https://www.brennancenter.org/our-work/research-reports/timeline-social-media-monitoring-vetting-department-homeland-security-and>

449 Case 25-cv-8566 International Union, ‘United Automobile, Aerospace and Agricultural Implement Workers of America & Others V. United States Department of State’, Complaint: https://www.eff.org/files/2025/10/16/uaw_v_dos_-_complaint.pdf

450 Ibid., para. 11.

451 Ibid., para. 30.

452 Ibid., para. 5.

punish noncitizens who express views that are disliked by the government.⁴⁵³

We contend that such a surveillance program could amount to an authoritarian use of SOCMINT. The government is exerting significant social and political control by threatening a severe consequence - adverse immigration action - for anyone who has certain political or ideological views that they disfavoured. Such threat is being used to undermine democratic principles and human rights, and creates a chilling effect on expression. Out of fear of reprisal, individuals are curtailing, amending or ceasing to exercise their freedom of expression, which in turn undermines the rights of others to access information. They are also adjusting their engagement or association with certain groups - for example, the trade unions bringing the challenge, - which undermines their freedom of association. Such control is being exercised against a targeted group of non-citizens.

Mexico

There have been reports of social media monitoring by the military in Mexico as part of wider military operations in cyberspace by the "Centro de Operaciones del Ciberespacio", whose activities are not part of the legal framework in Mexico, raising concerns about how these powers will be used and who they will target.⁴⁵⁴

Israel

In 2023, Israel passed an amendment to its counterterrorism law which introduced the "consumption of terrorist materials" as a criminal offence.⁴⁵⁵ In terms of the law, Hamas was identified as one of the terrorist groups the offence applied to. Since there have reportedly been hundreds of arrests concerning social media activity.⁴⁵⁶ Such arrests are likely only possible through the monitoring of social media.

SOCMINT is often used to monitor and enforce compliance with these laws because support for and association with groups is often done through social media. Out of fear of fear reprisal, individuals are likely to self-censor.

Turkey

During the state crackdown against protestors following Istanbul Mayor Ekrem İmamoğlu's arrest in March 2023, hundreds of people - mainly university students - were detained in night raids at their homes for charges including **sharing boycott calls and protest-related content on social media**.⁴⁵⁷ Of these students at least 20 were formally charged with

453 Case 25-cv-8566 International Union, United Automobile, Aerospace and Agricultural Implement Workers of America & Others V. United States Department of State, Complaint, para. 240, https://www.eff.org/files/2025/10/16/uaw_v_dos_-_complaint.pdf

454 R3D, 'Ejército de Bots: Las operaciones militares para monitorear las críticas en redes sociales y manipular la conversación digital', 27 February 2024, <https://r3d.mx/2024/02/27/ejercito-de-bots-las-operaciones-militares-para-monitorear-las-criticas-en-redes-sociales-y-manipular-la-conversacion-digital/>

455 AlJazeera, 'Israeli Parliament Bill Criminalises 'consumption of Terrorist Materials'', 8 November 2023, <https://www.aljazeera.com/news/2023/11/8/knesset-introduces-consumption-of-terrorist-publication-as-offense>

456 Lorenzo Tondo and Sufian Taha, 'My Arrest was Unjustified': Release Palestinians Decry their Imprisonment', The Guardian, 20 January 2025, <https://www.theguardian.com/world/2025/jan/20/my-arrest-was-illogical-released-palestinians-decry-their-imprisonment>; See also: Sara Monetta, Israeli Arabs arrested over Gaza social media posts, 21 October 2023, <https://www.bbc.co.uk/news/world-middle-east-67181582>

457 Human Rights Watch, 'Türkiye: Students, Journalists on Trial for Protest', April 2025 <https://www.hrw.org/news/2025/04/17/turkiye-students-journalists-trial-protest>

"inciting a crime" under Turkish Penal Code Article 214 for social media posts that Human Rights Watch found were largely just non-violent calls to join demonstrations.⁴⁵⁸

Colombia

In 2021, in the aftermath of the pandemic and after widespread protests in Colombia, a specific law enforcement unit used social media monitoring to gather information on protesters.⁴⁵⁹ The Attorney General's Office reportedly stated that the activities of this law enforcement unit - known domestically as the PMU-Ciber - were aimed at the "constant monitoring of social networks such as Facebook, Twitter and Instagram as well as any other which would enable the police to establish the opinion and trends that may present during the development of a social protest".⁴⁶⁰ You can find out more about this case in a report published by Dejusticia in which they warned about the lack of existing safeguards and regulation of the use of social media intelligence by intelligence agencies.⁴⁶¹

United Kingdom (UK)

In the UK, it was reported that in 2013 police in London monitored almost 9,000 activists it has deemed as "domestic extremists" using data scraped from social media platforms, in order to compile secret dossiers on each activist, despite many of them having no criminal background.⁴⁶² Over a decade later, the UK government proscribed Palestine Action⁴⁶³ as a terrorist organisation under section 3 of the Terrorism Act 2000. The ban, among other things, makes it a criminal offence to be a member of Palestine Action, express support for the group, or wear an item of clothing that would arouse "reasonable suspicion" that a person is a member of or supports the organization.⁴⁶⁴ Such conduct would include expressing support on social media, and is "punishable by criminal penalties, including fines and prison sentences of up to 14 years."⁴⁶⁵ This move has been characterised as a "dangerous escalation in the criminalisation of political dissent in the UK and represents an increase in the UK's architecture of surveillance."⁴⁶⁶ It has been severely criticised, including by the UN Human Rights Chief, Volker Türk, who noted:⁴⁶⁷

458 Ibid.

459 Carolina Botero, 'Poniéndoles el ojo a los PMU-Ciber: ¿qué son y para qué sirven in La Silla Vacía', April 2022 <https://www.lasillavacia.com/red-de-expertos/red-de-ciencia-e-innovacion/poniendoles-el-ojo-a-los-pmu-ciber-que-son-y-para-que-sirven/>

460 Ibid, translated from Spanish by PI.; See: Lucía Camacho-Gutiérrez, Daniel Ospina-Celis, Juan Carlos Upegui-Mejía – Bogotá, Editorial Dejusticia, State Intelligence Gathering on the Internet and Social Media: The Case of Colombia, November 2023, <https://www.dejusticia.org/wp-content/uploads/2024/01/StateIntelligence-Web.pdf>

461 Ibid.

462 Paul Lewis, Rob Evans and Vikram Dodd, 'National police unit monitors 9,000 'domestic extremists'', The Guardian, 2013 <https://www.theguardian.com/uk/2013/jun/25/undercover-police-domestic-extremism-unit>

463 UK Parliament, 'Palestine Action: Proscription', Hansard Volume 769, 23 June 2025, <https://hansard.parliament.uk/commons/2025-06-23/debates/25062337000014/PalestineActionProscription>

464 As per the UK Terrorism Act 2000

465 United Nations Human Rights Office of the High Commissioner, 'Press Release: UK Palestine Action ban 'disturbing' misuse of UK counter-terrorism legislation, Turk warns', <https://www.ohchr.org/en/press-releases/2025/07/uk-palestine-action-ban-disturbing-misuse-uk-counter-terrorism-legislation>

466 Open Rights Group, 'Banning Palestine Action: How the UK Government is Silencing Dissent', 4 July 2025, <https://www.openrightsgroup.org/blog/banning-palestine-action-how-the-uk-government-is-silencing-dissent/>

467 United Nations Human Rights Office of the High Commissioner, 'Press Release: UK Palestine Action ban 'disturbing' misuse of UK counter-terrorism legislation, Turk warns', 25 July 2025, <https://www.ohchr.org/en/press-releases/2025/07/uk-palestine-action-ban-disturbing-misuse-uk-counter-terrorism-legislation>

"The decision appears disproportionate and unnecessary. It limits the rights of many people involved with and supportive of Palestine Action who have not themselves engaged in any underlying criminal activity but rather exercised their rights to freedom of expression, peaceful assembly and association," [...] "As such, it appears to constitute an impermissible restriction on those rights that is at odds with the UK's obligations under international human rights law [...] "The decision also conflates protected expression and other conduct with acts of terrorism and so could readily lead to further chilling effect on the lawful exercise of these rights by many people." According to Türk, the move raises concerns that counter-terrorism laws are being applied to conduct which is not terrorist in nature, which poses a risk to the legitimate exercise of rights.

As a result of this, campaigners have highlighted a troubling trend of increased content removals across social media platforms such as Instagram, TikTok and X.⁴⁶⁸ These platforms have reportedly utilised algorithms that "obscure posts sympathetic to Palestinian causes", and that those who express their political beliefs online have been subject to police scrutiny.⁴⁶⁹

The UK Department for Education (DfE) was also found to have kept files monitoring the social media activity of UK based academics.⁴⁷⁰ The academics uncovered files held by the DfE on them, some of which were up to 60 pages. One academic found their file included critical tweets she had posted about the UK school inspectorate (The Office for Standards in Education, Children's Services and Skills) and flagged she had "liked" other social media posts promoting guidance about teaching young children that was written by educationists (in stead of by the government).⁴⁷¹ One academic also found an Excel spreadsheet in which DfE officials had detailed which people she had interacted with.⁴⁷² This monitoring also had led to an attempt by the DfE to cancel a conference because two of the speakers had criticised the government's policy.⁴⁷³

In 2019, PI investigated the use of overt SOCMINT by Local Authorities in the UK and found that 62.5% of Local Authorities that responded to freedom of information requests were using overt social media monitoring, while 31% were using covert social media monitoring.⁴⁷⁴ Our research revealed that Local Authorities could monitor social media accounts, such as Facebook, as part of their intelligence gathering and investigation tactics regarding subjects as diverse as council tax payments, children's services, benefits, and monitoring protests and demonstrations. In some cases, local authorities will go so far as to

468 Al Jazeera, 'The Question of Palestine Action's Digital Presence', 4 March 2026, <https://liberties.aljazeera.com/en/the-question-of-palestine-actions-digital-presence/>

469 Ibid.

470 Anna Fazackerley, 'Revealed: UK government keeping files on education critics' social media activity', The Guardian, 30 September 2023, <https://www.theguardian.com/education/2023/sep/30/revealed-uk-government-keeping-files-on-education-critics-social-media-activity>

471 Ibid.

472 Ibid.

473 Ibid.

474 Privacy International, 'When Local Authorities aren't your Friends', 24 May 2020, <https://privacyinternational.org/report/3584/when-local-authorities-arent-your-friends>

use such information to make accusations of fraud and withhold urgently needed support from families who are living in extreme poverty.⁴⁷⁵ Our research indicates that the large majority of public 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 SOCMINT is being used nor are therefore able to assess whether it is being used in a way that is legitimate, necessary, proportionate and effective.⁴⁷⁶

Human rights and data protection implications

Social media monitoring raises serious risks for individuals' fundamental rights as well as for the functioning of modern democracies. Social media platforms have come to play a vital role for the development of individuals' private social and political life, as well as their online identity. 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, environmental, and cultural change. Because of this, social media platforms have been referred to as the new marketplace of ideas or the "modern public square."⁴⁷⁷ However social media can, as documented above, be the source of governments to interfere directly with individuals right to privacy, freedom of expression, association and assembly. This has also been noted by the UN and other authoritative bodies.

Indeed, the UN Office of the High Commissioner on Human Rights (OHCHR) has stated how "globally, many authorities are collecting and analysing social media posts... such social media intelligence ranges from the investigation of specific users to dragnet collection, storage and analysis of vast amounts of data".⁴⁷⁸ They further noted that, even though the activities monitored are occurring on open social media platforms, individuals should have a space free from systematic observation and intrusion, in particular by government entities.⁴⁷⁹

Furthermore, the OHCHR noted that often, various types of predictive analytics form part of social media intelligence practices to assess the past, present and future behaviour of individuals including the likelihood that they may become offenders or security threats in the future as well as to make predictions about possible social unrest,⁴⁸⁰ asserting that: "These activities can serve manifold legitimate and illegitimate objectives, from crime investigation and prevention to vetting applicants for social benefits, monitoring protests, measuring public sentiment and profiling people's social conduct".⁴⁸¹

The UN Human Rights Committee has also acknowledged how social media monitoring can interfere with the right to peaceful assembly:

475 Ibid.

476 Ibid.

477 Case No. 15-1194, *Packingham v North Carolina*, pg. 8, https://www.supremecourt.gov/opinions/16pdf/15-1194_0811.pdf

478 A/HRC/51/17, *The right to privacy in the digital age*, report of the Office of the United Nations High Commissioner for Human Rights, 4 August 2022, para. 35, <https://docs.un.org/en/A/HRC/51/17>

479 Ibid.

480 Ibid., para. 36.

481 Ibid., para. 37.

*"The mere fact that assemblies take place in public does not mean that participants' privacy is not capable of being infringed...The same applies to the monitoring of social media to glean information about participation in peaceful assemblies. Independent scrutiny and oversight must be exercised over the collection of personal information and data of those engaged in peaceful assemblies".*⁴⁸²

The UN Special Rapporteur on freedom of assembly and of association has documented the "systematic monitoring of social media activity"⁴⁸³ and how "civil society actors, including those from major international human rights organisations, described how they dismantled visible public-facing profiles and withdrew from social media".⁴⁸⁴ As well as how they felt they had to restrict their social media engagement including what websites a person visits, searches they conduct, meetings they attend (including on-line), who they talk to or what they say, what public or private social activities they engage in, and if (or how) they participate in democratic processes and political activities, among others.⁴⁸⁵ The special rapporteur also documented "the remote identification of individuals at protests or through monitoring online social media activity."⁴⁸⁶ This was documented in Cuba where activists had house visits from law enforcement within 30 minutes of posting material online that was critical of the government.⁴⁸⁷ Forced erasure of one's social media presence was also apparent in other regions, as one southeast Asia-based activist explained, "Yeah, I deleted my Facebook account. I had 150,000 people following me. I deleted it. I deleted everything about me on social media".⁴⁸⁸

At the regional level, the European Data Protection Supervisor (EDPS), who monitors the processing of personal data by European institutions and bodies has also commented on the human rights and data protection concerns with SOCMINT. The EDPS has provided that:

*[Social media monitoring] involves uses of personal data that go against or beyond individuals' reasonable expectations. Such uses often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate.*⁴⁸⁹

The EDPS further underscored:

Social media users monitoring is a personal data processing activity that creates high risk

482 CCPR/C/GC/37, Human Rights Committee, General comment No. 37 on the right of peaceful assembly (article 21), 17 September 2020, para 62, <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>

483 Gina Romero et. al., "'PUSHED INTO THE SHADOWS'": Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association', United Nations Special Procedures, 2026, pg. 12, <https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf>

484 Ibid., pg. 62.

485 Ibid., pg. 22.

486 Ibid., pg. 33.

487 Ibid., pg. 33.

488 Ibid., pg. 63.

489 European Data Protection Supervisor, Formal consultation on EASO's social media monitoring reports (case 2018-1083), pg.3, https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf

for individuals' rights and freedoms [...] Repurposing of data is likely to affect a person's information self-determination, further reduce the control of data subjects' over their data [...] Indeed, the diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health of democracy.⁴⁹⁰

Conclusions

As evidenced by these examples, governments and non-state actors are deploying SOCMINT. In its authoritarian form, it poses a direct threat to human rights, systematically undermining the right to privacy, creating a chilling effect that suppresses freedom of expression and assembly, and disproportionately harming marginalised communities through biased targeting. When deployed without rigorous legal oversight and public accountability, SOCMINT becomes a powerful instrument of authoritarian control, eroding the trust, autonomy, and open discourse that are essential for democracy.

SOCMINT should not be deployed in authoritarian ways, and its use should be regulated to mitigate against abuse, including according to these recommendations:

1. SOCMINT collection, analysis, and retention must be governed by a **clear legal framework which includes explicit provision for this technology's use** (rather than being governed by internal policies) and includes a national data protection law and independent national data protection authority.
2. **Necessity, minimisation and proportionality, applied case-by-case:** SOCMINT must be justified against a specific, articulable threshold (e.g., reasonable suspicion of serious criminal conduct) rather than deployed as blanket, population-wide monitoring. Programs that scan "all visa holders" or "all protest attendees" fail proportionality regardless of stated security aims.
3. States must **prohibit the use of SOCMINT on individuals based on political opinion**, religion, national origin, migration status, or participation in lawful protest or association.
4. **Independent prior authorisation:** Collection of SOCMINT must be subject to robust oversight by requiring prior authorisation based on reasonable suspicion, and assessing necessity and proportionality, from an independent body (court, judicial commissioner) with the power to deny, limit, or set conditions.
5. SOCMINT scraped data and the dossiers built from it must have **fixed retention periods** with clear timelines for mandatory deletion, and states should establish accessible mechanisms for individuals to seek expungement of unlawfully or excessively retained records.
6. Agencies using SOCMINT should be required to publish **regular transparency reports** disclosing numbers monitored, which tools were used, the vendors contracted, and legal basis invoked.

⁴⁹⁰ Ibid.

7. Independent oversight: an independent body should be given the power to oversee the use of SOCMINT, including auditing and interrogating its use, investigating errors, issuing binding decisions, and providing public reporting as described above.
8. Individuals subject to SOCMINT-derived action (e.g. denial of a public benefit, arrest, deportation) should have a **right to be informed of the evidence against them** and access to an effective remedy to challenge this.
9. States must conduct and publish independent **human rights and data protection** impact assessments before acquiring or deploying SOCMINT, specifically evaluating discriminatory impact on marginalized groups, journalists, and human rights defenders, and should **consult with anticipated affected communities** and civil society representatives in advance.

A stylized illustration in light blue on a dark blue background. It features a communication tower on the right side, with a lattice structure and a central vertical mast. At the top of the mast is a large, rounded satellite dish or antenna. Several smaller, similar antennas are positioned along the mast. To the left of the tower, there is a network of nodes represented by circles of varying sizes, connected by thin lines, suggesting a data or communication network. The overall aesthetic is modern and technological.

05

**Mass Communications
Interception.**

Introduction

Subjecting the public's communications to systemic and widespread surveillance can amount to a serious intrusion on our fundamental rights. People may reasonably expect that their phone calls, text messages, and emails with friends, family, and colleagues will remain private. Yet modern communication surveillance technologies mean these many of these communications can be accessed at virtually any time. Among these technologies, mass communications interception poses one of the most significant intrusions to our privacy, as it can be directed not just at specific individuals but at entire populations. This scope and scale of surveillance are unprecedented in history.

The need to express, exchange and influence ideas—on our own terms, and with the assurance that our personal communications remain confidential—is fundamental to a functioning democracy. Yet the rapid pace of technological development has strengthened the ability of governments and private actors to carry out mass communications interception.⁴⁹¹ These practices not only enable access to intimate personal data at scale, but also risk generating a broader chilling effect, as individuals may self-censor or refrain from exercising their freedoms when they know or suspect they are being monitored.⁴⁹²

This chapter begins by defining what communications interception is and outlining the different forms it can take, including mass interception, as well as explaining the technologies and methods through which it operates. It then outlines examples of where it has been used in what we believe to be an authoritarian manner, and explains the various human rights, data protection, and privacy concerns that arise.

What is communications interception?

Communications interception can be defined as the monitoring, interception, collection, preservation and retention of information by a third party that has been communicated, relayed or generated over communications networks. The third party in question could be a law enforcement agency, intelligence agency, a private company, or a malicious actor.

Communications refers to “activities, interactions, and transactions transmitted through electronic mediums, such as the content of the communications, the identity of the parties to the communications, location-tracking, information including IP addresses, the time and duration of communications, and identifiers of communication equipment used in communications.”

491 A/RES/75/176, Resolution adopted by the General Assembly on 16 December 2020, The right to privacy in the digital age, pg. 2., <https://digitallibrary.un.org/record/3896430?v=pdf>

492 Gina Romero et. al., “‘PUSHED INTO THE SHADOWS’: Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association’, United Nations Special Procedures, 2026 <https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf>

How does communications interception work?

Modalities of communications interception can be categorised as mass and targeted interception.⁴⁹³

Targeted communications surveillance involves monitoring a specific individual or narrow group of individuals identified in advance based on the surveillance actor's particular interest.⁴⁹⁴ Contemporary technologies enable the collection of location data, retrieval of stored email and message content, and access to associated communications metadata, as well as the interception of emails, messages, and voicemails.⁴⁹⁵

For this report, we will focus on mass interception due to the potential of it being exploited as an authoritarian practice.

Mass communications interception

Mass communications interception uses systems or technologies that collect, analyse, and/or record data on a mass scale on an indefinite or large number of people or whole nations.⁴⁹⁶ This method is in direct contrast to targeted surveillance that would limit surveillance over an individual or individuals where there is reasonable suspicion of wrongdoing.

It involves the acquisition, processing, analysis, use, retention or storage of communications information about large numbers of people, without any regard to whether they are suspected of wrongdoing.⁴⁹⁷ Under currently available forms of mass surveillance, governments can capture virtually all aspects of our lives, through internet and telephone communications.⁴⁹⁸

Mass communications interception can reveal deeply intrusive information about our daily lives. It is further enabled by technological and regulatory trends. These include highly sophisticated data mining technologies and applications of word, voice and speech recognition software.⁴⁹⁹

Today, actors, including government bodies, can conduct mass communications interception through a diverse and increasing range of means, methods and technologies, partly due to their collaboration with the private surveillance industry.⁵⁰⁰ On the other hand, regulations, such as restrictions on anonymity and encryption on the internet makes individuals more vulnerable to surveillance over the digital means of communications.

Some of the methods and technologies that allow states to conduct mass communications surveillance include:

493 A/HRC/23/40, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, pg. 10-13.

494 Securing Societies Always, 'What is Target Intercept vs Bulk Intercept?', October 2020, <https://www.ss8.com/what-is-target-intercept-vs-bulk-intercept/>

495 Ibid.

496 Privacy International, 'Mass Surveillance', <https://privacyinternational.org/learn/mass-surveillance>

497 Ibid.

498 Ibid.

499 A/HRC/23/40, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, para. 38, <https://docs.un.org/en/A/HRC/23/40>

500 See following sections in this chapter.

Bulk communications interception

Bulk communications interception is carried out by tapping high-capacity fibre optic cables, allowing access to the world's internet communications.⁵⁰¹ This means actors conducting surveillance can achieve almost complete control of the public's telecom and online communications.⁵⁰²

Access to the bulk communications stored by telecoms operators and others is another method, facilitated by mandatory data retention requirements.⁵⁰³

International Mobile Subscriber Identity (IMSI) Catchers

IMSI catchers, also known as stingrays, function by mimicking nearby mobile cell towers, enabling them to intercept communications and location data transmitted by personal communication devices.⁵⁰⁴ This surveillance technology is widely used around the world, often by law enforcement and intelligence agencies.⁵⁰⁵ IMSI catchers are increasingly used during protests and can permit authorities to record everyone who attended and interfere with their communications.⁵⁰⁶

- Once connected, the device can:
- Identify the approximate location of any mobile device;
- Determine which phone number is associated with a specific SIM card;
- Disrupt or prevent calls and text messages from being transmitted; and
- In some cases, trigger a shift to a less secure network standard, such as from 4G to 2G, increasing the risk of unprotected communication being intercepted.⁵⁰⁷

These capabilities turn the IMSI catcher into a tool of mass surveillance, able to gather data from thousands of people.

The role of governments and the private surveillance industry in mass communications interception

Modern surveillance means and methods increasingly enable the actors of mass communications surveillance to employ intrusive tools over individuals' and communities'

501 Privacy International, 'How Bulk Interception Works', 30 September 2016, <https://privacyinternational.org/explainer-graphic/140/how-bulk-interception-works>

502 A/HRC/23/40, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, para. 38, <https://docs.un.org/en/A/HRC/23/40>

503 Privacy International, 'Comms Data Retention', <https://privacyinternational.org/learn/comms-data-retention>

504 Privacy International, 'How IMSI Catchers can be used at protest and how you can minimise risks to your data', 2021, https://privacyinternational.org/sites/default/files/2021-06/IMSI_catchers.pdf

505 Electronic Frontier Foundation, 'Gotta Catch 'Em All: Understanding How IMSI-Catchers Exploit Cell Networks', June 2019, <https://www.eff.org/wp/gotta-catch-em-all-understanding-how-imsi-catchers-exploit-cell-networks>

506 TEDIC, 'IMSI Catchers in Paraguay: The Invisible Surveillance Threatening Your Right to Protest', 18 March 2020, <https://www.tedic.org/en/imsi-catchers-in-paraguay-the-invisible-surveillance-threatening-your-right-to-protest/>; Ilica Mahajan, 'The High-Tech Tools Police Can Use to Surveil Protesters', The Marshall Project, 11 December 2024, <https://www.themarshallproject.org/2024/11/12/protest-surveillance-technologies>

507 Privacy International and Liberty, IMSI Catchers, <https://privacyinternational.org/sites/default/files/2019-06/Explainers-IMSI.pdf>

in an unprecedented capacity.⁵⁰⁸ Digital surveillance is no longer limited to nations with the resources to carry out mass and targeted monitoring using their own in-house technologies.⁵⁰⁹ While it is true that States continue to develop surveillance tech within their own agencies, private companies can offer sometimes more sophisticated tools on the international surveillance market.⁵¹⁰ According to a UN Special Rapporteur, “credible allegations have shown that companies are selling their tools to Governments that use them to target journalists, activists, opposition figures and others who play critical roles in democratic society”.⁵¹¹

Private security companies involved in the provision of mass communications surveillance services include ‘private business entities that provide military and/or security services, irrespective of how they describe themselves’.⁵¹² Already in 2016, Privacy International had found that 528 surveillance companies (overwhelmingly based in large arms-exporting countries) develop, market and sell digital surveillance products to government purchasers.⁵¹³

A joint report of PI and Geneva Centre for Security Sector Governance (DCAF)⁵¹⁴ explores the mass communications surveillance role of telecommunication service providers that manage landline, mobile or internet networks, as well as of over-the-top internet platforms.

Furthermore, over-the-top internet communications platforms that rely on the technical telecommunications infrastructure provided by operators can be potentially implicated in providing communications surveillance services.⁵¹⁵ Depending on political pressures and legislation in place, they could be made to grant access to data centres or decrypt and provide communications to law enforcement or intelligence agencies.⁵¹⁶

What makes the use of mass communications interception authoritarian?

Mass communications interception has been used across the world to facilitate social and political control, target dissidents, and suppress the right to share and receive information and opinions that allow societies to hold their regimes accountable. Such practices become authoritarian when surveillance systems are employed to erode the rule of law by granting excessive and unrestrained powers to those who seek to consolidate authority at the expense of freedoms and rights.

508 A/HRC/RES/34/7, Resolution adopted by the Human Rights Council on 23 March 2017, The right to privacy in the digital age, 7 April 2017, <https://digitallibrary.un.org/record/1307661?ln=en&v=pdf>

509 Ibid.

510 CitizenLab, ‘Communities at Risk: Targeted Digital Threats Against Civil Society’, Monk School of Global Affairs, University of Toronto, 11 November 2014, pg. 8-11, <https://targetedthreats.net/media/1-ExecutiveSummary.pdf>

511 A/HRC/41/35, ‘Surveillance and human rights Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression’, 28 May 2019, para. 6, <https://docs.un.org/en/a/hrc/41/35>

512 Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict, September 2008, <https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/montreux-document-eng.pdf>

513 Privacy International, ‘The Global Surveillance Industry’, 2016, www.privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

514 Ibid.

515 Ibid.

516 Geneva Centre for Security Sector Governance, ‘Understanding Private Surveillance: Technologies, Markets, Regulation and Human Right’, September 2024, pg. 10, https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Understanding%20Private%20Surveillance_WEB.pdf

We consider that several elements contribute to making the use of mass communications interception inherently authoritarian. The highly complex and opaque nature of the mass interception technologies means that the public is often unaware that such capabilities exist or that their communications can be secretly intercepted. Because these systems can operate at immense scale, possibly encompassing entire populations in each context, they risk not being proportionate when used in such a manner. When surveillance is deployed universally and without public knowledge, it collapses the boundary between private and public life.

As a result, this may lead individuals across a surveiled population – who are unable to determine whether or not they are personally targeted but are rather left in uncertainty – to assume that their interactions may be constantly observed or even accessed retrospectively at any point, in order to persecute or otherwise harm them. Such an environment deepens the chilling effect on the enjoyment of fundamental rights, particularly the right to privacy, and reshapes how people communicate, participate, and engage in civic life.

Examples of the authoritarian use of mass communications interception

Venezuela: Spying on Major Telecoms

Venezuela's digital censorship practices may have played a crucial role in its transformation to an authoritarian regime.⁵¹⁷ The Venezuelan government's control over the telecommunications infrastructure⁵¹⁸ seems to have taken a new level in 2010, when the parliament passed legislation that allowed the executive branch the powers to regulate all internet content accessible to users in the country.⁵¹⁹

Since then, it has been reported that the interception of communications through service providers has had a devastating impact on the rights of freedom of expression and association, posing particular threats against dissidents, journalists and human rights defenders.⁵²⁰ Intimidation, persecution, arbitrary detention, ill-treatment and torture of activists and citizens are among the serious concerns that have been exacerbated by the increased surveillance regime.⁵²¹ According to one report⁵²², the communications company Telefónica intercepted the communications of more than 1.58 million subscribers,⁵²³

517 Access Now, 'The Many Means of Surveillance and Control in Venezuela', 16 August 2019, <https://www.accessnow.org/the-many-means-of-surveillance-and-control-in-venezuela>

518 Derechos Digitales and Centro de Paz y Derechos Humanos de la UCV, 'Informe sobre el Estado de los Derechos Digitales en Venezuela', July 2018, https://www.derechosdigitales.org/wp-content/uploads/CPI_venezuela.pdf

519 Access Now, 'The Many Means of Surveillance and Control in Venezuela', 16 August 2019, <https://www.accessnow.org/the-many-means-of-surveillance-and-control-in-venezuela>

520 Probox, 'A un año del 28J: cómo el chavismo convirtió las redes en armas de represión digital', July 2025, <https://proboxve.org/investigacion/a-un-ano-del-28j-como-el-chavismo-convirtio-las-redes-en-armas-de-represion-digital/>; A/HRC/62/45, 'Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association', Gina Romero, 21 April 2026, <https://docs.un.org/en/A/HRC/62/45>

521 Office of the United Nations High Commissioner for Human Rights, 'Press release - Venezuela: New UN Report Details Responsibilities for Crimes Against Humanity', 20 September 2022, <https://www.ohchr.org/es/press-releases/2022/09/venezuela-new-un-report-details-responsibilities-crimes-against-humanity?sub-site=HRC>

522 Telefónica, 'Informe de Transparencia en las Comunicaciones 2021', <https://www.telefonica.com/es/wp-content/uploads/sites/4/2021/08/Informe-de-Transparencia-en-las-Comunicaciones-2021.pdf>

523 Balbi, Marianela, 'Venezuelan Authorities Spied on 20% of Major Telecom's Clients', Advox - Global Voices, 17 March 2023, <https://advox.globalvoices.org/2023/03/17/venezuelan-authorities-spied-on-20-of-major-telecoms-clients/>

amounting to 20% of major telecom's clients in Venezuela in 2021, as per the orders of the Maduro administration.

IMSI Catchers

As highlighted above, IMSI catchers are highly intrusive mass communications interception tools whose use is often unregulated.⁵²⁴ They are usually deployed in secret, sometimes without a clear legal basis, and often without appropriate safeguards and oversight mechanisms.⁵²⁵ Their authoritarian use as a technology can facilitate the surveillance of individuals that may lead to further human rights abuses but also can create a chilling effect when deployed in that context.

In the **US**, it was reported that IMSI catchers may have been used by law enforcement officials at the **Portland Immigration and Customs Enforcement** (ICE) facility during highly publicised protests against the government.⁵²⁶ While law enforcement agencies, including ICE, often refuse to confirm or deny the use of this secretive surveillance technology, records obtained in 2020⁵²⁷ indicated that ICE has utilized cell-site simulators, another name for IMSI catchers, hundreds of times in the past, around 466 times from 2017 to 2019.⁵²⁸

In the **United Kingdom**, UK police forces maintain a strict "neither confirm nor deny" policy on the use of IMSI catchers.⁵²⁹ Since 2015, multiple credible reports indicate the use of IMSI catchers in the United Kingdom, possibly including during protests.⁵³⁰ The former Chief Surveillance Inspector with the Office of Surveillance Commissioners stated, when asked whether IMSI catchers had been utilised at protests: "Certainly there appears to be enough evidence in the public domain to suggest that they have been used in that way before, yes."⁵³¹

524 Privacy International, 'Remember Those IMSI Catchers? UK Authorities Play Hide-and-Seek on Use of Intrusive Surveillance', 19 January 2023, <https://www.privacyinternational.org/news-analysis/5206/remember-those-imsi-catchers-uk-authorities-play-hide-and-seek-use-intrusive>

525 Ibid.

526 Mikael Thalen, 'Exclusive: Fake Cellphone Tower Likely Surveilled Protesters at Portland ICE Facility', Straight Arrow News, 25 September 2020, <https://san.com/cc/exclusive-fake-cellphone-tower-likely-surveilled-protesters-at-portland-ice-facility/>

527 Alexia Ramirez, 'ICE Records Confirm That Immigration Enforcement Agencies Are Using Invasive Cell-Phone Surveillance Devices', American Civil Liberties Union, 3 December 2020, <https://www.aclu.org/news/immigrants-rights/ice-records-confirm-that-immigration-enforcement-agencies-are-using-invasive-cell-phone-surveillance-devices>

528 Ibid.

529 Privacy International, 'Remember Those IMSI Catchers? UK Authorities Play Hide-and-Seek on Use of Intrusive Surveillance', 19 January 2023, <https://www.privacyinternational.org/news-analysis/5206/remember-those-imsi-catchers-uk-authorities-play-hide-and-seek-use-intrusive>

530 Tom Cheshire, 'Fake Mobile Phone Towers Operating in the UK', Sky News, 9 June 2015, <https://news.sky.com/story/fake-mobile-phone-towers-operating-in-the-uk-10356433>; BBC News, 'Mass Snooping Fake Mobile Towers Uncovered in UK', BBC News, 10 June 2015, <https://www.bbc.co.uk/news/business-33076527>; David Barrett, 'Fake Mobile Phone Masts Spy on Your Calls', The Telegraph, 10 June 2015, <https://www.telegraph.co.uk/news/uknews/law-and-order/11665110/Fake-mobile-phone-masts-spy-on-your-calls.html>

531 Ben Bryant, 'VICE News Investigation Finds Signs of Secret Phone Surveillance across London', VICE News, 14 January 2016, <https://www.vice.com/en/article/vice-news-investigation-finds-signs-of-secret-phone-surveillance-across-london>

The use of Bulk Communications Interception in Libya

In 2007, French technology firm Amesys reportedly⁵³² supplied sophisticated communications surveillance systems to the Libyan intelligence services. The systems allegedly permitted the interception of all country-wide, online and phone communications in Libya, and the subsequent processing of collected data. Under the Regime of Muammar Gaddafi, "the technology became a weapon that facilitated the targeting, arrest and imprisonment of thousands of people in Libya".⁵³³ Subsequent revelations showed a similar contract concluded by the same company Amesys in 2014 (then Nexa Technologies) with the Egyptian regime⁵³⁴ whose human rights score is also very concerning.⁵³⁵

In 2011, the International Federation for Human Rights (FIDH) and La Ligue des Droits de l'Homme (LDH) brought a criminal case against Amesys for complicity with human rights abuses committed by the Gaddafi regime in Libya because they provided surveillance equipment to the regime.⁵³⁶ In May 2017, Amesys was placed under the status of assisted witness for complicity in acts of torture.⁵³⁷

In June 2021, four executives of Amesys and Nexa Technologies were indicted by investigating judges of the crimes against humanity and war crimes unit of the Paris Judicial Court.⁵³⁸ The indictment relates to complicity in torture in the Libyan portion of the investigation and as well as complicity in torture and enforced disappearance in the Egyptian portion.⁵³⁹ The indictments demonstrate the potential link between bulk communications interception and severe human rights abuses.

Human Rights and Data Protection Implications

UN bodies have denounced unlawful or arbitrary surveillance and interception of communications as 'highly intrusive practices' that interfere with fundamental human rights.⁵⁴⁰ Mass communications interception is not only a fundamental concern for the right to privacy, freedom of expression, and association, but also for a democratic society to which we all contribute through our voices, concerns, actions, and criticism.

Its authoritarian uses create an environment of suspicion and threat, which can cause

532 FIDH - International Federation for Human Rights, 'Business and human rights: enhancing standards and ensuring redress', March 2014, https://www.fidh.org/IMG/pdf/201403_briefing_paper_enhance_standards_ensure_redress_web_version.pdf

533 Geneva Centre for Security Sector Governance, 'Understanding Private Surveillance: Technologies, Markets, Regulation and Human Rights', September 2024, pg. 15, https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Understanding%20Private%20Surveillance_WEB.pdf

534 Ibid.

535 See: Euromed Rights, 'Egypt's Human Rights Crisis and Crackdown on Defenders', <https://euromedrights.org/publication/new-report-egypts-human-rights-crisis-and-crackdown-on-defenders/>

536 International Federation for Human Rights and Cairo Institute for Human Rights Studies, 'Surveillance and Torture in Egypt and Libya: Amesys and Nexa Technologies' Alleged Complicity in Human Rights Violations', 23 October 2017, <https://www.fidh.org/en/region/north-africa-middle-east/egypt/surveillance-and-torture-in-egypt-and-libya-amesys-and-nexa>

537 Ibid.

538 Ibid.

539 Ibid.

540 A/RES/75/176, The right to privacy in the digital age, United Nations High Commissioner for Human Rights, 'Impact of new technologies on the promotion and protection of human rights in the context of assemblies, including peaceful protests', 24 June 2020, pg. 7-8.

people who are not engaged in any wrongdoing to change their behaviour, including the way they act, speak and communicate, in what is commonly described as the chilling effect of mass surveillance. As a result, mass communications interception stifles the capacity of entire social fabrics, limiting broader societal level potential for experimentation and evolution.⁵⁴¹ Peoples' awareness or suspicion (often hard to separate) of being surveilled in their communications inevitably influences behaviour, including in forms of self-censorship or discouragement from fully participating in their societies.⁵⁴²

Without the security of knowing that our communications are private, our ability to create safe boundaries and manage our relationships falls apart. As previously noted by Privacy International and the Geneva Centre for Security Sector Governance (DCAF), if diverse actors are systematically put under surveillance and censored, a community's collective rights to expression, assembly and association are abused, as these diverse perspectives are eliminated and their accounts silenced.⁵⁴³ Eventually, authoritarian uses of mass communications interception inhibit the legitimate exercise of our rights and foster an order of fear and persecution.

Therefore, it is not surprising that mass communications interception can end up solidifying authoritarian practices and regimes through the disproportionate targeting of journalists, human rights defenders, civil society organisations, whistleblowers and opposition political activists, without appropriate safeguards for privacy rights.⁵⁴⁴

Further, mass surveillance regimes often operate conveniently in secrecy without providing meaningful paths for the masses under surveillance to contest these policies and practices.⁵⁴⁵ Decisions to surveil can lead to death, torture, ill-treatment, intimidation and more.⁵⁴⁶ The complexity and secrecy involved in the implementation of mass surveillance systems, particularly in a security context, enable states and other actors to operate in impunity and without effective accountability mechanisms.

For these reasons, we think bulk interception is never proportionate and permissible. The European Court of Human Rights disagrees, have set out a set of 'end-to-end safeguards' to attempt to regulate this highly intrusive surveillance practice, at least as practiced by the UK.⁵⁴⁷ But these safeguards, while important, are not sufficient to restrain the potential

541 Privacy International, 'Mass Surveillance', <https://privacyinternational.org/learn/mass-surveillance>

542 PEN America, 'Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor', 12 November 2013, pg. 3, <https://pen.org/report/chilling-effects/>

543 Geneva Centre for Security Sector Governance, 'Understanding Private Surveillance: Technologies, Markets, Regulation and Human Right', September 2024, pg. 16, https://www.dcaf.ch/sites/default/files/publications/documents/DCAF_Understanding%20Private%20Surveillance_WEB.pdf

544 African Commission on Human and Peoples' Rights, Resolution on the deployment of mass and unlawful targeted communication surveillance and its impact on human rights in Africa, ACHPR/Res. 573 (LXXVII), 2023, <https://achpr.au.int/en/adopted-resolutions/573-resolution-deployment-mass-and-unlawful-targeted-communication>

545 A/HRC/51/17, Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, October 2022, <https://docs.un.org/A/HRC/51/17>

546 Ibid.

547 European Court of Human Rights, Big Brother Watch and Others v. the United Kingdom [GC], no. 58170/13 and others, para. 347, 25 May 2021, <https://hudoc.echr.coe.int/fre#%7B%22itemid%22%3A%5B%22001-210077%22%5D%7D>

abuse of mass interception which is becoming even more concerning in the age of advanced artificial intelligence.⁵⁴⁸

Conclusion

In conclusion, mass interception is amongst the biggest threats to fundamental rights in the era of technological advances. While advances in technology expand our ability to connect and participate in society, they also enable governments and private actors to monitor, intercept, and exploit personal communications at an unprecedented scale and without sufficient accountability for the human rights impact they cause.

Mass surveillance threatens our privacy, freedom of speech, and ability to take part in society without fear. When people believe they are being watched, they often stay silent or fear expressing their dissent. The growing role of private companies in selling and running these tools makes the problem even worse, especially when there is little oversight.

Mass communications interception poses a danger to democratic freedoms and civil liberties at a societal level and **should not be deployed by states.**

548 Privacy International, 'UK mass interception laws violates human rights and the fight continues...', May 2021, <https://privacyinternational.org/long-read/4526/uk-mass-interception-laws-violates-human-rights-and-fight-continues>; Marko Milanovic, 'The Grand Normalization of Mass Surveillance: ECtHR Grand Chamber Judgments in Big Brother Watch and Centrum för rättvisa', Blog of the European Journal of International Law, May 2021, <https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/>; <https://verfassungsblog.de/big-b-v-uk/>; Monika Zalnieriute, 'Procedural Fetishism and Mass Surveillance under the ECHR Big Brother Watch v. UK', Verfassungsblog, June 2021, <https://www.icj.org/resource/big-brother-watch-v-uk-a-landmark-judgment-missing-the-mark>

CONCLUSION

The five categories of technology examined in this report — and their documented authoritarian uses — point towards societal level assaults on human rights, fundamental freedoms, and civic spaces that are being facilitated in different regions across the world by the authoritarian uses of these technologies.

In democratic and authoritarian contexts alike, these five technologies are shown to be deployed in ways that erode — and in some cases effectively dismantle — the right to privacy and related protections that should be enjoyed by populations and individuals around the world. The uses recorded in this report of facial recognition technology, mobile phone extraction, spyware, social media surveillance and mass communications interception raise profound concerns not only for individual and collective human rights, but also for the integrity of civic space at the national, transnational, and international levels.

It is important to distinguish between the different technologies examined, as each engages distinct — and sometimes overlapping — human rights and data protection concerns. For example, FRT is rooted in the processing of sensitive biometric data for identification purposes, directly implicating the right to privacy, data protection principles governing sensitive data, and protections against misidentification, discrimination, and arbitrary interference.⁵⁴⁹ By contrast, MPE and spyware intrude far more expansively into many areas of individuals' the digital lives.⁵⁵⁰

These technologies can capture and analyse a vast range of sensitive personal data, including communications, contacts, location data, browsing histories, social media activity, financial and health records, stored files, legally privileged data, journalists sources, information relating to third parties and more. Their capacity to aggregate and infer additional insights from this data creates profound risks to privacy and data protection, while also often implicating the broader spectrum of human rights and thus giving "rise to compound human rights harm".⁵⁵¹ Although often justified as tools for combating serious crime and protecting national security, these technologies have repeatedly been deployed to monitor journalists, human rights defenders, political dissidents, activists, and minority communities.⁵⁵² In many cases, the effects of such use has been disproportionate, discriminatory, and undertaken without meaningful legal safeguards or independent oversight, facilitating intimidation, persecution, and the suppression of dissent.⁵⁵³ Consequently, technologies ostensibly intended to enhance public safety have been

549 See: Chapter 1 of this report.

550 See: Chapter 2 of this report.

551 Gina Romero et. al., "'PUSHED INTO THE SHADOWS': Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association", United Nations Special Procedures, 2026 <https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf>

552 See: for example, this report and A/HRC/48/31, United Nations High Commissioner for Human Rights, 'The right to privacy in the digital age', 13 September 2021, <https://www.ohchr.org/en/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet?LangID=E&NewsID=27469>

553 See: for example, this report and Gina Romero et. al., "'PUSHED INTO THE SHADOWS': Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association", United Nations Special Procedures, 2026, <https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf>

weaponised against the very individuals and democratic institutions they claim to protect.

In conclusion, we have identified the following five core areas of common concern regarding the authoritarian use of the technologies covered within this report:

1. Some technologies are by-design disproportionately intrusive and should not be used

Certain technologies are so inherently intrusive by design that they are incapable of being reconciled with human rights standards. In particular, live FRT and mass communications interception exemplify this category of disproportionately intrusive technologies. As discussed in Chapter 2, it is difficult to envisage any circumstances in which the use of live FRT could fully comply with international human rights law and data protection principles. The same concern applies to the deployment of mass interception which is inherently disproportionate.

2. Technologies are used for authoritarian purposes

Even where technologies are not inherently or disproportionately intrusive, and where their rights-compliant deployment could in principle be ensured through appropriate legal frameworks, safeguards, and oversight, the purposes for which they are often used remain deeply problematic. Too frequently, the uses of all technologies covered in this report serve authoritarian objectives, leading to adverse impacts on human rights and data protection.⁵⁵⁴ In such contexts, we believe that technology risks facilitating or amplifying repressive practices and systems, and becoming an instrument of authoritarian governance.

The use of retrospective FRT, MPE, spyware and SOCMINT should therefore be permissible only in strictly limited circumstances. Any such use must be subject to prior, independent — and preferably judicial — authorisation; grounded in reasonable suspicion; and constrained by robust safeguards that satisfy the principles of legality, necessity, and proportionality.

3. Technologies' use is often incompatible with the rule of law

Some of the authoritarian uses of technology documented in this report, such as uses of FRT and of MPE, have occurred in the absence of adequate legislative and regulatory frameworks, meaningful safeguards, independent oversight, or effective redress mechanisms. Meanwhile, the use of other technologies such as spyware have been repeatedly decried as being fundamentally incompatible with the respect for human rights, namely the right to privacy.⁵⁵⁵

As states double down on their techno-solutionist approaches to national security, governments must couple the use of these five technologies with the establishment of comprehensive legal and regulatory frameworks that either strictly circumscribe – or prohibit – the use, procurement, export, and transfer of given surveillance technologies,

⁵⁵⁴ See “Country examples” sections in each chapter of this report.

⁵⁵⁵ Council of Europe Commissioner for Human Rights, ‘Highly intrusive spyware threatens the essence of human rights’, The Council of Europe, 27 January 2023, https://www.coe.int/en/web/commissioner/blog/2023/-/asset_publisher/aa3hyyf8wKBn/content/highly-intrusive-spyware-threatens-the-essence-of-human-rights; European Data Protection Supervisor, ‘Preliminary Remarks on Modern Spyware’, February 2022, https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

as our as our end-of-chapter recommendations make clear. Indeed, such frameworks should embed mandatory and proscribed human rights and data protection safeguards, impact assessments and due diligence obligations, as well as public and CSO consultation obligations, and should ensure transparency and robust safeguards when it comes to procurement and public–private partnerships.

4. Inaccessible redress raises mass impunity risks for authoritarian use of technologies

When it comes to the use of the five technologies covered in this report, in practise, access to effective remedy is highly inaccessible in most cases. Individuals are too often unaware that they have been subjected to surveillance and had their data subject rights or right to privacy infringed upon. The use of FRT without notifying the data subject that their biometric data has been collected and processed,⁵⁵⁶ the use of SOCMINT to collect personal data from online platforms and the use of spyware (which usually requires expert or onerous forensic analysis to confirm), as discussed in this report, all evidence this concern.

These concerns were acknowledged by the UN Special Rapporteur for the rights to freedom of assembly and of association, who stated that “surveillance occurs remotely, is largely invisible” and that individuals “do not – and often cannot – know if, when or how, surveillance is practiced, or by whom. This results in new power asymmetries, creating systemic uncertainty, and undermining the ability to challenge surveillance through public scrutiny, or via political or legal means”, and that the right to an effective remedy is therefore undermined.⁵⁵⁷

Even where the knowledge of a harmful surveillance practise does exist, lack of transparency (described below) presents serious impediments to accessing the information necessary to obtain redress, the processes for which are moreover often long, complex, resource intensive and simply beyond the accessibility of most people. Where harms are transnational — for example, involving exported spyware or cross-border data flows — jurisdictional complexity can further compound the difficulty of seeking redress.⁵⁵⁸

5. Lack of transparency facilitates authoritarian use of technologies

We find there to be a generalised and pervasive lack of adequate transparency in the use of the five technologies featured in this report. Such opacity often shields responsible actors from scrutiny and can foment impunity for authoritarian practices and the harms they cause, as discussed above. Again, the UN Special Rapporteur on the rights of freedom of assembly or association recognised that the use of surveillance technologies “is characterised by opacity and lack of transparency”.⁵⁵⁹

556 Joy Buolamwini, Unmasking the bias in facial recognition algorithms, 13 December 2024, <https://mitsloan.mit.edu/ideas-made-to-matter/unmasking-bias-facial-recognition-algorithms>

557 Gina Romero et. al., ““PUSHED INTO THE SHADOWS”: Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association”, United Nations Special Procedures, 2026 <https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf>

558 See: Chapter 3 Mobile Phone Extraction case study.

559 Gina Romero et. al., ““PUSHED INTO THE SHADOWS”: Evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association”, United Nations Special Procedures, 2026 <https://www.ohchr.org/sites/default/files/documents/form/digital-surveillance-chilling-effects-shadows-erosion-freedom-1-en.pdf>

Lack of transparency further significantly hinders accountability for harms and malpractice in the use of these technologies, since the way they are being used and the actors responsible remain in the shadows.

Without clear primary legislation, mandated transparency obligations, independent oversight, and accessible avenues for effective remedy, these technologies' use runs the risk of entrenching authoritarian practices, undermining freedom of expression and assembly, creating a societal chilling effect and thus hampering democratic mechanisms and participation.

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org