PRIVACY INTERNATIONAL

Submission to the Office of the United Nations High Commissioner for Human Rights on the promotion and protection of human rights in the context of peaceful protests

October 2019

October 2019

Privacy International's submission on the promotion and protection of human rights in the context of peaceful protests

Privacy International welcomes the United Nations Human Rights Council Resolution 38/11 on the promotion and protection of human rights in the context of peaceful protects that requests "the United Nations High Commissioner for Human Rights to prepare a thematic report on new technologies, including information and communications technology, and their impact on the promotion and protection of human rights in the context of assemblies, including peaceful protests."

In this submission, Privacy International[1] aims to provide the UN High Commissioner for Human Rights with information on how surveillance technologies are affecting peaceful protests in new and often unregulated ways.

Based on Privacy International's research, we provide the following observations:

- the relationship between the right to peaceful protest and right to privacy;
- the impact of new surveillance technologies on peaceful protests;
- right to peaceful protest online.

1. Relationship between the right to peaceful protest and the right to privacy

Unlawful interference with someone's privacy, particularly in the form of communication surveillance, may have significant, negative impact in the capacity of individuals to exercise their right to peaceful protest as protected by Article 21 of the International Covenant on Civil and Political Rights (ICCPR).

[1] Privacy International (PI) PI was established in 1990 as a non-profit, non-governmental organisation based in London, working with partners around the globe, at the intersection of modern technologies and rights. It envisions a world in which the right to privacy is protected, respected, and fulfilled. PI believes that privacy is essential to the protection of autonomy and human dignity, serving as the foundation upon which other human rights are built. In order for individuals to fully participate in the modern world, developments in law and technologies must strengthen and not undermine the ability to freely enjoy this right. We are building the global movement because people must have access to privacy protection without regard to citizenship, race and ethnicity, economic status, gender, age, or education (https://privacyinternational.org/).

Planning of peaceful protests against governments or non-state actors' policies and practices requires the capacity of individuals to communicate securely and safely confidentially without interference. From protests in support of LGBTI rights to protests against specific projects that undermine local communities' wellbeing, these movements would not have been possible without the ability to exchange ideas and develop plans in private spaces. The recent and on-going developments during protests in Hong Kong demonstrate the fragility of peaceful protests in the face of digital surveillance technologies.[2]

During protests and demonstrations, individuals often may not wish to be recognised and in fact may rely on the anonymity of the crowd to protect them against retaliation. From protests against authoritarian governments, such as during the Arab springs, to demonstrations in support of LGBTI movements in countries where homosexuality is criminalised, to environmental protests against powerful companies, being part of an anonymous crowd is what allows many to participate in these peaceful assemblies. However, anonymity in public spaces is increasingly challenged with the deployment of new surveillance technologies (see below).

The protection of the right to privacy not only facilitates the enjoyment of the right to peaceful protest, but it is often a condition for its exercise. UN member states underlined the links between privacy, assembly and freedom of expression in various UN General Assembly and Human Rights Council Resolutions. Among others, the Human Rights Council recognised that "privacy online is important for the realization of the right to freedom of expression and to hold opinions without interference, and the right to freedom of peaceful assembly and association".[3]

While this recognition is an important starting point, Privacy International believes that more analysis is needed on the interplay between the rights to privacy and freedom of assembly. Therefore, Privacy International encourages the UN High Commissioner for Human Rights to consider the links between peaceful protest and privacy.

2 Frederike Kaltheuner, "What Hong Kong's Protestors Can Teach Us About the Future of Privacy", Gizmodo, 2019, available at https://gizmodo.com/what-hong-kongs-protestors-can-teach-us-about-the-futur-1835715794.

3 It further added: "Emphasizing that, in the digital age, technical solutions to secure and protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association," The promotion, protection and enjoyment of human rights on the Internet, UN HRC Resolution 38/7, 5 July 2018 (A/HRC/RES/38/7), Preamble, at §§ 12-13.

"Emphasizing that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, including measures for encryption and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association". The Right to Privacy in the Digital Age, UN HRC Resolution 34/7, 23 March 2017 (A/HRC/34/7), Preamble, at § 24.

"*Emphasizing* that, in the digital age, technical solutions to secure and to protect the confidentiality of digital communications, which may include measures for encryption, pseudonymization and anonymity, can be important to ensure the enjoyment of human rights, in particular the rights to privacy, to freedom of expression and to freedom of peaceful assembly and association, and recognizing that States should refrain from employing unlawful or arbitrary surveillance techniques, which may include forms of hacking," The Right to Privacy in the Digital Age, UN GA Resolution 73/179, 17 December 2018 (A/RES/73/179), Preamble, § 29.

"The capacity to use communication technologies securely and privately is vital to the organization and conduct of assemblies." Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies, 4 February 2011 (A/HRC/31/16), at § 75.

2. The impact of new surveillance technologies on peaceful protests

Thanks to the availability of data and new technologies to process it, private companies and public authorities are increasingly collecting and analysing the personal information of individuals, which can also be obtained from public spaces.

Privacy International believes that that test of legality, necessity and proportionality must apply to the assessment of the use of any new technologies deployed by the police and other law enforcement and security agencies to monitor peaceful protests.

Most of the debate about this collection and processing of publicly available information has centred on the right to privacy. Governments often argue that these practices have little impact on people's privacy as and when it relies "only" on *publicly available* information. This inaccurate representation fails to account for the intrusive nature of collection, retention, use, and sharing of a person's personal data obtained from public places. Further it fails to consider the implication of these practices vis-à-vis the right to peaceful protest.

Privacy International's research has identified two technologies deployed by public authorities in monitoring assemblies that raise particular concerns: IMSI catcher and facial recognition.

2.1 IMSI catcher

In many places around the world, individuals carry mobile phones on their person wherever they go, including when they peacefully assemble. Governments have many ways of conducting surveillance of mobile phones. One means of capturing mobile phone data is through the use of a device known as an "International Mobile Subscriber Identity" catcher or "IMSI catcher."[4] IMSI catchers operate by impersonating mobile phone base stations and tricking mobile phones within their range to connect to them. Once connected to an IMSI catcher, mobile phones reveal information that can identify their users[5] and that process also permits the IMSI catcher to determine the location of the phones.[6] Some IMSI catchers also have the capability to block or intercept data transmitted and received by mobile phones, including the content of calls, text messages and web sites visited.[7]

[4] IMSI catchers are one type of mobile phone surveillance technology. See generally, Privacy International, Phone Monitoring, available at https://privacyinternational.org/explainer/1640/phone-monitoring. IMSI catchers are known by a multitude of different names, including "cell site simulators," "cell grabbers," "mobile device identifiers, "man-in-the-middle devices," or by their specific brand names, such as "StingRay" or "DRTbox."

[5] IMSI catchers typically capture the IMSI and the "International Mobile Station Equipment Identifier" ("IMEI") of mobile phones. The IMEI is unique to each mobile phone whereas the IMSI is unique to each Subscriber Identification Module ("SIM") card.

[6] See Privacy International, Phone Monitoring, *supra*; Jennifer Valentino-DeVries, "How 'Stingray' Devices Work," *Wall St Journal*, 21 September 2011, available at https://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/.

[7] See Stephanie K. Pell & Christopher Soghoian, Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy, 28 *Harvard Journal of Law & Technology* 1 (2014); Adrian Dabrowski *et al*, IMSI-Catch Me If You Can: IMSI-Catcher-Catchers, Annual Computer Security Applications Conference 2014, p 2.

IMSI catchers interfere with a range of human rights, including the rights to privacy and freedom of expression. However, IMSI catchers pose unique threats to the right to freedom of peaceful protest because they conduct surveillance on all individuals within a particular physical area, identify (de-anonymise) those individuals, and can, in certain circumstances, intercept or manipulate their communications and data. By their design, IMSI catchers are uniquely effective tools for conducting surveillance on individuals peacefully assembling or associating with others.

First, IMSI catchers are designed to manipulate all mobile phones in a particular physical area to connect to them and turn over identifying information. They therefore permit the easy identification and collection of personal data of all persons present within their proximity. The scale of this surveillance can vary widely depending on the IMSI catcher, which can be carried by hand, concealed in a backpack, installed in a car or mounted on an aircraft, and cover areas ranging from a few square blocks to potentially entire cities.

Second, IMSI catchers offer a way to easily identify individuals, especially in settings – such as a large public gathering – where they would otherwise remain anonymous. Indeed, "an activity can be anonymous even though it is also public" and it is that duality – that one can be both public and maintain her identity – that allows individuals to freely participate in venues that critique governments or powerful actors, or expose wrongdoings.[8]

IMSI/IMEI[9] data are unique identifiers associated with a particular mobile phone user. Thus, once public authorities have gathered IMSI/IMEI data, they can easily connect that data to individual mobile phone users. Even more troubling, where IMSI/IMEI data can be linked to further information held by public authorities, the government can not only identify but also potentially track and profile individuals. This danger is acute, for example, in countries with compulsory SIM card registration, which require sellers of SIM cards to record personal information about each buyer and maintain this information in a registry that is accessible to or directly held by the government.[10]

Finally, certain sophisticated models of IMSI catchers can, by insinuating themselves into the mobile network infrastructure, interfere with mobile phones in a variety of other ways, including by intercepting or even manipulating communications or data.[11] These IMSI catchers operate as "man-in-the-middle" devices, presenting themselves as a legitimate mobile phone base station to mobile phones and as a mobile phone to legitimate base stations, enabling traffic passing to and from the phone to flow through them.[12] By placing themselves in the middle of this flow,

8 Article 19, Right to Online Anonymity, 18 June 2015, p 1, available at https://www.article19.org/resources/report-the-right-to-online-anonymity/; see also Privacy International, Securing Safe Spaces Online, 2015, p 8, available at https://privacyinternational.org/report/1634/securing-safe-spaces-online-encryption-online-anonymity-and-human-rights.

9 IMSI catchers typically capture the IMSI and the "International Mobile Station Equipment Identifier" ("IMEI") of mobile phones. The IMEI is unique to each mobile phone whereas the IMSI is unique to each Subscriber Identification Module ("SIM") card.

10 For example, see Privacy International and Article 19's intervention in *Breyer v. Germany*, App No 50001/12, European Court of Human Rights, available at https://privacyinternational.org/legal-action/breyer-v-germany-germany-mandatory-sim-card-registration, which addresses how a German mandatory SIM card registration provision interferes with anonymity and the rights of privacy and freedom of expression.

11 See Stephanie K. Pell & Christopher Soghoian, *supra*; Adrian Dabrowski *et al*, *supra*.

12 The scope of what these IMSI catchers can do will depend on the network and the capability of the IMSI catcher itself. Some networks encrypt communications and data flowing over the network in order to protect them from third parties. In addition, certain applications or services, such as a messaging platform, may apply another layer

IMSI catchers can capture and even edit or reroute calls, text messages and internet data as well as block service, either to all mobile phones within their range or to select devices.

The use of IMSI catchers interfere with the right to freedom of peaceful assembly in a number of ways:

- By capturing mobile phone communications and data, IMSI catchers can chill the exercise of the right to freedom of assembly, as the monitoring and recording of participants at an assembly may prevent them from joining.[13]
- By editing or rerouting communications and data or blocking service, IMSI catchers can undermine and disrupt the ability of individuals attending a gathering to communicate with one another or organise further.
- It's even possible, in some circumstances, for a government to use an IMSI catcher to send a message to mobile phones in the area as a way of intimidating users or manipulating them to disband or conduct some other activity.[14]

Some of the above interferences are, prima facie, indiscriminate in nature and likely not to meet the test of necessity and proportionality.

Over the past few years, Privacy International has been researching the proliferating use of IMSI catchers by governments around the world. We have been tracking this proliferation through our own research and investigations[15] and through export control data on this type of technology.[16] This research complements Privacy International's long-standing work documenting

of encryption. Some IMSI catchers may bypass mobile network encryption through what is known as a downgrade attack, which convinces mobile phones to switch to older communications protocols employing weaker encryption. IMSI catchers will be unable, however, to decrypt encryption mechanisms used by applications or services, such as the "off-the-record messaging" protocol, which encrypts instant messaging conversations.

13 Joint report of the United Nations Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies, 4 February 2016 (A/HRC/31/66), at §76.

14 For example, in November 2013, Ukrainian protestors demonstrating against the government in Kiev's Maidan Nezalezhnosti and others in the vicinity of the protest received the following text message on their mobile phones: "Dear subscriber, you are registered as a participant in a mass disturbance." The mass delivery of the message suggested the Ukrainian government's use of an IMSI catcher to identify mobile phones and transmit such a message. Tyler Lopez, "How did Ukraine's Government Text Threats to Kiev's EuroMaidan Protesters?," *Slate*, 24 January 2014, available at http://www.slate.com/blogs/future_tense/2014/01/24/ukraine_texting_euromaidan_protesters_kiev_demonstrators_receive_threats.html.

15 See, eg Privacy International, Shadow State: Surveillance, Law and Order in Colombia, 2015, available at https://privacyinternational.org/report/991/shadow-state-surveillance-law-and-order-colombia.

16 For example, export control data published by the United Kingdom's Department of International Trade in 2015-16 has helped reveal that the British Government has granted export licences for the sale of IMSI catchers to numerous governments, including those of Algeria, Botswana, Brazil, Colombia, El Salvador, South Africa, Gabon, Kuwait, Lebanon, Macedonia, Morocco, Namibia, Nigeria, Oman, Pakistan, Paraguay, Saudi Arabia, Serbia, Turkey, Turkmenistan, and the United Arab Emirates. Joseph Cox, "This Map Shows the UK's Surveillance Exports," *Motherboard*, 3 April 2017, available at https://motherboard.vice.com/en_us/article/538a75/uk-surveillance-export-map. Similarly, Freedom of Information requests in Finland have similarly uncovered that the Finnish Government has granted export licences for the sale of IMSI catchers to governments that include Bosnia, Colombia, Indonesia, Kuwait, Macedonia, Mexico, Morocco, Serbia and the United Arab Emirates. Joseph Cox, "New Data Gives Peek at European IMSI Catcher Exports," *Motherboard*, 23 March 2018, available at https://motherboard.vice.com/en_us/article/wj75yq/imsi-catcher-exports.

the surveillance technology trade, including the transfer of IMSI catchers to countries with poor human rights records.[17]

Despite the threat that IMSI catchers pose to a range of human rights, and in particular to the right to freedom of peaceful assembly and association, including peaceful protests, the public remains in the dark about their use and whether that use is subject to the necessary safeguards and oversight pursuant to domestic and international law.

2.2 Facial recognition

Facial recognition technology uses cameras with software to match live footage of people in public with images on a 'watch list'. It is by definition an invasive tool, especially if used in public spaces and when deployed live. Facial recognition cameras are far more intrusive than regular CCTV. Facial recognition is essentially biometric identification at a distance, involving the collection and processing of biometric data. Potentially, every technology could have a positive use, but the problem with facial recognition is multi-faced.

First, facial recognition is a highly contested and contestable technology. There are quite strong concerns across the world around facial recognition in public, and it is mounting. In response to outrage and concern, there are cities placing moratoriums not only for use of live facial recognition in public spaces but also in the use of bodycams by police authorities.[18]

When used in public spaces, the use of the technology directly infringes the right to privacy as there is no way to escape such surveillance technology, protesters can't opt-out or refuse that their face is scanned. Having facial recognition deployed in contexts, such as peaceful protest, can have a terrible chilling effect and might prevent people from engaging in public activities.

People have been already scanned, among others in the UK, without being informed, about the use of the technology and the data that were gathered.[19] This raises serious concerns regarding transparency and accountability.

Second, facial recognition technology has been used by UK police forces, among others, despite the fact that there is no law giving the police the power to use facial recognition, nor are there any Government policies or guidelines. The lack of regulation is due partly by this technology being classed by police forces as "*overt surveillance*", *therefore not attracting the level of scrutiny of "covert surveillance" techniques.*

[17] See Privacy International, Privacy International Launches the Surveillance Industry Index and New Accompanying Report, October 2017, available at https://www.privacyinternational.org/blog/54/privacy-international-launches-surveillance-industry-index-new-accompanying-report.

[18] The State of California recently placed a moratorium in the use of body cameras. Matthew Guariglia, "Victory! California Governor Signs A.B. 1215", Electronic Frontier Foundation (EFF), 9 October 2019, available at https://www.eff.org/deeplinks/2019/10/victory-california-governor-signs-ab-1215.

[19] See recent examples at in the Kings Cross area were being deployed in secret. Dan Sabbagh, "Facial recognition technology scrapped at King's Cross site", The Guardian, 2 October 2019, available at https://www.theguardian.com/technology/2019/sep/02/facial-recognition-technology-scrapped-at-kings-cross-development. See also, Privacy International, Every Police force in the UK will soon use body worn video cameras to record us in public, 3 March 2019, https://privacyinternational.org/long-read/2724/every-police-force-uk-will-soon-use-body-worn-video-cameras-record-us-public.

The technology has been used in protests but also in other public gatherings, music concerts and football matches, shopping centres and high streets, and festivals. There is a valid concern that it could eventually be rolled out across all public spaces. The Metropolitan Police (MET) in the UK conducted ten trials already. A trial was conducted by Leicestershire Police at a music festival in 2015.[20] In August 2016, the MET used for the first time automated facial recognition technology to monitor and identify people at the Notting Hill Carnival.[21]

In March 2018, South Wales Police deployed facial recognition at a peaceful protest for the first time. Cardiff resident Ed Bridges attended this protest. He and Liberty took South Wales Police to court to force it to stop using facial recognition in public places but they court's decision has.[22] This has been the first time that any court in the world has considered automated facial recognition (AFR). The Divisional Court held that the current legal regime is adequate to ensure the appropriate and non-arbitrary use of AFR in a free and civilised society.[23] However, this decision will most probably be challenged.

Third, it is often unclear who might be on a 'watch list' or where the authorities obtain the images included in their watch list databases. The images in a watch list could come from a range of sources and do not just include images of people suspected of criminal wrongdoing. For example, the images may come from a custody images database, which contains pictures of people who have come into contact with the police, including thousands of innocent people.

Images could also come from social media. For example, FindFace, a face recognition application launched in early 2016 by a Russian based company, allows users to photograph people in a crowd and compares their picture to profile pictures on the popular social network VKontakte, identifying their online profile with 70% reliability.[24]

Four, the accuracy of facial recognition is far from being proven. Researchers from the University of Essex, among others, concluded that the technology failed 80% of the time.[25] They also pointed out that the watchlist was flawed with out-of-date information.

[20] Matthew Sparkes, "Police trial facial recognition software that can ID suspects 'in seconds'", *Daily Telegraph,* 17 July 2014, available at http://www.telegraph.co.uk/technology/news/10973185/Police-trial-facial-recognition-software-that-can-ID-suspects-in-seconds.html.

[21] The official statement is that they were just to trial the technology. They nonetheless stopped a number of people (26 in Sheffield's) and had a high rate of failure. Helena Hickey, "Met trialling facial recognition technology at Notting Hill Carnival", *Police Oracle*, 27 August 2016, available at https://www.policeoracle.com/news/police_it_and_technology/2016/Aug/26/met-trialling-facial-recognition-technology-at-notting-hill-carnival_92773.html/specialist;
Metropolitan Police Service, 30 August 2016, available at https://news.met.police.uk/news/notting-hill-carnival-2016-181523.

[22] See "Cardiff Resident launches first UK legal challenge to police use of facial recognition technology in public spaces", 13 June 2018, available at https://www.libertyhumanrights.org.uk/news/press-releases-and-statements/cardiff-resident-launches-first-uk-legal-challenge-police-use.

[23] The Court also held that South Wales Police's (SWP) use to date of AFR by has been consistent with the requirements of the Human Rights Act 1998 (HRA) and data protection legislation. R (Bridges) v Chief Constable of South Wales Police and Secretary of State for the Home Department [2019] EWHC 2341 (Admin), available at https://www.bailii.org/ew/cases/EWHC/Admin/2019/2341.html .

[24] Shaun Walker, "Face recognition app taking Russia by storm may bring end to public anonymity", *The Guardian,* 17 May 2016, available at https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity-vkontakte.

[25] Pete Fussey and Daragh Murray, "HRBDT Researchers Launch New Report on London Metropolitan Police's Trial of Live Facial Recognition Technology", 3 July 2019, available at https://hrbdt.ac.uk/hrbdt-researchers-launch-new-report-on-london-metropolitan-polices-trial-of-live-facial-recognition-technology/.

Finally, last but not least, the involvement of private companies in potential law enforcement measures, raises important questions around the rule of law. With private actors being involved in state functions, such as detecting crime, it is difficult to measure how individuals would be provided with the same guarantees against potential abuse, and how industry involvement in such measures is effectively regulated and openly scrutinised.

The use of facial recognition technologies during peaceful assemblies raise similar concerns to the ones discussed above with regard to IMSI catchers. Such indiscriminate interference with participants privacy inevitably affects the exercise of the freedom of peaceful protest.

Left unregulated, the routine collection and processing of *personal* information during peaceful protests may lead to the kind of abuses observed in other forms of covert surveillance operations. Given the serious interferences that government use of IMSI catchers and different types of facial recognition technologies pose to the right to freedom of peaceful assembly, including peaceful protests (and other fundamental rights), it is vital that governments are transparent about their use and adopt robust regulation of the use of this surveillance technology.

In particular, governments must make clear whether they use these technologies to conduct surveillance of peaceful gatherings or other associative activities and, if so, what rules, if any, govern this type of surveillance. They further need to be able to demonstrate that their use of these technologies is lawful, necessary and proportionate to achieve a legitimate aim as required under Article 21 of the International Covenant on Civil and Political Rights. Given the intrusiveness of such methods, the threshold for these tests should be especially high.[26]

It is also imperative that governments are transparent and set up a clear legal framework to regulate the retention, storage, access and deletion of any data collected via these surveillance methods. The indefinite retention of data of any person that wishes to peacefully protest is not compatible with the data protection principles and it interferes with the exercise of freedom of peaceful protest. Instead at the moment many governments around the world continue to shroud their use of these and other technologies in secrecy.[27]

Furthermore, Privacy International is concerned that there has not been enough consideration of the cumulative negative impact of the deployment of different surveillance technologies during peaceful protests. Their combined deployment can also result to disproportionate interference with the exercise of freedom of peaceful protest, right to privacy and other human rights.

Finally, Privacy International encourages the UN High Commissioner for Human Rights to develop her analysis on states' positive obligation to protect the right to peaceful protest against abuses by non-state entities, such as companies and private individuals. As the Special Rapporteur on Freedom of Expression underlined "The activities of companies in the ICT sector implicate rights to privacy, religious freedom and belief, opinion and expression, assembly and association, and

[26] Joint report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association and the Special Rapporteur on extrajudicial, summary or arbitrary executions on the proper management of assemblies, 4 February 2011 (A/HRC/31/16), at § 74.
[27] Thomas, Elise, "New Surveillance Tech Means You'll Never Be Anonymous Again", Wired UK, 16 September 2019: https://www.wired.co.uk/article/surveillance-technology-biometrics.

public participation, among others."[28] Instead of validating by default the use of such technologies, governments should be continuously justifying their use, and when it is decided to use them they must be adopting legislation and taking measures to ensure that strict limitations of the use of such technologies are in place.

3. The right to peaceful protest online

Demonstrators are often relying on social media platforms both to organise protests and also to protest online. Whether the online space is used as a medium facilitating peaceful protests or as a platform for protesting, social media platforms, mobile applications, and other web resources empower and facilitate exchanges of information, expressions of views and organisation of peaceful assemblies.

Social media were extensively used to raise awareness and mobilise protests during what became known as 'Arab Spring' (starting from Tunisia in 2010, followed by the protests in Egypt, Libya, Syria and Yemen). In their aftermath, the potential of new technologies in facilitating and enhancing the freedoms of peaceful assembly and association became apparent.[29] Most recently the "gilets jaunes" movement in France relied heavily on Facebook to raise awareness and mobilise the public – from the online petition that sparked the first gatherings to post-protest photos, polls on specific maters and live videos.[30]

These platforms are almost invariably owned by a handful of private companies. As noted by the Special Rapporteur on Freedom of Expression "Internet companies have become central platforms for discussion and debate, information access, commerce and human development."[31]

Privacy International encourages the UN High Commissioner for Human Rights to develop her analysis of states' obligations to ensure that individuals can enjoy their right to freedom of assembly online without undue interferences by state and non-state actors. There has been little to no guidance so far regarding the safeguards that states need to put in place to respect and protect the exercise of the peaceful protest online.

Privacy International has particular concerns in relation to the increased and unregulated use of intelligence-gathering both by state and non-state actors, known as social media intelligence.

3.1 Social media intelligence (SOCMINT)

[28] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018 (A/HRC/38/35), at § 5.
[29] Other examples include the online protests in the USA in 2012 against United States Stop Online Privacy Act (SOPA) and Protect IP Act (PIPA); the anti-austerity indignados movement in Spain; the Occupy protects in New York and London; the Put People First (PFF) in the UK; the 2009 Pink Chaddi campaign in India; the 2015 Coalition for Clean and Fair Elections (Bersih) in Malaysia; the StopEvictions online campaign in Pakistan and others.
[30] See, Pauline Bock, "How Facebook fuelled France's violent gilet jaunes protests", *Wired*, 6 December 2018: https://www.wired.co.uk/article/les-gilet-jaunes-yellow-vest-protests-in-france-facebook.
[31] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, 6 April 2018 (A/HRC/38/35), at § 9.

SOCMINT refers to the collective of tools and solutions that allow governments and companies to monitor social media channels, conversations and internet use, respond to social signals and synthesise social data points into meaningful trends and analysis. SOCMINT includes monitoring of content, such as messages or images posted, and other data, which is generated when someone uses a social media networking site. This information can be private and public.[32]

Any 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.

The authorities' collection and analysis of *publicly available* social media data without informed public awareness and debate, clear and precise statutory frameworks, and robust safeguards fall short of standards of protection of the right to privacy and of personal data protection. Governments and companies have defended the use of publicly available data because by their public nature they do not interfere with people's privacy. However, this inaccurately represents the intrusive method of collection, retention, use and sharing of an individual's personal data. First, 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. Second, the development of technologies that can process and aggregate a vast range of data, including personal data, allow the creation of profiles of individuals. These profiles can be used to infer data about a person and assign additional characteristics, revealing personal details about that person far exceeding what they "publicly" posted.

In Thailand, there is increasing monitoring of social media and other internet-based communications services for the purpose of identifying political dissent, often for prosecutions under the overbroad crime of *lèse majesté* and related crimes. This degree of intrusion amounts to an unlawful interference with privacy and chills assembly and freedom of expression.[33]

In the United Kingdom, police forces systematically gather and analyse social media and internet postings from so-called "*domestic extremists*". A 2013 report suggested that a staff of 17 officers in the National Domestic Extremism Unit was scanning the public's tweets, YouTube videos, Facebook profiles, and other public online postings.[34] The UK independent reviewer of terrorism legislation has commented that, "UK law enforcement and security and intelligence agencies of course use [open source intelligence], though the extent of that use is not publicly known.".[35] The UK Surveillance Commissioner added, "Perhaps more than ever, public authorities

[32] Privacy International, Social Media Intelligence explainer, available at https://privacyinternational.org/explainer/55/social-media-intelligence. See also Privacy International, How your social media activity is monitored by the police, 11 March 2019 available at https://privacyinternational.org/long-read/2722/how-your-social-media-activity-monitored-police.

[33] See Privacy International, Submission to the Human Rights Committee: Thailand, 3 April 2017, available at https://privacyinternational.org/advocacy-briefing/978/submission-right-privacy-thailand-human-rights-committee-119th-session.

[34] Paul Wright, "Meet Prism's little brother: Socmint", *Wired,* 26th June 2013, available at http://www.wired.co.uk/article/socmint.

[35] David Anderson QC, "A Question of Trust: Report of the Investigatory Powers Review", June 2015, at § 4.29.

now make use of the wide availability of details about individuals, groups or locations that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices. I repeat my view that just because this material is out in the open, does not render it fair game".[36] The continuous surveillance of persons online, what they say or do, when, with whom, does not differ from physically following individuals around the city.

In the United States, the Department of Homeland Security is seeking to expand the use of social media intelligence, including by recording social media handles.[37] Similar practices have been reportedly adopted by Israeli, Egyptian and other governments.

The unregulated use of SOCMINT negatively affects the exercise of the right to freedom of peaceful assembly. It has a chilling effect on individuals wishing to organise online, as well as using social media platforms to organise and promote peaceful assemblies. Furthermore, the degree of intrusiveness does not only constitute an unlawful interference with the right to privacy, but it also directly undermines the exercise of freedom of peaceful assembly. SOCMINT techniques and technologies allow to do much more than collecting and retaining publicly available information.

4. Conclusions

Privacy International encourages the UN High Commissioner for Human Rights while developing the thematic report on the promotion and protection of human rights in the context of peaceful protests to take into account and address the above, particularly:

- To highlight the relationship between the right to privacy and the right to freedom of peaceful protests;
- To determine the standards and conditions for the deployment of new surveillance technologies, focusing on specific technologies such as IMSI catchers and facial recognition, to ensure compliance with human rights standards; and
- To address the issue of peaceful protest online and in particular to ensure that limitations are imposed to the use of SOCMINT techniques and technologies both for state and non-state actors.

[36] Office of Surveillance Commissioners Annual Report for 2014-15, at § 5.72.
[37] See Privacy International, Submission to Department of Homeland Security, Privacy Office (USA), Regarding DHS Social Media Retention Policy, 19 October 2017, available at https://privacyinternational.org/sites/default/files/2017-10/PrivacyInternational_DHS_Oct2017_0.pdf.

PRIVACY INTERNATIONAL

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint
Instagram @privacyinternational

UK Registered Charity No. 1147471