Privacy International's response to call for input to a report on the right to privacy in the digital age by the UN High Commissioner for human rights

April 2018

Introduction

Privacy International supports the work of the Office of the High Commissioner for Human Rights (OHCHR) and other UN human rights bodies and experts to promote the right to privacy in the digital age. This forthcoming report offers an opportunity to reflect on the developments that have taken place since the first report by the UN High Commissioner in 2014 and to assess the extent that states, companies and other actors have implemented the recommendations contained therein.

Privacy International suggests the following main recommendations be included in the report of the High Commissioner:

- Clarify that authorisation of surveillance measures requires reasonable suspicion that a particular individual has committed or is committing a criminal offence or is engaged in acts amounting to a specific threat to national security.
- Recognise that the nature of the interference with the right to privacy is the same whether an intelligence agency initially obtains communications and data on its own, or accesses communications and data obtained by another intelligence agency, and intelligence sharing should therefore be subject to the same principles of legality, necessity and proportionality that govern surveillance activities.
- Explicitly recognize the interference with privacy and other fundamental rights as well as the and security risks posed by government hacking and recommend that states refrain from using this surveillance technique.
- Note that human rights law prohibits the imposition of a requirement of blanket, indiscriminate retention of communications data on telecommunications and other companies.
- Note that the right to privacy applies in public places, online and offline.
- Note that there can be serious privacy implications of monitoring 'publicly available' information on social networking sites. The fact that data is *publicly available* does not justify unregulated and un-checked collection, retention, analysis and other processing.

- Recommend that states should only collect and retain biometric data when they can demonstrate it is necessary and proportionate to achieve a legitimate aim and never in a generalised, indiscriminate matter.
- Recognise that the right to privacy gives individuals the right to object to profiling and to control over decisions made by profiling, including providing individuals with access to the data on which such decisions are based, information about the way in which the data is automatically processed and the extent to which decisions will rely on data derived or predicted through profiling.
- Recommend that automated decision-making, without meaningful human intervention, are prohibited, except in cases where the individuals concerned give their explicit and informed consent.
- Recommend that states adopt comprehensive data protection legislation and establish independent data protection authorities, with powers to investigate reports, receive complaints from individuals and organisations, issue fines and other effective penalties for the unlawful processing of personal data by private and public bodies. Independent authorities, such as data protection authorities, should be in a position to audit automated decisions to test for bias and unlawful discrimination.

Additional recommendations are included at the end of each sections below.

1 Surveillance and communications interception

Since the 2014 report of the High Commissioner on the right to privacy in the digital age, UN human rights mechanisms have significantly increased their scrutiny of surveillance laws and practices.[1] Unfortunately, however, recommendations by these mechanisms have often been ignored by member states.

Privacy International would like to highlight three broad trends:

- **Mass surveillance**: Governments around the world continue to conduct mass surveillance. Some governments operate these programs outside of any existing domestic legal framework. Other governments have adopted laws that seek to legalise post facto these programs.
- **Intelligence sharing**: Governments have failed to place their intelligence sharing practices on adequate legal footing. They have further failed to subject such practices to adequate safeguards and oversight, despite their interference with privacy.
- **Hacking for surveillance purposes**: Governments are increasingly relying on hacking for surveillance purposes, which presents novel risks for both privacy

[1] For a compendium of recent jurisprudence and recommendations by international and regional bodies and experts, please see Privacy International's Guide to International Law and Surveillance, https://www.privacyinternational.org/feature/993/guide-international-law-and-surveillance.

and security. This proliferation is due in part to the growing availability and relative affordability of hacking technologies.

1.1 Mass surveillance

Since 2014, international human rights bodies and experts have found mass surveillance to be in violation of human rights law. Notably, that year, the UN Special Rapporteur on counter-terrorism stated that "the adoption of mass surveillance technology undoubtedly impinges on the very essence of [the right to privacy] […] mass surveillance of digital content and communications data presents a serious challenge to an established norm of international law." He continued to note that "it is incompatible with existing concepts of privacy for States to collect all communications or metadata all the time indiscriminately" and that "[t]he very essence of the right to the privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis."[2] In 2016, the UN High Commissioner on Human Rights reiterated that "[m]ass secret surveillance is not permissible under international human rights law, as an individualised necessity and proportionality analysis would not be possible in the context of such measures."[3]

The European Court of Human Rights has similarly found that a government, in authorising surveillance, "must be capable of verifying the existence of a reasonable suspicion against the person concerned, in particular, whether there are factual indications for suspecting that person of planning, committing or having committed criminal acts or other acts that may give rise to secret surveillance measures, such as, for example, acts endangering national security."[4] It must also "ascertain whether the requested [surveillance] meets the requirement of 'necessity in a democratic society', as provided by Article 8 § 2 of the [ECHR], including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means." The Court concluded that an authorisation for surveillance must identify "a specific person" or "a single set of premises" in order to facilitate the necessity and proportionality analysis.[5]

Despite this clear jurisprudence and legal analysis, states, particularly in Europe, have continued to pass laws authorising mass surveillance. Moreover, other states

---

[2] Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc. A/69/397, 23 Sept. 2014.
[3] UN High Commissioner for Human Rights, Report on best practices and lessons learned on how protecting and promoting human rights contribute to preventing and countering violent extremism, UN Doc. A/HRC/33/29, 21 July 2016.
[4] Zakharov v Russian Federation, European Court of Human Rights, Grand Chamber, App. No. 47142/06, 4 Dec. 2015, para. 260.
[5] *Id.* at paras. 259-267.

continue to carry out mass surveillance even in the absence of explicit legislation regulating this practice.

- In **France** two new surveillance laws were adopted in 2015.[6] These laws interfere with the right to privacy and other fundamental freedoms in an excessive and disproportionate manner, as noted by the UN Human Rights Committee in July 2015[7] and by five UN Special Rapporteurs in January 2016.[8] In particular, Law No. 2015-912 of 24 July 2015 provides for the installation of "black boxes" on the telecom and internet networks to conduct real-time automated processing of data in ways that is indiscriminate.[9]
- In **Germany**, the Communications Intelligence Gathering Act, adopted in 2016, authorises the Federal Intelligence Service (BND) to gather and process communications of foreign nationals abroad. As noted by the UN Special Rapporteur on privacy, "mass and targeted surveillance of extraterritorial communications between non-German citizens would be effectively authorized in cases where the communication interception is carried out in Germany".[10]
- In **Kenya**, the Security Law (Amendment) Act 2014 expands the surveillance powers of the intelligence services, while at the same time weakening the judicial authorisation procedure for those powers.[11]
- In **South Africa**, the National Communications Centre (NCC) - the government's national facility for intercepting and collecting electronic signals on behalf of the intelligence and security services – collects and analyses foreign signals (communication that emanates from outside the

---

[6] Intelligence Law n.2015-912 of 24 July 2015, available at http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&ca; International Surveillance Law n° 2015-1556 of 30 November 2015, available at http://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte.

[7] UN Human Rights Committee, Concluding observations on the fifth periodic report of France, UN Doc. CCPR/C/FRA/CO/5, 17 Aug. 2015.

[8] See UN Office of the High Commissioner for Human Rights, Déclaration publique sur la loi relative à l'état d'urgence et sur la loi relative à la surveillance des communications électroniques internationales, 19 Jan. 2016, http://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=16961&LangID=F.

[9] For a legal analysis of the privacy implicaitons, see Privacy International's the European Court of Human Rights in *Association Confraternelle de la Presse Judiciare and 11 Other Applications v. France*, available at: https://www.privacyinternational.org/feature/721/association-confraternelle-de-la-presse-judiciare-and-11-other-applications-v-france

[10] Report of the UN Special Rapporteur on the right to privacy in the digital age, UN doc. A/71/368, 30 August 2016, paragraph 37.

[11] See Privacy International, Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya, March 2017, https://www.privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf.

borders of South Africa or passes through or ends in South Africa) without a specific legal framework to do so. Reports suggest that NCC has the capacity to carry out mass interception of communications.[12]

- In **Switzerland**, the Federal Act of 25 September 2016 on the Intelligence Service introduces powers to conduct mass surveillance by intercepting communications running through internet cables that pass through Switzerland.[13] The Human Rights Committee expressed concerns the law "grants very intrusive surveillance powers to the Confederation's intelligence services on the basis of insufficiently defined objectives such as the national interest".[14]
- In the **United Kingdom**, the bulk powers included in the Investigatory Powers Act 2016 constitute, in the words of the High Commissioner, "one of the most sweeping mass surveillance regimes in the world, permitting the interception, access, retention and hacking of communications without a requirement of reasonable suspicion."[15]

Recommendations:

- The High Commissioner should reassert that mass surveillance is unlawful as it is an inherently disproportionate interference with the right to privacy.[16]
- The High Commissioner should clarify that authorisation of surveillance measures requires reasonable suspicion that a particular individual has committed or is committing a criminal offence or is engaged in acts amounting to a specific threat to national security.

1.2 Intelligence sharing between foreign intelligence agencies

Intelligence sharing is one of the most pervasive, and least regulated, surveillance practices in our modern world. Such sharing is facilitated by rapidly changing technology that has allowed for the storage and transfer of vast amounts of data within and between countries. Despite these dramatic changes, in many countries

[12] See Privacy International, Right2Know and Association for Progressive Communications, The right to privacy in South Africa, Submission to the UN Human Rights Committee, March 2016, https://www.privacyinternational.org/sites/default/files/2017-12/HRC_SouthAfrica_0.pdf.
[13] Loi fédérale sur le renseignement du 25 septembre 2015, available at http://grundrechte.ch/2015/6597.pdf.
[14] UN Human Rights Committee, Concluding observations on the fourth periodic report of Switzerland, UN Doc. CCPR/C/CHE/CO/4, 22 Aug. 2017.
[15] UN High Commissioner for Human Rights Zeid Ra'ad Al Hussein delivered the following speech at the Law Society in London, 26 June 2017, https://www.unog.ch/unog/website/news_media.nsf/(httpNewsByYear_en)/6B25EB688245C4D0C125814C002FEE4A?OpenDocument.
[16] Privacy International notes that many states describe mass surveillance by other terms, e.g. bulk collection.

around the world, the activities of intelligence agencies are insufficiently regulated, let alone their intelligence sharing practices. And yet non-transparent, unfettered and unaccountable intelligence practices, including intelligence sharing, pose substantive risks to human rights and the democratic rule of law.

Because intelligence sharing is such an opaque area of surveillance activity, we lack sufficient information about what these arrangements look like in practice. The Five Eyes Alliance (between the United States, the United Kingdom, Canada, Australia, and New Zealand) is one of the best known. But despite being nearly 70 years old, the public remains largely in the dark about this alliance, including the actual agreements that form it. Even less is known about some of the other surveillance partnerships that incorporate the Five Eyes, which include a range of European states.[17] Similarly, little is known about intelligence sharing in other parts of the world. A prominent example of such an arrangement is the Shanghai Cooperation Organisation, a security, economic, and political cooperation forum in which intelligence sharing is undertaken between China, India, Kazakhstan, Kyrgyzstan, Pakistan, Russia, Tajikistan, and Uzbekistan.[18]

Intelligence sharing constitutes a form of surveillance and therefore interferes with the right to privacy. Whether an intelligence agency initially obtains communications and data on its own, or accesses communications and data obtained by another intelligence agency, the nature of the interference with the right to privacy is fundamentally the same. Intelligence sharing also poses the risk that a state may use it to circumvent constraints on domestic surveillance by relying on their partners to obtain and then share information the state could not obtain

[17] For example, SIGINT Senior Europe ("SSEUR", the Five Eyes plus France, Germany, Spain, Italy, Belgium, the Netherlands, Denmark, Norway and Sweden); 9-Eyes (the Five Eyes plus Denmark, France, the Netherlands and Norway); 14-Eyes (the 9-Eyes plus Belgium, Germany, Italy, Spain and Sweden); 43-Eyes (the 14-Eyes plus the addition of the 2010 members of the International Security Assistance Forces to Afghanistan.) For further reading on the 43-Eyes see Five Eyes, 9-Eyes, and Many More, Electrospaces.net, 15 Nov. 2013, http://electrospaces.blogspot.co.uk/2013/11/five-eyes-9-eyes-and-many-more.html. The full list of 43 Eyes states are as follows: US, UK, Canada, Australia, New Zealand, Denmark, France, Netherlands, Norway, Belgium, Germany, Italy, Spain, Sweden, Albania, Armenia, Austria, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Finland, Georgia, Greece, Hungary, Iceland, Ireland, Latvia, Lithuania, Luxembourg, Macedonia, Montenegro, Poland, Portugal, Romania, Slovakia, Slovenia, South Korea, Switzerland, Turkey, and Ukraine. Privacy International acknowledges that the make-up of these alliances, particularly the 43-Eyes, may have shifted over time. The general lack of clarity around intelligence sharing arrangements makes it difficult to confirm their exact scope.

[18] Eleanor Albert, Council on Foreign Relations, The Shanghai Cooperation Organization Backgrounder, 14 Oct. 2015, available at https://www.cfr.org/backgrounder/shanghai-cooperation-organization.

under domestic law .[19] Examples of common constraints on domestic surveillance include restrictions on the types of surveillance techniques a state may use or on a state's ability to conduct surveillance of its own citizens or residents or members of a protected profession, such as journalists, lawyers and members of parliament. It is not clear, for instance, how these constraints might meaningfully apply where a state accesses or receives data obtained in bulk by another state. This data can contain the personal information of a vast number of individuals, the majority of whom are not suspected of any crime.

In addition, states may share intelligence with other states, who may then use that intelligence in a manner that facilitates serious human rights abuses. This risk is particularly acute where intelligence is shared with states with authoritarian governments, weak rule of law and/or a history of systematically violating human rights. In these contexts, such intelligence may form the basis for extrajudicial killings or contribute to unlawful arrest or detention or to torture and other cruel, inhuman or degrading treatment. Moreover, certain groups may be particularly vulnerable to these abuses, such as dissidents, journalists and human rights defenders.[20] Relatedly, intelligence received by one state from another may have been obtained in violation of international law, including through torture and other cruel, inhuman or degrading treatment.

The human rights risks posed by intelligence sharing are heighted by the current lack of transparency, accountability and oversight of intelligence sharing arrangements. Such arrangements are most often confidential and not subject to public scrutiny. Agreements may expressly state that they are not to be construed as legally binding instruments according to international law.[21]

---

[19] *See* European Commission for Democracy through Law (Venice Commission), *Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on the Democratic Oversight of Signals Intelligence Agencies*, Study No. 719/2013 CDL-AD(2015)006, 7 Apr. 2015, para. 11; Commissioner for Human Rights, Council of Europe, *Positions on Counter-Terrorism and Human Rights Protection*, 5 June 2015, p. 11 (noting that "the principle of making data available to other authorities should not be used to circumvent European and national constitutional data-protection standards").

[20] *See* Born et al., *Making International Intelligence Cooperation Accountable*, 2015, pp. 40-45; International Commission of Jurists, *Assessing Damage, Urging Action*, 2009, pp.81-85.

[21] *See, e.g.*, Memorandum of Understanding Between the National Security Agency/Central Security Service (NSA/ CSS) and the Israeli SIGINT National Unit (ISNU) Pertaining to the Protection of U.S. Persons, available at www.statewatch.org/news/2013/sep/nsa-israel-spy-share.pdf (noting that "this agreement is not intended to create any legally enforceable rights and shall not be construed to be either an international agreement or a legally binding instrument according to international law"). This agreement was first published by The Guardian on 11 September 2013.

Recent UN Security Council resolutions on counter-terrorism expressly encourage intelligence sharing.[22] But as noted by the UN Special Rapporteur on Counter-Terrorism and Human Rights in 2015, "the absence of laws to regulate information-sharing agreements between States has left the way open for intelligence agencies to enter into classified bilateral and multilateral arrangements that are beyond the supervision of any independent authority."[23]

Regretfully this remains the situation now, as recently confirmed in the report of the European Union Agency for Fundamental Human Rights.[24] With very few exceptions, even newly enacted, allegedly all-encompassing surveillance legislation has failed to place intelligence sharing on proper statutory footing, compliant with the principle of legality under international human rights law. This failure, combined with the secrecy surrounding intelligence sharing practices, makes independent oversight and accountability of such practices extremely challenging.

The need for transparency and oversight is especially pressing because intelligence sharing inherently poses a number of accountability challenges. Generally speaking, intelligence agencies lack control over the actions of their foreign partners. In addition, many intelligence sharing arrangements prohibit the disclosure of information shared between agencies to third parties, which may include oversight mechanisms, without the prior consent of the state from which the information originated.[25]

These transparency, oversight and accountability gaps has also been observed by a range of international human rights bodies.[26] As a result, human rights bodies have

---

[22] *See* UN Security Council, Resolution 2396, UN Doc. S/RES/2396, 21 Dec. 2017.This resolution builds upon prior UN Security Council calls to increase intelligence sharing in the counter-terrorism context. *See, e.g.*, UN Security Council, Resolution 1373, UN Doc. S/RES/1373, 28 Sept. 2001.

[23] Report of the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, UN Doc. A/69/397, para. 44, 23 Sept. 2014.

[24] Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume II: field perspective and legal update, Oct. 2017, http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega; see also Privacy International, Human Rights Implications of Intelligence Sharing, Sept. 2017, https://privacyinternational.org/sites/default/files/2017-11/PI-Briefing-to-National-Intelligence-Oversight_0.pdf.

[25] This prohibition is typically referred to as the "third party rule" or the "originator control principle." A requirement that oversight bodies seek the consent of a foreign intelligence agency to access information is fundamentally detrimental to oversight. As a matter of principle, requiring oversight bodies to seek such permission can cripple their independence. And as a matter of practice, foreign partners are unlikely to consent to such a request.

[26] For example, the EU Fundamental Rights Agency noted how "[v]ery few Member States allow expert bodies to assess international agreements and/or cooperation criteria" establishing intelligence sharing either ex ante or ex post. Surveillance by intelligence services: fundamental

repeatedly emphasized the importance of and called for effective oversight of intelligence sharing arrangements. For example, in *Szabó and Vissy v. Hungary*, the European Court of Human Rights noted:

> "The governments' more and more widespread practice of transferring and sharing amongst themselves intelligence retrieved by virtue of secret surveillance – a practice, whose usefulness in combating international terrorism is, once again, not open to question and which concerns both exchanges between Member States of the Council of Europe and with other jurisdictions – is yet another factor in requiring particular attention when it comes to external supervision and remedial measures."[27]

The UN Human Rights Committee has accordingly recommended that a number of states put in place "effective and independent oversight mechanisms over intelligence-sharing of personal data".[28] And the Council of Europe Commissioner for Human Rights has recommended that intelligence oversight bodies be mandated to scrutinise the human rights compliance of security service co-operation with foreign bodies, including co-operation through the exchange of information.[29]

Recommendations:

- The High Commissioner should recognise that the nature of the interference with the right to privacy is the same whether an intelligence agency initially obtains communications and data on its own, or accesses communications and data obtained by another intelligence agency; and intelligence sharing should therefore be subject to the same principles of legality, necessity and proportionality that govern surveillance activities.
- The High Commissioner should recommend that states establish, through primary legislation, publicly accessible legal frameworks governing intelligence sharing, which should include giving independent oversight bodies the mandate to exercise their powers with respect to intelligence

---

rights safeguards and remedies in the EU, Volume II: field perspective and legal update, Oct. 2017, http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega.

[27] Szabó and Vissy v. Hungary, European Court of Human Rights, App. No. 37138/14, 12 Jan. 2016, para. 78.

[28] See UN Human Rights Committee, Concluding Observations on the Seventh Periodic Report of Sweden, UN Doc. CCPR/C/SWE/CO/7, 28 Apr. 2016, paras. 36-37; UN Human Rights Committee, Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland, UN Doc. CCPR/C/GBR/ CO/7, 17 Aug. 2015, para. 24; UN Human Rights Committee, Concluding Observations on the Sixth Periodic Report of Canada, UN Doc CCPR/C/CAN/CO/6, 13 Aug. 2015, para. 10.

[29] Council of Europe Commissioner for Human Rights, Democratic and effective oversight of national security services, 2015, recommendation 5, https://rm.coe.int/1680487770.

sharing, including by, *inter alia*, fully accessing information held by the intelligence services, including information related to intelligence sharing, and undertaking investigations on the oversight body's own initiative.

1.3 Government hacking for surveillance purposes

A growing number of governments around the world are embracing hacking to facilitate their surveillance activities. But as a form of government surveillance, hacking presents unique and grave threats to our privacy and security.

Governments employ hacking for surveillance in a variety of contexts and using a wide range of techniques. Some government officials are justifying the adoption of hacking for surveillance as a way to access encrypted communications. In making this argument, they fail to distinguish between the content of communications and metadata, the latter of which is typically not encrypted and remains widely available to intelligence agencies and police forces using traditional surveillance methods. Further, hacking is perhaps the most intrusive of surveillance techniques and is used to intercept and collect all kind of communications and data, encrypted or not. For these reasons, Privacy International does not accept that hacking is the only method available to obtain useful intelligence from encrypted communications.

- Reports have emerged that governments are using hacking to target journalists and human rights defenders in **Bahrain**[30]**, Mexico**[31]**, Morocco**[32] **and the United Arab Emirates**.[33]
- Other countries, such as **France, Italy, the Netherlands, and Switzerland** have recently introduced legislation to authorise government hacking for surveillance or are in the process of doing so (e.g. **Argentina** and **Sweden**.)
- The **United Kingdom** has explicitly included bulk hacking powers in the Investigatory Powers Act 2016, allowing for mass hacking by both law

[30] See Privacy International, Bahraini Government, With Help From FinFisher, Tracks Activists Living In The United Kingdom, available at: https://www.privacyinternational.org/blog/1231/bahraini-government-help-finfisher-tracks-activists-living-united-kingdom

[31] See Privacy International, Letter and briefing on human rights implications of reported Mexican government hacking, available at: https://www.privacyinternational.org/advocacy-briefing/994/letter-and-briefing-human-rights-implications-reported-mexican-government

[32] See Privacy International, Their Eyes on Me, available at: https://www.privacyinternational.org/report/1125/their-eyes-me-stories-surveillance-morocco

[33] See Office of the U.N. High Commissioner for Human Rights, *UN rights experts urge UAE: "Immediately release Human Rights Defender Ahmed Mansoor,"* 28 Mar. 2017, available at http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=21449&LangID=E

enforcement bodies as well as the security and intelligence services.[34] It is significant that even the Home Office has suggested that the authorising authority would be unable to assess the proportionality and necessity of bulk hacking by the security and intelligence services.[35]

Government hacking also raises significant extraterritoriality concerns. Government hacking can easily cross borders and affect individuals across many jurisdictions, including those who may be unrelated to a government operation. For example, in 2015, on the basis of a single warrant, the **United States** FBI ultimately hacked over 8,700 computers located in 120 countries and territories.[36]

Government hacking has the potential to be far more privacy intrusive than any other surveillance technique, permitting the government to remotely and secretly access our personal devices and the data stored on them as well as to conduct novel forms of real-time surveillance, for example, by turning on microphones, cameras, or GPS-based locator technology. Hacking allows also governments to manipulate data on our devices, including corrupting, planting or deleting data, or recovering data that has been deleted, all while erasing any trace of the intrusion. For that reason the UN Special Rapporteur for Counter-Terrorism has observed that hacking constitutes a "new form[ ] of surveillance" as it permits states "to alter – inadvertently or purposefully – the information contained therein," which "threatens not only the right to privacy [but also] procedural fairness rights with respect to the use of such evidence in legal proceedings."[37]

At the same time, government hacking has the potential to undermine the security of our devices, networks and infrastructure. Government hacking often depends on exploiting vulnerabilities in systems to facilitate surveillance objectives. It is therefore fundamentally at cross-purposes with computer security, which seeks to identify vulnerabilities in order to secure systems. Government hacking may also involve manipulating people to undermine the security of their own systems. These

[34] See Privacy International and Open Rights Group's Submission to the Joint Committee on Human Rights on the Draft Investigatory Powers Bill, 7 Dec. 2015; Privacy International, **Written Evidence to the Science and Technology Committee**, 27 Nov. 2015.

[35] See Privacy International's submission on consultation on the draft Codes of Practices, Investigatory Powers Act, https://www.privacyinternational.org/sites/default/files/2017-12/Privacy%20International%20-%20Response%20to%20Consultation%20on%20IPA%20Codes%20of%20Practice%20-%20April%202017.pdf.

[36] See United States v. Levin, United States v. Werdene, United States v. Eure, United States v. Tippens, Privacy International amicus curiae briefings to US Courts of Appeals, available at https://www.privacyinternational.org/feature/141/united-states-v-levin-united-states-v-werdene-united-states-v-eure-united-states-v.

[37] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/23/40, 17 April 2013, para. 62.

techniques prey on user trust, the loss of which can further undermine the security of systems and the internet.

For these reasons, even where governments conduct surveillance in connection with legitimate activities, they may never be able to demonstrate that hacking as a form of surveillance is compatible with international human rights law, notable its necessity and proportionality. To date, however, there has been insufficient public debate about the scope and nature of these powers and their privacy and security implications. To address this gap, Privacy International published a set of ten minimum safeguards to assess government hacking in light of applicable international human rights law.[38]

Recommendations:

- The High Commissioner should explicitly recognize the interference with privacy and other fundamental rights as well as the and security risks posed by government hacking and recommend that states refrain from using this surveillance technique.
- The High Commissioner should recommend that any government which nonetheless conducts hacking for surveillance purposes should carry out a thorough assessment based on international human rights law to establish if these powers are compatible with human rights law, and in particular with the principles of legality, necessity and proportionality.

2. National legislative and regulatory frameworks concerning the collection, processing, retention or use of personal data

2.1 Data retention

States across the world continue to subject the interception of and access to communications data to no or significantly lower safeguards than the content of communications, despite the recognition by the UN Human Rights Council that "metadata, when aggregated, can reveal personal information that can be no less sensitive than the actual content of communications".[39]

In particular, states continue to impose mandatory obligations on telecommunications companies and internet service providers to retain

[38] Privacy International, Government hacking and surveillance: 10 necessary safeguards, available at: https://www.privacyinternational.org/advocacy-briefing/1057/hacking-safeguards-and-legal-commentary

[39] Human Rights Council resolution on the right to privacy in the digital age, UN Doc. A/HRC/RES/34/7, 23 Mar. 2017.

communications data of their subscribers in an untargeted and indiscriminate manner, which violates established human rights standards.

The UN Human Rights Committee has confirmed that data retention policies constitute an interference with the right to privacy and that as a general rule states should "refrain from imposing mandatory retention of data by third parties".[40] Further, data retention has significant implications for the right to freedom of expression, particularly as mandatory data retention de facto limits the capacity of individuals to remain anonymous.[41]

- **Colombia** imposes an obligation on telecommunications service providers to retain data for up to five years for the purposes of criminal investigation and intelligence activities.[42]
- **EU member states** – Despite the Tele-2/Watson judgment of the Court of Justice of the European Union (21 December 2016), which found that laws requiring general and indiscriminate retention of all traffic and location data to be in violation of the European Charter on Fundamental Rights, most EU member states' legislation are not in compliance with the judgment.[43]
- In **Pakistan**, the Prevention of Electronic Crimes Act (PECA 2016) provides for mandatory mass retention of traffic data by service providers for a minimum of one year.[44]
- In **South Africa**, the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) requires telecommunication service providers to store communications data, i.e. information about a communication, but not the content of such communication, for up to five years.[45]

---

[40] UN Human Rights Committee, Concluding Observations of the Fourth Periodic Report of the United States of America, UN Doc. CCPR/C/USA/CO/4, 23 April 2014, para. 22.

[41] See Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/29/32, 22 May 2015, para. 55, noting that "Broad mandatory data retention policies limit an individual's ability to remain anonymous. A State's ability to require Internet service and telecommunications providers to collect and store records documenting the online activities of all users has inevitably resulted in the State having everyone's digital footprint."

[42] Articles 4 and 5 of Decree 1704 of 2012 and Article 44 of Law 1621 of 2013.

[43] See Privacy International, National Data Retention Laws since the CJEU's Tele-2/Watson Judgment, Sept. 2017, https://www.privacyinternational.org/report/53/report-national-data-retention-laws-cjeus-tele-2watson-judgment.

[44] Section 32 of the Prevention of Electronic Crimes Act (PECA 2016) http://www.na.gov.pk/uploads/documents/1472635250_246.pdf

[45] Article 30(1)(b) of the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA) http://www.justice.gov.za/legislation/acts/2002-070.pdf

- In **Thailand**, the Computer Crimes Act requires that traffic data be retained by service providers for a period that can be extended for up to a year if requested by a competent official.[46]

Recommendations:

- The High Commissioner should reiterate that surveillance of communications data represents an equally serious interference with the right to privacy as surveillance of communications content.
- The High Commissioner should clarify that human rights law prohibit the imposition of a requirement of blanket, indiscriminate retention of communications data on telecommunications and other companies.

3. Growing reliance on data driven technologies

Increasingly devices, networks and services generate data that is used to identify and distinguish individuals from each other and map their behaviour, predict their future behaviour and affect (or even direct) such behaviour.

In this briefing, Privacy International focuses on the following aspects of modern data driven technologies, which can have significant implications for human rights:

- Processing of data obtained from **publicly available sources** in physical and digital spaces (e.g. **Smart Cities and Social Media Intelligence)**;
- Adoption of **biometric technologies** for identification schemes and delivery of social services by public authorities;
- **Profiling and automated decision making**.

3.1 "Publicly available" data and privacy

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 be obtained from public spaces. This includes physical spaces, such data collected in the context of **smart cities** projects. Similarly, in "digital spaces", there has been a significant rise in the application of social medial intelligence (**SOCMINT**) to monitor individuals' public postings online.

Governments and companies argue that this collection and analysis of data 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

[46] Section 26 of the Computer Crimes Act B.E. 2550 (2007).

data obtained from public places and through social media. The privacy intrusion is then furthered when publicly available data sets are aggregated.

For example, machine learning systems have been able to identify about 69% of protesters who are wearing caps and scarves to cover their faces.[47] 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.[48]

Whilst this data is derived from *publicly available* information, international human rights standards apply. The European Court on Human Rights has long held that "there is […] a zone of interaction of a person with others, even in a public context, which may fall within the scope of 'private life'". Among the relevant considerations, the Court held, is "the question whether there has been a compilation of data on a particular individual, whether there has been processing or use of personal data […] in a manner or degree beyond that normally foreseeable."[49]

Left unregulated, the routine collection and processing of *publicly available* information for intelligence gathering may lead to the kind of abuses observed in other forms of covert surveillance operations.

- For example, in **Colombia**, the Police Code contains a definition of privacy, which is unduly narrow (Article 32.) By linking the right to privacy with private physical spaces, it excludes from privacy protection any person or assets (such as cars or electronic devices) placed in public places, including bars, restaurants, etc. Conversely, the code defines public space in a very broad way, including notably "the electromagnetic spectrum". The combined result of these definitions is of significant concern to the protection of privacy. The Human Rights Committee has expressed concerns that the code "defines the concept of "public areas" in a very broad sense that includes the electromagnetic spectrum, and by the fact that all the information and data gathered in public areas are considered to be in the public domain and to be freely accessible".[50]

[47] Singh, A., Patil, D., Reddy, G.M. and Omkar, S.N., 2017. Disguised Face Identification (DFI) with Facial KeyPoints using Spatial Fusion Convolutional Network. https://arxiv.org/pdf/1708.09317.pdf.
[48] Available from: https://www.theguardian.com/technology/2016/may/17/findface-face-recognition-app-end-public-anonymity- vkontakte
[49] Peck v. United Kingdom, European Court on Human Rights, Application no. 44647/98, 28 Jan. 2003.
[50] UN Human Rights Committee, Concluding observations on the seventh periodic report of Colombia, UN Doc. CCPR/C/COL/CO/7, 17 Nov. 2016.

3.1.1 Smart Cities

While the term "smart cities" encompasses many different programs, Privacy International's research suggest that these initiatives have in common a focus on collection and processing of data, facilitated by ever more capable sensor technologies.[51] The World Bank, for example, defines smart cities as "a technology-intensive city, with sensors everywhere and highly efficient public services, thanks to information that is gathered in real time by thousands of interconnected devices."[52]

These sensors in public places vary widely in purpose and design – they include traditional CCTV (including to facilitate Automated Number Plate Recognition and Facial Recognition), microphones (e.g. to capture specific sounds), environmental sensors (e.g. to detect variations in heat and humidity), movement sensors (e.g. to track the number and variety of people or vehicles), beacons (e.g. to detect Bluetooth devices), wifi networks (e.g. to detect wifi capabilities on devices), and IMSI catchers (e.g. to identify mobile phones). Much of this data generation and transmission is done without the knowledge or involvement of the individual whose data is being captured; and it is increasingly the case that the individual can do little to prevent it.

- For example, in 2012, the Davao City Government of the **Philippines** invested in an IBM Intelligent Operation Centre (IOC) specifically for security reasons. The platform enables the coordination of the various agencies that work on public safety. It was designed to allow staff from the Public Safety Security Command Centre (PSSCC) – a division under the office of the City Mayor dedicated to providing "protection, security, safety and risk management to the people of Davao City" – to "monitor and respond to a wide range of safety related incidences from a central location."[53] However, Davao City has witnessed serious repressions of political dissent and high rates of extrajudicial killings and abuses by security services, which

[51] See Privacy International, Smart Cities: utopian visions, dystopian realities, October 2017, available at: https://www.privacyinternational.org/report/638/smart-cities-utopian-vision-dystopian-reality

[52] See "Smart Cities, The World Bank, 8 January 2015, available at http://www.worldbank.org/en/topic/ict/ brief/smart-cities

[53] See "City of Davao and IBM Collaborate to Build a Smarter City," IBM, 27 June 2012. More information available in Privacy International's report, supra.

undermines the idea that 'smart' policing technology would be effective to address serious human rights violations.[54]

3.1.2 Social Media Intelligence (SOCMINT)

Among the disturbing examples of "*overt*" methods of intelligence-gathering is social media intelligence (SOCMINT.) 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. 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. This privacy invasion is heightened by the development of technologies that can process and aggregate a vast range of data, including personal data, creating profiles of individuals.

- **Thailand** 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, which results in unlawful intrusion into privacy and chills freedom of expression.[55]
- In the **United Kingdom**, police forces 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.[56] 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.".[57] The UK Surveillance Commissioner added, "Perhaps more than ever, public authorities 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

[54] "Ex-Officer in Philippines Says He Led Death Squad at Duterte's Behest," Felipe Villamor, 20 February 2017, available at: https://www.nytimes.com/2017/02/20/world/asia/rodrigo-duterte-philippines-death- squad.html

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

[56] *Wired*, 26th June 2013: http://www.wired.co.uk/article/socmint

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

communication devices. I repeat my view that just because this material is out in the open, does not render it fair game".[58]

- 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.[59]

Recommendations:

- The High Commissioner should clarify that the right to privacy applies in public places, online and offline.
- The High Commissioner should note that there can be serious privacy implications of monitoring 'publicly available' information on social networking sites. The fact that data is *publicly available* does not justify unregulated and un-checked collection, retention, analysis and other processing.

3.2 Biometric technologies

Scores of developing countries across Africa, Asia and Latin America have been rushing to adopt biometric technology for a range of purposes: from conducting population registration in countries where birth registration has not previously been systematic, to conducting elections, or as a means of facilitating access and delivery of certain services such as food, health care and other basic social needs.[60]

Whilst the majority of developing countries include the right to privacy in their constitutions, they often lack laws, including data protection laws, to implement this right. In fact, the adoption of new technologies is rarely preceded by the adoption and implementation of robust regulatory frameworks. This failure means that the risks are not accessed and identified and thus corresponding risk mitigating measures are not implemented.

The use of biometric data does not guarantee the protection of one's identity. And unlike regular ID cards, the use of biometric data raises additional concerns and irreversible consequences. For example, if one's biometric data is stolen or misused it means their legal identity is compromised.[61]

---

[58] Office of Surveillance Commissioners Annual Report for 2014-15, at §5.72.

[59] See Privacy International, Submission to Department of Homeland Security, Privacy Office (USA), Regarding DHS Social Media Retention Policy, 19 October 2017, https://privacyinternational.org/sites/default/files/2017-10/PrivacyInternational_DHS_Oct2017_0.pdf

[60] For an overview of the concerns, additional examples and references, see Privacy International, Biometrics: friends or foes to privacy, available at: https://www.privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf

[61] Van den Hoogen, S. (2009), Perceptions of Privacy and the Consequences of Apathy: Biometric Technologies in the 21st Century, Dalhousie Journal of Interdisciplinary Management, Volume 4,

State-imposed requirements for identity can lay the foundations for systematic and extensive human rights violations including discrimination on a mass scale, and in some cases they can prevent access to basic services that guarantee human rights such as voting or receiving welfare benefits.[62] The creation of mass databases of biometric data also raise significant human rights concerns, particularly as this data may be used for different purposes from those for which it was collected, including unlawful surveillance.

- In **India**, the development of India's Unique Identity Scheme (UID), known as Aadhaar, illustrates the worrying trend of idealising biometric technology and its (expected but not proven) capacity as a tool for development. To date, the Aadhaar project has been conducted without a corresponding legislative implementation framework. This means that no protection mechanisms have been put in place to protect the rights of individuals whose information is being collected, or to secure the biometric data itself. The program is currently being challenged before the Indian Supreme Court, which last year recognised the right to privacy as a constitutionally protected right.

Recommendation:

- The High Commissioner should recommend that states should only collect and retain biometric data when they can demonstrate it is necessary and proportionate to achieve a legitimate aim and never in a generalised, indiscriminate matter. States should strictly regulate the collection and retention of biometric data and its use, including limiting authorised access to biometric data to specific actors, based on the purpose for the collection; establishing strict data retention permissions outlining the fixed time period for the destruction of each data set; developing secure physical and digital infrastructure; setting up independent oversight and monitoring mechanisms to ensure accountability and responsibility of those collecting, storing and retaining biometric data; and ensuring rights of redress in the case of errors or unlawful processing.

Spring 2009, pp. 8-9. Available at: www.djim.management.dal.ca/issue_pdfs/Vol4/van_den_Hoogen_S.pdf; Electronic Frontier Foundation, Mandatory National IDs and Biometric Databases, https://www.eff.org/issues/national-ids

[62] Gellman, R., Privacy and Biometric ID Systems: An Approach Using Fair Information Practices for Developing Countries, CGD Policy Paper 028, August 2013, Washington DC: Center for Global Development. Available at: http://www.cgdev.org/sites/default/files/privacy-and-biometric- ID-systems_0.pdf

3.3 Profiling and automated decision making

Another new form of intelligence is that gleaned from the data processed by algorithms, to "identify" and "predict" an individual's behaviour and, ultimately, to make decisions that affect the individual concerned ("profiling" and "automated decision making".)

Widespread availability of data; increased abilities to link data; advances in data processing technology are all contributing to the increasing use of profiling by private and public bodies across a range of sectors, from banking and finance, healthcare, taxation, insurance, marketing and advertising, to justice and policing.

As noted by the European Data Protection Regulators "advances in technology and the capabilities of big data analytics, artificial intelligence and machine learning have made it easier to create profiles and make automated decisions with the potential to significantly impact individuals' rights and freedoms."[63] This echoes the UN Human Rights Council's resolution which stated that "automatic processing of personal data for individual profiling may lead to discrimination or decisions that have the potential to affect the enjoyment of human rights, including economic, social and cultural rights."[64]

Profiling is about recognizing patterns, revealing correlations and making inferences. Through profiling, highly sensitive information can be inferred, derived or predicted from other non-sensitive data. As a result, data about an individual's behaviour can be used to generate previously unknown information about someone's *likely* identity, attributes, behaviour, interests, or personality.[65] This includes information revealing or predicting an individual's likely racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual behaviour or sexual orientation.[66] Because of the

[63] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679.

[64] Human Rights Council resolution on the right to privacy in the digital age, UN doc. A/HRC/RES/34/7.

[65] Publicly accessible data (such as tweets) can be used to infer people's location, which in turn can be used to estimate someone's average income based on one's neighbourhood, average housing cost, debt, and other demographic information, such as political views. See Ilaria Liccardi and others, 'I know where you live: Inferring details of people's lives by visualizing publicly shared location data' (Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems May 2016) *http://people.csail.mit.edu/ilaria/papers/LiccardiCHI2016.pdf*

[66] One study combined Facebook 'likes' with limited survey information and found that researchers accurately predicted a male user's sexual orientation 88% of the time; a user's ethnic origin 95% of the time; and whether a user was Christian or Muslim 82% of the time. See Michael Kosinski, David Stilwell and Thore Graepel. Private traits and attributes are predictable from digital records of

inherently probabilistic nature of profiling, individuals are frequently misidentified, misclassified or misjudged as having certain attributes or characteristics. Some individuals belong to groups of society that are *systematically* misidentified, misclassified, or misjudged.

Profiling is often used for **targeted advertising** which can lead to discrimination: an individual[67] or a segment of the population can be excluded from receiving information or opportunities, or targeted with "negative" advertising, which might reinforce existing social disadvantages.[68]

Profiling is also increasingly used by political parties to identify and target potential supporters. While data-driven campaigning has been deployed for decades, the granularity of data that is available and the complexity of the data processing is something new.[69] The practice of targeting voters with personalised messaging raises concerns about political manipulation and the impact of such profiling on the democratic process. Personalised, targeted political advertising often means that parties operate outside of public scrutiny.[70]

- In **Kenya**, where the risk of political violence during the 2017 election was extremely high, a US digital media company Harris Media created highly inflammatory campaigns against presidential hopeful Raila Odinga. Harris Media uses data analytics to create political campaigns that target audiences using information gleaned from how people use their social media accounts. It is not known how the company used the data in the Kenyan context, and this lack of transparency and accountability is a common concerning feature of profiling for political advertising.[71]

---

human behaviour. Proceedings of the National Academy of Sciences of the United States of America, http://www.pnas.org/content/110/15/5802.full.pdf

[67] Facebook's Ad Targeting options alone allows for a level of granularity, such as the ability to use combinations of behaviours, demographics, and geolocation data to reduce an audience to as little as one person. See Kim, L. (2017). 5 Ridiculously Powerful Facebook Ad Targeting Strategies.

[68] A 2015 study by Carnegie Mellon University researchers found that Google's online advertising system showed an ad for high-income jobs to men much more often than it showed the ad to women. See Datta, A., Tschantz, M. C., & Datta, A. (2015). Automated Experiments on Ad Privacy Settings.

[69] In the **US** the Republican National Committee provides all Republican candidates with free access to a database that includes data on 200 million voters and includes over 7 trillion micro targeting data points. Sensitive information, such as political beliefs, can be revealed from completely unrelated data using profiling.

[70] In **Germany**, the Afd radical party publicly promised to stop sharing offensive posters, yet continued to target specific audiences with the same images online.

[71] For more information, see Privacy International, https://www.privacyinternational.org/feature/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack

Increasingly important decisions are being made automatically (with no meaningful human intervention) based on profiling, ranging from whether to approve loan applications to whether to hire a candidate for a job. These decisions significantly affect individuals' human rights and particular concerns emerge in relation to their discriminatory effects.

- In the **United States**, risk assessment software purporting to predict the likelihood of reoffending has been used to aid sentencing decisions since the early 2000s. A 2016 study by the non-profit news organisation ProPublica revealed this software's bias against African-Americans, who are more likely to be given a higher risk score compared with white offenders charged with similar crimes.[72]

Recommendations:

- The High Commissioner should recognise the significant privacy invasiveness and potential discriminatory effects of profiling.
- The High Commissioner should recognise that the right to privacy gives individuals the right to object to profiling and to control over decisions made by profiling, including providing individuals with access to the data on which such decisions are based, information about the way in which the data is automatically processed and the extent to which decisions will rely on data derived or predicted through profiling.
- Automated decision-making, without meaningful human intervention, should be prohibited, except in cases where the individuals concerned give their explicit and informed consent.
- The High Commissioner should recommend that states adopt comprehensive data protection legislation and establish independent data protection authorities, with powers to investigate reports, receive complaints from individuals and organisations, issue fines and other effective penalties for the unlawful processing of personal data by private and public bodies. Independent authorities, such as data protection authorities, should be in a position to audit automated decisions to test for bias and unlawful discrimination.

[72] Angwin, J., Larson, J., Mattu, S and Kirchner, L., 2016, Machine Bias. *ProPublica*. Available from: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.