NB: this draft content for the Open Government Guide has been developed by Privacy International and is posted for comments. Please attach comments to this document, or as comments on the blogpost, or by email to info@opengovguide.com.

NB: The finalised topic will be integrated into the Open Government Guide as an online Topic at http://www.opengovguide.com

THE GUIDE TO OPENING GOVERNMENT

Draft content on: Privacy and data protection

Introduction

Privacy is an internationally recognised human right, enshrined in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the constitutions of more than 100 countries across the globe. Privacy is not only an important right in itself, but it is a key element of individual autonomy and dignity, and a strong enabler of political, spiritual, religious and even sexual freedoms. It is central to defining the relationship and social interaction between a citizen and their government.

As information technology has made it possible for data to be collected, stored, shared and analysed in previously unimagined ways, the right to privacy has evolved to encapsulate a right to protection of personal data. [1] The concept of data protection implies that individuals have the right to decide whether to share or exchange their personal information and on what terms. Data protection laws generally incorporate safeguards protecting the security of personal data and allowing it to be used by others only in prescribed circumstances.

The rights to privacy and data protection have a bearing for a multitude of government institutions, whether they collect and hold data on citizens, or regulate others. In particular police and public security services have responsibilities which inevitably involve intrusion into the private sphere in pursuit of broader public aims such as the administration of criminal justice and the protection of public safety and national security. The functions of police and security agencies that may implicate privacy issues include search and seizure powers, communications surveillance activities, and the establishment of DNA databases.

Privacy is also a concern in relation to right to information laws, where there are implications for

individuals, and in the establishment of identification and registration databases such as in healthcare or for elections.

Because technologies are so rapidly changing the nature and value of information, and because huge volumes of personal data are being rapidly generated, transmitted, shared and collated, it is essential that governments are transparent about the types and amount of data they collect and the means and modes of surveillance they conduct. There must be strong oversight and accountability mechanisms in place and clear, explicit laws must govern State use of surveillance powers and access to communications data.

Expert organisations

- Privacy International - https://www.privacyinternational.org/
- Open Rights Group - http://www.openrightsgroup.org/
- Electronic Frontiers Foundation - https://www.eff.org/
- European Data Protection Supervisor - https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS
- OECD www.oecd.org/sti/security-privacy
- Global Privacy Enforcement Network https://www.privacyenforcement.net

Overview of Illustrative commitments

Initial steps	• Publish educational material about the importance of protecting personal information • Publish all laws setting out the surveillance powers of law enforcement and intelligence agencies
Intermediate steps	• Enact data protection legislation • Repeal any requirements compelling the identification of phone or internet users
Advanced steps	• Publish transparency reports about access to communications data and surveillance activities • Reform legislation relating to surveillance by state agencies to ensure it complies with the International Principles on the Application of Human Rights to Communications Surveillance
Innovative steps	• Establish a public oversight body responsible for ensuring that all new technologies and techniques adopted by police and public security agencies comport with the right to privacy

(NB: more details of each illustrative commitment - see below)

Initial step: Publish educational material about the importance of protecting personal information

Justification

The first step towards securing the protection of individuals' personal information is educating citizens about the value of that information and the reasons why they should expect that data to be protected. Individuals need to be informed about the nature of digital technologies and the internet, how companies gather and use data, and how governments might be able to gain access to that data. Empowering individuals with respect to personal information is in line with the Organisation for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), which emphasise the participation of individuals in the protection of their own personal data.

Recommendations

1. Publish easy-to-read information about personal information and how it can be paired with other data and analysed in ways that might endanger privacy.
2. Provide individuals with simple steps they can take to protect their personal information, both online and off, to ensure that citizens play a proactive role in the protection of their personal data.

Country examples

The UK Information Commissioner's Office has published a booklet called *Protecting your personal information online* which provides a useful example of the types of material that are helpful - http://www.ico.org.uk/upload/documents/library/data_protection/practical_application/protecting_your_personal_information_online.pdf. Several UK government departments, with private sector partners, have also funded an initiative that provides comprehensive advice about online safety: https://www.getsafeonline.org.

Relevant standards and guidance

European Data Protection Directive, 1995 - http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981 - http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Organisation for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980) - http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Federal Trade Commission, How to keep your personal information secure - http://www.consumer.ftc.gov/articles/0272-how-keep-your-personal-information-secure

Electronic Frontier Foundation's Top 12 Ways to Protect Your Privacy Online - https://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy

Initial step: Publish all laws setting out the surveillance powers of law enforcement and intelligence agencies

Justification

The administration of justice and the protection of national security in democratic countries require a transparent and open legal framework detailing the powers and responsibilities of police and public security agencies, including intelligence agencies. Where law enforcement and intelligence agencies are empowered to conduct surveillance in order to achieve security and policing aims, these powers must be clearly delineated and articulated in a way that enables individuals to foresee their application and scrutinise their use.

A fundamental principle of international human rights law is that infringements of the right to privacy must be necessary, proportionate, and in accordance with the law. The European Court of Human Rights has emphasised that for surveillance to be "in accordance with the law" legislation must detail the following: [2]

- "The nature of the offences which may give rise to surveillance;
- The categories of people liable to be subject to surveillance;
- A limit on the duration of surveillance;
- The procedure to be followed for examining, using and storing the data obtain;
- The precautions to be taken when communicating the data to other parties; and
- The circumstances in which data may or must be erased or the tapes destroyed."

Recommendations

1. Publish all laws and regulations setting out the surveillance powers of law enforcement and intelligence agencies and adopt such laws where these do not exist. These should cover internal regulations and procedures, although internal regulations should, where possible, be legislated to ensure they are subject to sufficient scrutiny.
2. Ensure laws and regulations setting out surveillance powers are sufficiently clear in scope and detail to meet the requirements of foreseeability and accessibility necessitated by the rule of law.
3. Educate citizens about the oversight mechanisms in place that investigate and monitor the compliance of law enforcement and intelligence agencies with the laws and regulations pertaining to surveillance powers. Provide information about means of redress for citizens who believe that agencies have breached legislation relating to surveillance.

Country examples

Relevant standards and guidance

International Principles on the Application of Human Rights to Communications Surveillance - https://necessaryandproportionate.org/take-action/ORG

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on privacy and communication surveillance, April 2013 - http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement

Intermediate step: Enact data protection legislation

Justification

The concept of data protection implies that individuals have the right to decide whether to share their personal information and to determine on what terms they are prepared to do so. Data protection (DP) laws generally incorporate safeguards protecting the security of personal data and allowing others to use it only in prescribed circumstances. More than 100 governments have enacted or are in the process of enacting data protection legislation.[3]

Most DP regimes derive inspiration from the OECD's 1980 Privacy Guidelines. They apply to all personal data, defined as "any information relating to an identified or identifiable individual". The Guidelines are not legally binding but have long been recognised as a statement of norms that should govern personal data privacy and guide OECD members and private organisations in crafting their policies. The Guidelines call for any personal data collected to be relevant and necessary for the purposes for which it is collected, to be obtained lawfully and fairly and to be kept accurate and up-to-date (Part II, Basic Principles). Personal information should be protected by reasonable security safeguards and should not be disclosed or otherwise made available for purposes other than the ones originally specified at the time of collection, except with the consent of the data subject or by the authority of law.

These Guidelines stipulate that the following principles should be adhered to when collecting and processing personal information and data:

- **Collection limitation**: there should be limits to the collection of personal data, and data, which should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the individual;
- **Data quality**: personal data should be relevant to the purposes for which they are used, and should be accurate, complete and kept up-to-date;
- **Purpose specification**: the purposes for which personal data are collected should be specified and any subsequent use must be limited to that specification;
- **Use limitation**: data should not be disclosed, made available or otherwise used for purposes other than those specified except a) with the consent of the individual or b) by the authority of law;
- **Security safeguards**: data should be protected by reasonable security safeguards to protect against lost, destruction, use, modification or disclosure;
- **Openness**: there should be a general policy about openness with respect to personal data
- **Individual participation**: an individual should have the right to find out information about their data and to have incorrect data erased or rectified
- **Accountability**: a data controller is accountable for complying with these measures.

Recommendations

1. Enact data protection legislation regulating the use of personal information by both the private and public sectors.
2. Establish a data protection authority to oversee compliance with data protection legislation and to mediate complaints.
3. Provide educational material to inform citizens and businesses about data protection standards, their application and opportunities for redress when data breaches occur.

Country examples

The Dominican Republic committed to enact the law on personal data protection as part of its Open Government Action Plan
http://www.opengovpartnership.org/country/commitment/enact-law-personal-data-protection

Relevant standards and guidance

European Data Protection Directive, 1995 -
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981 -
http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

Organisation for Economic Co- operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980) -
http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

Intermediate step: Repeal any requirements compelling the identification of phone or internet users

Justification

One of the most important features of the Internet is the ability to anonymously access and impart information, and to communicate securely without having to be identified. Initially, this was possible because there was no “identity layer” built into the Internet. However, in the name of security and law enforcement, States have gradually eradicated opportunities for anonymous communication. In many States, individuals must identify themselves at cybercafés and have their transactions on public computers recorded. Increasingly, identification and registration are also required when buying a SIM card or mobile telephone device, for visiting certain major websites, or for making comments on media sites or blogs.

Restrictions on anonymity facilitate State communications surveillance by making it easier to identify individuals accessing or disseminating prohibited content, making such individuals more vulnerable to other forms of surveillance. Thus restrictions on anonymity dissuade the free expression of information and ideas and can in practice result in people being unable to access

vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities. Furthermore, restrictions on anonymity allow for the collection and compilation of large amounts of data by the private sector, placing a significant burden and responsibility on corporate actors to protect the privacy and security of such data.

Reference: UN General Assembly, 2013, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue

Recommendations

1. Repeal any laws or regulations that require the use of real names or the verification of identity in online fora, social media or other internet spaces.
2. Remove requirements that individuals identify themselves when using cybercafés or public computers.
3. Roll back mandatory SIM registration rules, making SIM registration an optional practice.

Country examples

Relevant standards and guidance

The Mandatory Registration of Prepaid SIM Card Users – A White Paper, November 2013 - http://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, on privacy and communication surveillance, April 2013 - http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/133/03/PDF/G1313303.pdf?OpenElement

Advanced step: Publish transparency reports about access to communications data and surveillance activities

Justification

Transparency around the use of surveillance powers is a crucial means of ensuring that law enforcement and intelligence agencies are kept in check and the privacy of individuals is not

interfered with outside the strict confines of the law. Transparency allows the citizenry to watch over the government, ensure that it is not exceeding its powers, and to know when the balance between protecting security and infringing on human rights has tipped too far in favour of the police and public security forces.

In recent years, numerous internet services and service providers have taken to publishing transparency reports, detailing the numbers of requests they receive from governments for access to individuals' communications data, and the number of requests they get for the removal of information from their services.

Examples include:

- Facebook Global Government Requests Report - https://www.facebook.com/about/government_requests
- Google Transparency Report - http://www.google.com/transparencyreport/
- Microsoft Law Enforcement Requests Report - https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
- Twitter Transparency Report - https://transparency.twitter.com/

Governments should embrace a similar process. By publishing transparency reports detailing the number of requests they make to communications services providers and internet services, and the number of authorisations granted to law enforcement and intelligence services for different types of online or offline surveillance, governments can ensure that its surveillance is scrutinised by the public in a way that ensures accountability.

Recommendations

1. Enact legislation compelling law enforcement and intelligence agencies to publish yearly disaggregated data about the number of requests made and acceded to by the private sector for access to corporate communications data, and the number of requests made to and approved by the courts or other oversight mechanisms for authorization to conduct online or offline surveillance.
2. Ensure transparency reports are published in an easy and accessible way.

Country examples

Relevant standards and guidance

Global Network Initiative Principles - http://www.globalnetworkinitiative.org/principles/index.php

Advanced step: Reform legislation relating to surveillance by state agencies to ensure it complies with the International Principles on the Application of Human Rights to Communications Surveillance

Justification

As technologies that facilitate surveillance of communications advance, and the powers of intelligence agencies expand, there is a failure on the part of governments to ensure that laws and regulations related to communications surveillance adhere to international human rights and adequately protect the rights to privacy and freedom of expression. There needs to be an updated understanding of how international human rights law applies in the current digital environment, particularly in light of the increase in and changes to communications surveillance technologies and techniques.

The International Principles on the Application of Human Rights to Communications Surveillance were developed to provide governments with a framework to evaluate whether current or proposed surveillance laws and practices are consistent with human rights. The Principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology.

Recommendations

1. Thoroughly review all laws and regulations pertaining to the surveillance powers of law enforcement and intelligence agencies to identify where legislation conflicts with or falls short of the standards articulated in the International Principles.
2. Amend legislation to ensure compliance with the International Principles.

Country examples

Relevant standards and guidance

International Principles on the Application of Human Rights to Communications Surveillance - https://necessaryandproportionate.org/take-action/ORG

Innovative step: Establish a public oversight body responsible for ensuring that all new technologies and techniques adopted by police and public security agencies uphold the right to privacy

Justification

In general legislation has not kept pace with the changes in technology, resulting in legal standards which are either non-existent or inadequate to deal with the modern communications surveillance environment. Governments therefore are increasingly seeking to justify the use of new technologies using old legal frameworks, which do not reflect the expanded capabilities of newer technologies. In many countries, this means that vague and broadly conceived legal provisions are used to legitimize and sanction the use of intrusive techniques. Technologies applied and techniques that go far beyond what was originally foreseen by legislation are being applied without explicit laws authorizing them or defining the scope of their use, making it impossible for individuals to foresee – or even know about – their application. At the same time, laws are being adopted to broaden the breadth of national security exceptions, providing for the legitimization of intrusive surveillance techniques without oversight or independent review.

A specially constituted public oversight body with competency to deal with technology and surveillance issues from a human rights perspective could play an important role in ensuring that new technologies adopted by law enforcement and intelligence agencies comply with existing laws and human rights standards.

Reference: UN General Assembly, 2013, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue

Recommendations

1. Adopt legislation constituting a new public oversight body with expertise in law and technology;
2. Delegate to the body responsibility for ensuring that all new surveillance technologies and techniques adopted by law enforcement and intelligence agencies comport with the right to privacy;
3. Ensure the deliberations and decisions of the oversight body are open to the public.

Country examples

Relevant standards and guidance

International Principles on the Application of Human Rights to Communications Surveillance - https://necessaryandproportionate.org/take-action/ORG

---

[1] Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

[2] *Weber and Saravia v Germany,* application no 54934/00, admissibility, 29 June 2006, at [95]

[3] See *Global Tables of Data Privacy Laws and Bills:* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2280875