MULTIMEDIA TRAINING KIT

INTERNET RIGHTS ARE HUMAN RIGHTS: THE RIGHT TO PRIVACY HANDOUT

Developed by: Carly Nyst

About this document

These materials are part of the Multimedia Training Kit (MMTK). The MMTK provides an integrated set of multimedia training materials and resources to support community media, community multimedia centres, telecentres, and other initiatives using information and communications technologies (ICTs) to empower communities and support development work.

This module has been commissioned by the Association for Progressive Communications (APC) and conducted with support from the Swedish International Development Cooperation Agency (Sida).

Copyright information

Module outline

This module looks at the right to privacy in the context of the internet and ICTs. It begins by analysing the right to privacy in international and national legal frameworks, and summarises some of the primary challenges to the protection and promotion of privacy in different cultures and contexts. It then goes on to consider the impact of the internet and ICTs on privacy, taking an in-depth look into questions of implementation and enforcement with regards to access to and use of personal information by governments, corporate entities and third parties. It focuses on the changing nature of the right to privacy and the difficult balance that must be struck between promoting privacy and ensuring the enjoyment of other human rights.

Throughout this module, the following questions will be posed:

1. How do we understand the right to privacy in the context of differing cultures and political contexts?
2. What issues or situations challenge our conceptualisations of the right to privacy, and threaten the promotion of privacy?
3. How have the internet and ICTs changed and challenged the right to privacy?
4. How is the right to privacy threatened by government access to and use of personal information?
5. How is the right to privacy threatened by corporate access to and use of personal information?
6. How is the right to privacy threatened by third party access to and use of personal information?

Introduction to privacy

Defining privacy

In simple terms, the right to privacy is the right to be left alone. Privacy embodies the concept that individuals have the right to determine who has information about them and to control how, when and to what extent that information is communicated. The right to privacy is a fundamental human right. It is an important safeguard of individual autonomy and human dignity, as it allows individuals to make choices about how they live their lives. It is essential to the exercise and enjoyment of other fundamental human rights, particularly those related to freedom of expression and belief.

The right to privacy in international human rights instruments

The right to privacy is articulated in all of the major international and regional human rights instruments:

- **United Nations Declaration of Human Rights (UDHR) 1948, Article 12**: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.
- **International Covenant on Civil and Political Rights (ICCPR) 1966, Article 17**: 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour or reputation. 2. Everyone has the right to the protection of the law against such interference or attacks.
- **European Convention on Human Rights (ECHR) 1950, Article 8** – Right to respect for private and family life: 1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the

economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

The right to privacy is also defined in the Convention on the Rights of the Child 1990 (Article 16), the Charter of Fundamental Rights of the European Union 2000 (Article 7) and the American Convention on Human Rights 1969 (Article 11). The ASEAN Human Rights Declaration, adopted in November 2012, also articulates the right to privacy (Article 21).

An important element of the right to privacy, particularly in relation to the internet, is the right to protection of personal data. While the right to data protection can be inferred from the general right to privacy, some international instruments also stipulate a more specific right to protection of personal data, including:

- **Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1981**
- **Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data 1985**
- **Charter of Fundamental Rights of the European Union 2000, Article 8**

The right to protection of personal data is also referred to or defined in the Asia-Pacific Economic Cooperation (APEC) Privacy Framework 2004, the ASEAN Human Rights Declaration 2012, and European Directives of 1995, 1997 and 2002.

The right to privacy is not an absolute right. There are instances in which the right to privacy can be legitimately limited by the state in order to ensure the protection or enjoyment of other fundamental human rights. However, interferences with the enjoyment of the right to privacy must only occur under prescribed circumstances. For an interference with the right to be permissible under human rights law, it must meet the following requirements:

1. It must be **in accordance with the law**: This means that the limitation must have a legal basis, that the law in question is precise, and that there are safeguards in place to protect against the arbitrary application of the law.
2. It must **pursue a legitimate aim**: Such legitimate aims are akin to those elucidated in Article 8(2) of the European Convention on Human Rights, such as the interests of national security or the prevention of disorder and crime.
3. It must be **necessary in a democratic society**: This means that the limitation must respond to a pressing social need and that it must be proportionate to the legitimate aim pursued.

Although these requirements are not explicitly articulated in the UDHR and ICCPR, they can be found in the ECHR definition and have been consistently applied by the European Court of Human Rights (see, for example, Olsson v. Sweden (No. 1), ECtHR, Application No. 10465/83, Judgement of 24 March 1988). In his 2009 report on protecting the right to privacy while countering terrorism, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, confirmed that the permissible limitations test applies when interpreting of the right to privacy under the UDHR and ICCPR (A/HRC/13/37).

Implementation of privacy rights in national laws

At the national level, the right to privacy finds relevance in numerous legislative and regulatory instruments. In order to ensure that privacy is comprehensively protected in domestic legal regimes, legislation is required that ensures different types of privacy – including that relating to communications, information and personal data, and physical privacy – across a range of different sectors, such as information technology and communication, banking and finance, health, criminal justice and law enforcement, and immigration.

Although the types of legislative and regulatory instruments used to protect and effect privacy differ considerably between countries and regions, examples of the kind of instruments that might constitute the privacy framework of a given country include:

- A **constitutional provision** establishing an explicit right to privacy, or constitutional jurisprudence establishing an inferred right to privacy.
- A clause in a **bill of rights or national human rights act** establishing a right to privacy, or national jurisprudence establishing an inferred right to privacy.
- **Data protection legislation** stipulating how an individual's personal data may be used, stored and transferred, and establishing a regulatory authority, such as a commissioner.
- **Freedom of information legislation** articulating how information may be controlled and made public, and establishing a regulatory authority, such as a commissioner.
- **Law enforcement and national security legislation**, including criminal procedure codes or legislation, anti-terrorism legislation, cybercrime legislation, and other legislative instruments which regulate the ability of law enforcement authorities to conduct searches and intercept and monitor communications.
- Legislation regulating the **intelligence services**, establishing the authority of intelligence services to conduct searches and intercept and monitor communications.
- **Information and communications legislation**, governing the collection of communications information, including traffic data and content, stipulating the circumstances under which information can be accessed by relevant authorities, and governing the roles and responsibilities of communications service providers.
- **Legislation, regulations or codes of practice governing**
  - The use of CCTV cameras
  - The operation of cyber cafes
  - The establishment of national identification systems, including DNA databases, national biometric systems and ID card systems
  - Workplace monitoring and surveillance.
- **Financial and banking legislation**
- **Health services legislation**
- **Trade practices and consumer legislation**
- **Legislation or regulations relating to e-governance and data sharing practices.**

Privacy across cultures and contexts

Although the ways in which the right to privacy is articulated and protected differ greatly between countries, almost every country has some form of privacy law incorporated into its domestic legal regime. Explicit constitutional rights to privacy can be found in at least 45 national constitutions, including in countries as diverse as Bulgaria and Burundi, Chile and Croatia, and implied privacy rights have been established in many more constitutions. The adoption of data protection legislation is an increasingly critical element of international trade and business arrangements, particularly as European Union regulations prohibit outsourcing by European corporations and governments to countries without data protection legislation. Equally, growing recognition of cross-border communications and cyber security issues has lead to the adoption of related legislation in many countries.

However, one of the most persistent criticisms faced by privacy advocates is that the right to privacy is a Western construct, valued by individualistic cultures but irrelevant to more collectivist cultures. Critics argue that the right to privacy developed as part of the Western liberal tradition, and finds no salience in Asian cultures.[1] The right to privacy is also critiqued from a feminist perspective, which in some cases views privacy as dangerous as it encourages the non-intervention of the state, perpetuating the subjugation of women in the domestic sphere.[2]

[1] See, for example, Julie E. Cohen, *Configuring the Networked Self: Law, Code and the Play of Everyday Practice,* Yale University Press, 2012.

As with other cultural relativist debates in human rights discourse, such critiques often neglect to take into account the complex process of cultural and societal change and development that has occurred across Asia in the last 50 years. Moreover, they oversimplify a complex issue. For example, in Thailand, privacy awareness is high vis-à-vis voter privacy, police intrusion and physical privacy, but low with regards to consumer protection. On the other hand, in Bangladesh there is a strong interest in consumer privacy issues. Studies from China show increasing interest in privacy issues, particularly as they relate to data protection.

A scan of legislative frameworks and local jurisprudence from across Asia supports a conclusion that privacy is relevant and important to Asian societies. Nevertheless, it is clear that conceptualisations of privacy are bound to vary across cultures and places, just as they differ across historical periods. The challenge is to look beyond simplistic cultural arguments to try to understand how privacy is conceived of and exhibited within local, cultural and temporal contexts. Despite being articulated in international human rights instruments, privacy cannot be understood independently from society.

Challenges to privacy

The realisation of the right to privacy faces challenges from every angle. New security threats and realities, changing societal attitudes towards identity and relationships, rapid technological advancements, privatisation and modernisation, and the challenges of delivering public services to growing populations all give rise to challenges and create conditions which put privacy at risk. Some of the more pressing challenges to privacy are detailed below.

Data protection

One of the chief challenges to privacy is the protection of personal data and information. Today massive amounts of data are being generated about individuals by a variety of sources at unprecedented speeds and frequencies. Because of innovations in technology, data are important not only to the individual to whom they pertain, but can be used for a variety of different purposes. For example, companies are able to analyse online data for commercial purposes such as deriving trends and patterns, tracking behaviour, and analysing customer preferences. Governments can compile and analyse data provided to government agencies in order to have better knowledge – and control – of their citizens.

There are many ways in which an individual's privacy, and their enjoyment of other human rights, might be infringed in relation to the use of their personal data. If data are inadequately stored or handled, they are vulnerable to theft or fraudulent alteration. If information provided by an individual on a confidential basis to a company or to the government is shared, lost or inaccurate, that individual could experience discrimination when, for example, applying for a job or taking out a loan, or could be subject to more serious forms of financial fraud. When information is retained for long periods of time it can be collated together with other forms of information to create whole profiles of an individual's communications, movements, activities and purchases. These profiles may be used by corporations for decisions about advertising or pricing. If an individual becomes subject to legal proceedings, such information may be used against them.

Identity issues

Identification systems, including ID cards and biometric and DNA databases, are increasingly being adopted by governments as a means of keeping track of citizens and improving the delivery of public services, increasing the effectiveness of law enforcement efforts, and managing migration. ID systems challenge the right to privacy in that they involve the collation and aggregation of large amounts of information that subsequently becomes representative of

[2] See, for example, Catherine MacKinnon, *Toward a Feminist Theory of the State*, Harvard University Press, 1989.

an individual, without any guarantee of the veracity of that information. On the basis of the information connected with ID cards, serious decisions can be made about an individual that may imperil their enjoyment of other human rights. ID cards often record sensitive information such as an individual's ethnicity or religion that could be used for discriminatory purposes. ID cards are also vulnerable to fraud or duplication. When biometric or DNA information is tied to identification systems, further risks arise. Biometric data are often unreliable and their use can thus have exclusionary impacts. DNA data are extremely sensitive and in the absence of strong safeguards are vulnerable to theft and misuse.

The aggregation of large amounts of biometric, DNA and identity information in centralised databases is particularly worrying from a human rights perspective. Such databases constitute an incredibly valuable resource and are difficult to secure against theft or fraud. As a result, the information contained therein is at risk of being stolen, fraudulently changed, misused or misapplied, to the detriment of the individual in question.

Surveillance

Surveillance is a serious and growing challenge to privacy. Both communications surveillance – including surveillance of online activity and interception of telephone communications – and physical surveillance are popular means of countering crime, disorder and terrorism, as well as pursuing other national security aims. There has been a global proliferation of CCTV cameras; in Britain alone, there are an estimated 300,000.[3] The capacity and quality of cameras continues to improve, as the extent of their usage continues to increase – in many cities they are now used in private as well as public places, in addition to in phone booths, vending machines, buses, trains, taxis, alongside motorways and inside ATMs. CCTV capabilities are now an essential part of crime detection and control strategies across the world. They are also increasingly employed in workplaces as part of a broader move towards workplace surveillance.

Communications surveillance is also an increasingly popular means of detecting and prosecuting crimes. Spurred by national security issues, particularly terrorism, over the past decade laws have become gradually more permissive and communications surveillance practices more indiscriminate and invasive. As individuals live their lives increasingly online, governments have acquired improved abilities and technologies to monitor and intercept online activity.

Although surveillance has a lawful purpose when it is used in appropriate instances for law enforcement activities, in many countries it is also used more widely as a mechanism of control and a means of suppressing dissent. Governments now have access to technologies which can facilitate countrywide mass interception and monitoring of communications, allowing for scanning for voices and key words, location of individuals, and behavioural profiling. Technologies possessed by some countries even enable governments to intercept and delete or amend emails, to listen in to Skype calls, and to remotely turn on microphones and cameras on laptops or smartphones. Such technologies are freely sold and marketed as effective means of tracking human rights defenders, political dissidents and activist organisations.

Vulnerable groups

Challenges to the right to privacy disproportionately affect some groups that are historically marginalised, and often persecuted, by government policies. Such groups include women, children, individuals subject to oppression on the basis of their political affiliation or membership of an ethnic or sexual minority, and people living with HIV/AIDs. Surveillance particularly disadvantages women, whose voices are already silenced and marginalised by structural discrimination and traditional patriarchal attitudes. Data protection violations, particularly when they relate to the provision of public services such as health care, are of far

[3] See Privacy International, "CCTV frequently asked questions", available at www.privacyinternational.org/blog/cctv-frequently-asked-questions.

greater consequence to women, whose identity, choices and decisions regarding their sexual and reproductive rights are often under attack from political and religious forces. People living with HIV/AIDs also experience heightened risks of privacy violations when they interact with government services, which often fail to treat their health status with the confidentiality it deserves.

The impact of the internet and ICTs on privacy

It is clear that how we understand and exercise our right to privacy has changed drastically with the advent of the internet and ICTs. Whereas the internet and ICTs have played a transformative and positive role in relation to a number of human rights, particularly the freedom of expression and information, they have also increased the threats and risks to the enjoyment of privacy. The internet (and the processes of technological innovation and digitisation that have developed alongside it) has resulted in the proliferation of personal information about individuals and the expansion of mechanisms for communications surveillance. ICTs generate information and records not only about an individual's communications, but about their location, browsing behaviour and purchases. Technological advancements have outpaced changes to laws and regulations, and as a result much of the personal information and data generated through the internet and ICTs remain unprotected and thus vulnerable to exploitation, with serious implications for the right to privacy.

Perspectives on the impact of the internet and ICTs on the right to privacy have differed over time and across various communities. During the early years of the internet and new media, and up until the late 1990s, some argued that modern technologies perhaps allowed too much privacy.[4] Technology and, particularly, the use of cryptography were seen as preventing effective law enforcement. In the early 2000s, heightened national security fears fuelled a discourse in which privacy was seen as an inhibiter of security.[5] During this time, the law enforcement approach to ICTs shifted: they became an enabler of greater surveillance, facilitating new forms of profiling and tracking. This balance between security and privacy continues to be an overriding feature of the discourse around the internet and human rights.

Similarly, whereas privacy rights advocates were initially at the forefront of adapting to the internet and supporting technological advancements, in recent years they have often been cast as anti-innovation when calling for constraints and rules with respect to privacy online. This shift has also revealed the differences in perspectives within the human rights community, which as a whole views the internet and ICTs as essential, transformative tools that support the promotion and protection of all human rights. At the same time, initiatives such as APC's Internet Rights Charter, which places the right to privacy amongst other internet-related human rights, seek to transcend these differences.

New challenges continue to arise which undermine our previous understandings of the right to privacy: from changing attitudes towards sharing information online, to new technologies which facilitate previously unimagined surveillance and tracking. Anonymity is an essential element of freedom of expression online, and yet it prevents the application of traditional defamation laws and may threaten the right to privacy and protection of reputation. The provision of information online can enhance an individual's browsing experience and improve efficiency, all the while placing them at risk of privacy breaches.

It is clear that traditional conceptualisations of privacy continue to change as the internet and ICTs become more entrenched in individuals' lives.[6] Equally, understandings of the nature of human rights obligations are also undergoing a transformation. Private sector companies rather than governments are the primary collectors and users of personal information and

[4] See, for example, Amitai Etzioni, *The Limits of Privacy,* Basic Books, 1999.

[5] See, for example, Richard Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency*, Oxford University Press, 2006.

[6] David Souter for APC, "Human Rights and the Internet: A review of perceptions in human rights organisations", 2012, available at www.apc.org/en/system/files/HumanRightsAndTheInternet_20120627.pdf

data, and yet they are not traditionally subject to the human rights obligations that are imposed on governments. In this context, initiatives such as Google's Transparency Report are an important step towards addressing issues of corporate accountability and transparency in the context of privacy and the internet.

Attitudes towards privacy, the internet and ICTs are also changing. As the reality of government surveillance of individuals and corporate exploitation of personal data becomes more evident, individuals are increasingly taking measures to protect their information online. Growing outrage at approaches to privacy by social networking sites like Facebook and Instagram[7] is evidence of increased awareness of the importance of privacy online. Privacy "scandals" have been effective in increasing attention for privacy issues and catalysing legal and regulatory changes. Examples of such events include the sale by Octopus Rewards – Hong Kong's digitised public transportation payment system – of the personal data of 1.97 million registered users,[8] and a data leak by South Korean online game company Nexcon which saw the publication of the personal information of 13.2 million people.[9]

People are becoming more aware of the risks to their privacy and more able to make informed decisions about the way they use the internet and ICTs. Yet tensions between the right to privacy and other human rights remain. The proliferation of ICTs, particularly in Africa, is enabling greater connectivity, facilitating the flow of information, and engaging and empowering communities. Yet it also raises serious privacy concerns – devices are vulnerable to theft and are easily hacked – and can have discriminatory impacts, excluding the poorest and most marginalised groups.[10] Similarly, increased privacy protections such as encryption tools, passwords and encrypted sites are an important means of protecting privacy online, yet they may also thwart law enforcement efforts to advance security. These issues lie at the heart of the discourse around privacy, the internet and human rights.

The implementation, enforcement, enjoyment and violation of the right to privacy

Government use of and access to personal information

The right to privacy is an essential component of the social contract; it mediates the division of power between the individual and the government. As both individuals and governments integrate the internet into their lives and activities, that division of power is unsettled. With increasing frequency, governments are adopting legislation and regulations to enable them to access information online, monitor an individual's internet activities, and compel communication service providers to hand over information about internet users. Intelligence services often have wide powers to intercept and record communications, and law enforcement authorities regularly approach online service providers such as Google and Facebook for access to records and emails. They have the capability to amass information derived from numerous sources or provided to multiple government departments in order to create comprehensive profiles of individuals. In some countries, governments have also acquired technology that would facilitate extralegal surveillance, such as mass interception of communications. As a result, the balance of power is increasingly tipped in favour of the government when it comes to the protection of privacy.

[7] Most recently, Instagram's decision to alter its privacy policy to allow advertisers to use the photos and data of its users was met with strong criticism, forcing a reversal of the decision. See Duncan Robinson, "Instagram sparks backlash over privacy", *Financial Times,* 18 December 2012, available at www.ft.com/cms/s/0/6ed97d8e-4938-11e2-b25b-00144feab49a.html#axzz2H4Z28dZq

[8] Privacy International, "A New Dawn: Privacy in Asia", December 2012, available at www.privacyinternational.org/reports/a-new-dawn-privacy-in-asia

[9] James Delahunty, "South Korean data leak affects 13 million gamers", *After Dawn*, 27 November 2011, available at www.afterdawn.com/news/article.cfm/2011/11/28/south_korean_data_leak_affects_13_million_gamers

[10] Russell Southwood for APC*, Policy and regulatory issues in the mobile internet*, 2011, available at www.apc.org/en/pubs/issue/policy-and-regulatory-issues-mobile-internet

The collection of information is a core element of government control over its citizens.[11] Citizens' personal data are used by governments for a number of purposes:

- **Governance and the delivery of public services**: Accurate population information can help governments identify where public services need to be delivered and to whom, and can inform budgetary allocations and other governance decisions. Governments use the internet to facilitate the provision of services such as social security provision, school enrolments, the sharing of medical records and online income tax return filing, and can utilise the data provided in online systems to gain a fuller picture of a country's citizenry and improve their delivery of services accordingly.
- **Law enforcement**: Governments can use individuals' personal information for law enforcement purposes. By following procedures set down in national legislation to access online communications and activities, governments can get access to emails, financial transactions, social networking sites and other online activities in order to detect or prosecute crimes. Information retained in government databases about an individual's identity can be matched with geo-location information obtained from ICTs and with CCTV footage in order to create a comprehensive profile of an offender.
- **Identity management and social sorting**: Through the use of ID cards and biometric systems, governments can create profiles of citizens which can be used for a number of purposes. Identity management can be used to track the movement of the population and their activities across a range of different areas, from where individuals travel to where they eat, whether they attend an internet café and what sites they visit there, where they study and where they work. ID systems can also be used for more intrusive purposes: with information about an individual's ethnicity and religion, and with biometric and DNA information, governments have the capacity to isolate and discriminate against selected sectors of society. Ethnic and sexual minorities, migrants and homeless persons may be particularly vulnerable in this regard.
- **Surveillance of communications and behaviour**: Governments have the technological capabilities to monitor online communications and activities on social networking sites such as Facebook and Twitter. The legality of communications surveillance and behaviour varies from country to country. In some countries, legislation delegates wide powers to law enforcement agencies to intercept and monitor communications without scrutiny or judicial oversight. In others, law enforcement authorities have to obtain a warrant or subpoena in order to access individual communications. Given that legislative changes have fallen behind technological ones, in some cases online monitoring by law enforcement is regulated only by internal policies and guidelines. As a result, police and other government authorities have wide discretion in choosing who to surveil, and how. Information provided by individuals freely online can be mined to derive political or social preferences and can be tracked to identify illicit behaviour. When this information is paired with CCTV footage and other personal information held by governments, the result is a comprehensive profile of an individual's movements and behaviours.

An important safeguard to ensure that the data collected by government are accorded the highest degrees of privacy and confidentiality is data protection legislation. While such legislation differs between countries, the generally agreed international standard is that laid out in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Part Two). 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, 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.

[11] Some argue that the state would not be able to even exist without basic information about its citizens: James C. Scott, *Seeing Like A State*, Yale University Press, 1998.

- **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.

Although the OECD Guidelines do not explicitly address data retention, privacy advocates support a position whereby data are not retained any longer than is strictly necessary for the completion of the purpose for which they were obtained. Controversially, the EU Data Retention Directive, adopted in 2006, requires communications providers to retain certain categories of information for between six months and two years, and to make information available on request to law enforcement authorities. Data retention is increasingly being incorporated into legislative frameworks across the globe under the guise of improving the effectiveness of law enforcement efforts.

Corporate use and access to personal information

The sale and trade of data is big business these days. Individuals' personal information is extremely valuable to the private sector, which can generate profit from data via the following methods and mechanisms:

- **Behavioural advertising and profiling**: The delivery of advertisements to internet users on the basis of their previous activities. This occurs in single services, such as on Amazon and Facebook, which keep records of your previous activities and market to you based on these records. It also occurs across different websites through the use of cookies, which identify users to a third party advertising network that keeps a profile of the user's interests based on the websites they visit. An individual's personal information is thus shared with third parties without their consent, and that information becomes a valuable resource to corporate entities wishing to attract customers. In fact, the business models of most major online service providers, including Google and Facebook, are built around maximising advertising revenue through such techniques.
- **Data mining**: This process involves extracting information or patterns from a set of data. Data mining can help a company understand its customers and more appropriately market certain products to certain individuals. It can be used in the fields of science and engineering, educational research and medical research, for example, to detect patterns in electronic health records. Data mining is also used by the United States government under the Analysis, Dissemination, Visualisation, Insight and Semantic Enhancement (ADVISE) programme that analyses huge amounts of data, from blogs and emails to government records and intelligence reports, to search for patterns of terrorist activities.[12]
- **Big data**: While data mining can be conducted on manageable datasets, the rate of production of information and data is now so great that datasets are being created which are too large and complex to be processed using traditional database management tools. An analysis of big datasets can reveal more information than smaller datasets, and as such represents enormous value to the private sector, scientific research, and governance. In 2012, the Obama administration announced the establishment of the Big Data Research and Development initiative, to explore how big data could be used to address governance issues. Analysis of big data holds particular promise for the medical research field.

[12] Mark Clayton, "US plans massive data sweep", *The Christian Science Monitor*, 9 February 2006, available at www.csmonitor.com/2006/0209/p01s02-uspo.html

The legal issues raised by corporate use of personal information are complex. The private sector is subject to a number of different legal frameworks in this regard:

- **Terms of service/user agreements**: These stipulate what a company can and cannot do with its users' information, and act as an enforceable contract between the provider and the user. However, lengthy and complicated terms of service are rarely read by users, and in effect permit companies to use personal information in a variety of different ways.
- **Data protection**: In an increasing number of countries the private sector is subject to the same data protection requirements as the public sector. However, data protection legislation remains absent in many countries, including most of Africa. In this regard it is important to note that there is no international data protection regime, and as such, when conducting online activities it is possible that an individual's personal information will be provided to a corporate entity registered in a non-data protection country.
- **Government access to corporate data**: Governments regularly seek access to data held by corporations, particularly the major online service providers. For example, from January to June 2012, Google received more than 20,000 requests from foreign authorities seeking access to users' email accounts or internet searches.[13] In most countries, domestic legislation stipulates a process with which law enforcement must comply in order to get access to an individual's emails or intercept their phone calls, usually requiring a judicial order. In practice, however, law enforcement authorities regularly approach corporate entities directly and simply request user data. Some companies hand over user information without requiring the production of a warrant or subpoena. This occurs not only within a country but between governments and foreign corporate entities. Corporate entities do not always hand over information; in many cases authorities are forced to pursue a formal application through the Mutual Legal Assistance Treaties (MLAT) process. However, often user data are handed over informally, particularly where a pressing need is demonstrated.

Use of and access to personal information by other individuals and third parties

Personal information and data are also vulnerable to other forms of abuse or misuse, such as online fraud, hacking, the use of fraudulent solicitations, the distribution of fraudulent security software, or identity theft and fraudulent misrepresentation. Each of these situations represents a serious infringement upon an individual's right to privacy. Many of these actions fall within the scope of computer misuse or cybercrime legislation, which varies greatly between countries. Moreover, the types and scope of online attacks continue to grow, making it difficult for law enforcement authorities to respond adequately. Examples include the "human flesh search engine" in China[14] and "revenge porn" websites.[15]

The right to privacy is also at risk when the media access and publish private information. The difficult balance between freedom of expression and the right to privacy is in sharp relief when considering the role of the media and questions of defamation and reputation. Again, there is no international consensus on the responsibility of the media to respect the right to privacy, and courts and legislatures in countries across the globe continue to struggle with this question. The 2012 UNESCO Global Survey on Internet Privacy and Freedom of Expression summarises the different national positions and gives recommendations about how to resolve this difficult balance.[16]

---

[13] See the Google Transparency Report: www.google.com/transparencyreport/userdatarequests

[14] A form of online vigilante justice where users hunt down and punish individuals with the help of the online community. See Tom Downey, "China's Cyberposse", *The New York Times*, 3 March 2010, available at www.nytimes.com/2010/03/07/magazine/07Human-t.html?pagewanted=all&_r=0

[15] Where naked photos are posted of an individual online without their consent as a form of revenge. See Joe Mullin, "Lawsuit against 'revenge porn' site also targets GoDaddy", *Wired*, 23 January 2013, available at www.wired.co.uk/news/archive/2013-01/22/revenge-porn

[16] Toby Mendell, Andrew Puddephatt, Ben Wagner, Dixie Hawtin and Natalia Torres, *Global Survey on Internet Privacy and Freedom of Expression,* UNESCO, 2013, available at

As more and more media move online, and the publications of bloggers and Twitter users are elevated alongside traditional forms of media, the question of defamation becomes even more complex. Questions of place of publication and jurisdiction compound the issue, as do online anonymity and the use of pseudonyms. Identity policies online form one of the major ongoing privacy battles. Whereas anonymity has been the norm since the inception of the internet, increasingly fears of cybercrime, cyber bullying and trolling, concerns about paedophilia and grooming, and terrorist fears have supported a drive towards requiring real-name registration and traceability of internet users.

Summary

The internet and ICTs have posed new and difficult challenges to understandings of the right to privacy in the modern era. Ensuring the protection of personal data is a particular challenge, especially as changes in technology continue to outpace legislative reform. In the absence of effective data protection, individuals face having their personal information accessed and exploited by both corporations and governments.

A second overarching concern is the expansion of surveillance technologies and techniques. Surveillance and interception of communications by law enforcement authorities are becoming more and more widespread. Such practices not only persistently violate the right to privacy, but also threaten the enjoyment of other rights and freedoms, including freedom of expression, association and movement.

Privacy must be understood in the context of changing societal norms and attitudes, and as the internet grows and changes, so too will the content and confines of the rights to privacy. However, the core of the right to privacy is an important element of a liberal, democratic society, and must remain protected. To this end, it is vital that the human rights community work to understand the risks to privacy posed by the internet and ICTs, and incorporate those understandings into its advocacy work going forward.