UNESCO Publishing

United Nations
Educational, Scientific and
Cultural Organization

Global Survey on INTERNET PRIVACY AND FREEDOM OF EXPRESSION

Toby Mendel • Andrew Puddephatt • Ben Wagner • Dixie Hawtin • Natalia Torres

UNESCO SERIES ON INTERNET FREEDOM

Global Survey on INTERNET PRIVACY AND FREEDOM OF EXPRESSION

Toby Mendel • Andrew Puddephatt • Ben Wagner • Dixie Hawtin • Natalia Torres

UNESCO SERIES ON INTERNET FREEDOM

Authors

- Andrew Puddephatt, Director, Global Partners & Associates
- Toby Mendel, Executive Director, Centre for Law and Democracy
- Ben Wagner, Researcher, European University Institute
- Dixie Hawtin, Project Manager, Global Partners & Associates
- Natalia Torres, Researcher, Center for Studies on Freedom of Expression and Access to Information (CELE) of the University of Palermo, Argentina

With special thanks to the following who kindly agreed to be interviewed for this publication:

Guo Liang, Yang Wang, Ceren Unal, Ang Peng Hwa, Erick Iriarte Ahon, Katitza Rodriguez, Karen Reilly, Ali G. Ravi, Moez Chackchouk, Primavera de Filippi, Peter Parycek, Robert Bodle, Sameer Padania, Peter Bradwell, Ulrike Höppner, Eduardo Bertoni, Hong Xue, Monique Fanjoy, Abu Bakar Munir, Joe McNamee, Amr Gharbeia, Jamie Horsley, Nepomuceno Malaluan, Cynthia M. Wong, Sinfah Tunsarawuth, Prim Ot van Daalen, Sunil Abraham, and a number of anonymous former employees of large technology companies.

Published in 2012 by
the United Nations Educational,
Scientific and Cultural Organization
7, place de Fontenoy, 75352 Paris 07 SP, France

ISBN 978-92-3-104241-6

Typeset and printed by UNESCO

This publication was first printed thanks to the contribution of the Swedish International Development Cooperation Agency (Sida)

Printed in France

CONTENTS

FOREWORD

UNESCO, as enshrined in its Constitution, promotes the "free flow of ideas by word and image", and has committed itself to enabling a free, open and accessible Internet space as part of promoting comprehensive freedom of expression online and offline.

As demonstrated by UNESCO's 2011 publication *Freedom of Expression: Freedom of Connection, the Changing Legal and Regulatory Ecology Shaping the Internet*, freedom is not the inevitable by-product of technical change, and it must be safeguarded by appropriate legal and regulatory measures. At a time of rapid change, we are fully aware that freedom of expression on Internet is complex, and that this means working to find a balance between this right and other, sometimes conflicting, imperatives – such as national security, protection of authors' rights, and respect for privacy.

UNESCO approaches these issues within the framework of the follow-up process to the World Summit of Information Society and our activities in relation to the Internet Governance Forum.

We know well that we now live in a world with two billion Internet users and five billion mobile phone users, who are posting millions of public blogs, tweets, images, podcasts, as well as their personal information on daily basis.

In this context, UNESCO has recognised that privacy, as a fundamental right, impacts on other rights and freedoms, including freedom of expression, association and belief. The challenge is that mechanisms to protect online privacy can sometimes be used to infringe legitimate freedom of expression in general and the democratic roles of journalism in particular. An additional challenge in balancing these rights on the Internet lies in the discrepancy of the legal frameworks between online and off-line territories, as well as national and international jurisdictions.

With all this in mind, this publication seeks to identify the relationship between freedom of expression and Internet privacy, assessing where they support or compete with each other in different circumstances. The publication maps out the issues in the current regulatory landscape of Internet privacy from the viewpoint of freedom of expression. It provides an overview of legal protection, self-regulatory guidelines, normative challenges, and case studies relating to the topic.

Providing up-to-date and sharp information on emerging issues relevant to both developed and developing countries, we hope that this publication will provide UNESCO Member States and other stakeholders, national and international, with a useful reference tool. Multiple stakeholders, preferably in dialogue, can use this publication in their own spheres of operation, adapting where appropriate from the range of experiences as recorded in these pages. The publication also supplies additional sources of reference for interested readers to use to further investigate each of the subjects highlighted.

It is our wish that this publication will contribute to bringing stakeholders together for informed debate on approaches that are conducive to privacy protection without compromising freedom of expression. In the coming years, UNESCO will specifically

seek to disseminate information about good practices and international collaboration concerning the points of intersection between freedom of expression and privacy. Research on safeguarding the principle of freedom of expression in Internet policy across a range of issues will continue to be part of UNESCO's normative mandate and technical advice to stakeholders.

Jānis Kārkliņš
Assistant Director-General
for Communication and Information
UNESCO

EXECUTIVE SUMMARY

Privacy is a fundamental right, even though it is difficult to define exactly what that right entails. Privacy can be regarded as having a dual aspect – it is concerned with what information or side of our lives we can keep private; and also with the ways in which third parties deal with the information that they hold – whether it is safeguarded, shared, who has access and under what conditions.

Understandings of privacy have long been shaped by the technologies available, with early concerns about privacy surfacing with newspapers in the nineteenth century. So the Internet, in turn, inevitably reshapes what we understand privacy to be in the modern world.

The right to privacy underpins other rights and freedoms, including freedom of expression, association and belief. The ability to communicate anonymously without governments knowing our identity, for instance, has historically played an important role in safeguarding free expression and strengthening political accountability, with people more likely to speak out on issues of public interest if they can do so without fear of reprisal. At the same time, the right to privacy can also compete with the right to freedom of expression, and in practice a balance between these rights is called for. Striking this balance is a delicate task, and not one that can easily be anticipated in advance. For this reason it has long been a concern of the courts to manage this relationship.

The Internet presents significant new challenges for protecting the right to privacy. In broad terms, the Internet:

- Enables the collection of new types of personal information – technological advances have resulted in tools for collecting and understanding types of information which in the past would have been impossible or unfeasible.
- Facilitates the collection and location of personal information – each computer, mobile phone or other device attached to the Internet has a unique IP address, which provides unique identifier for every device and which means in turn that they can be traced. The ability to locate any device creates significant new privacy challenges.
- Creates new capacities for government and private actors to analyse personal information. Increased computing power means that vast quantities of information, once collected, can be cheaply and efficiently stored, consolidated and analysed. Technological advances allow databases of information to be connected together allowing even greater quantities of data to be processed.
- Creates new opportunities for commercial use of personal data. Many of the services provided by these companies are free and their business models rely on collecting user information and using it for marketing purposes.
- Creates new challenges for regulation given the transnational nature of the Internet. Despite the emergence of international best practice standards for data protection, there is still much progress to be made towards the harmonisation of national laws. Online companies still find it hard to navigate the complex patchwork of national

privacy laws when operating international Internet services that span national boundaries, with legal ambiguity undermining privacy protection.

A range of threats to privacy which have developed through the Internet are considered in more detail in Section 2 of the paper. The following issues are explored:

(1) The opportunities and challenges for maintaining control over personal data online.

(2) A range of initiatives to protect privacy and anonymity online.

(3) The roles and responsibilities of service providers and intermediaries.

(4) The specific challenges posed by different applications, communications platforms and business models including cloud computing, search engines, social networks and other different devices.

(5) The problems posed by e-government and other government approaches.

(6) The threats posed by different mechanisms of surveillance and data collection including: Unique Identifiers; Cookies (and other associated forms of user identification); Adware; Spyware and Malware conduct covert data logging and surveillance; Deep packet inspection (DPI); and data processing and facial recognition and surveillance technology.

International legal standards on privacy, and responses to these emerging issues, are explored in Section 3. The section sets out the explicit understandings and protections for the right to privacy under international human rights law. The section then analyses key legislation and regulatory frameworks that impact on the protection of privacy rights online at the regional and national level in countries across the world; and furthermore analyses the strengths and weaknesses of self-regulation as a privacy protection tool – whether it be used as a central mechanism, or supplementary to legal protections.

The rights to privacy and freedom of expression relate to each other in complex ways – Section 4 explores these intersections in greater detail. In some ways privacy is a necessary precondition for freedom of expression – this is especially true in countries where it may be dangerous to discuss certain issues (such as politics, religion or sexuality) openly. However there are also significant tensions between the two rights, for example where a newspaper wishes to publish private details about a leading politician, perhaps because the newspaper believes this is in the public interest. These tensions have come into far greater prominence with the massive changes in freedom of expression brought about by the Internet and other digital communications systems.

The paper explores international law and the practice of other States, in terms of respecting privacy on the Internet, taking into account potential conflicts with other rights, in particular freedom of expression. Section 5 contains our recommendations to states and corporations for better practice based on our research and consultations. The recommendations cover: legal and regulatory measures (constitutional measures, civil law protection, criminal law protection, data protection systems), corporate policy and practice and awareness raising.

Finally, Section 6 provides an overview of literature, background material and tools on international and national policy and practice on privacy and freedom of expression on the Internet. This section is intended as a resource for readers who wish to access further instruments, tools and information.

1. INTRODUCTION

The need for privacy is deep-rooted in human beings. In its essential form, privacy is based on the notion of personal integrity and dignity. However, this is also hard to define with any agreed precision – in different contexts it embraces the right to freedom of thought and conscience, the right to be alone, the right to control one's own body, the right to protect your reputation, the right to a family life, the right to a sexuality of your own definition. In addition these meanings vary from context to context. Despite its ubiquity there is no one definition of privacy that is universally understood in the same way. Privacy in the modern world has two dimensions – firstly, issues to do with the identity of a person and secondly, the way their personal information is handled.

Understandings of privacy have long been shaped by available technologies. At the most obvious level privacy involves restricting invasions of physical space, and the protection of home and personal possessions, which is why early privacy protections focused upon the inviolability of the home and family life. Concerns about controlling what information is known about a person came with communication technologies. Concerns about the erosion of privacy are not new – in fact, it might be argued they are feature of the twentieth century. Warren and Brandeis' seminal paper on "The Right to Privacy" in 1890, drafted at a time when newspapers were printing pictures of people for the first time, defined the right as the "right to be left alone". Their definition – driven by an emerging technology as is often the case with privacy – was concerned with protecting the "inviolate personality" and encompassing such values as individual dignity, personal autonomy and independence.[1] The growth of modern mass media and the advertising industry's focus on understanding consumers' wants led Myron Brenton to argue that we are living in the "age of the goldfish bowl", where private lives are made public property by the manipulation and exchange of personal data.[2]

There is a tension between the right to freedom of expression – in particular the media's exercise of the right – and the right to privacy. Freedom of expression, whether exercised by individuals or by the media, and the ability to exercise it, is an essential feature of any open, liberal and democratic society. It is only through exercising free expression that societies can sustain real democratic accountability. However the right to freedom of expression is not unlimited and it can be qualified to protect the rights and freedoms of others. It is a delicate balance to decide where the boundary between free expression and privacy lies but one the courts are used to negotiating.

Latterly, privacy was also defined as the right of people to determine when, how and to what extent information about them is communicated to others[3] as a response to the growing processing power of computers. Privacy, according to Westin "is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others ... [It is] the desire of people to

---

1 Bloustein, E. (1964) Privacy as an aspect of human dignity: an answer to Dean Prosser 39 NYU L Rev 962

2 Brenton, M (1964) The Privacy Invaders

3 Westin AF (1967) Privacy and Freedom New York: Atheneum, page 7

choose freely under what circumstances and to what extent they will expose themselves, their attitudes and their behaviours to others".[4] The specific dimension affecting privacy as brought by the Internet is considered in more detail in Section 2 Global overview of challenges and opportunities for privacy protection on the Internet.

Debates about privacy and information technologies since the 1990s have taken little account of gender. Concerns have been expressed about the potential of invasive informational technologies to violate women's privacy for sexual purposes and the "enforced privacy" imposed by patriarchal cultures upon women and girls. Neither of these are central to the privacy issues discussed in this paper or to the exercise of privacy rights as developed in the later sections. For this reason our paper refers to people throughout rather than distinguishing between women and men, as we believe that privacy rights are universal and applicable to both women and men on an equal basis.

Just as the notions of privacy have shifted with changing circumstances, early forms of legal protection were not overarching systems to protect privacy but rather sought to address specific problems in specific contexts and situations (which today might be viewed as aspects of the general right to privacy). One early example of such "privacy" legislation was England's Justices of the Peace Act of 1361. It provided for the arrest of "peeping toms" and eavesdroppers.[5] The pioneering Entick v Carrington [1765] case which shaped the fourth amendment of the US constitution came from a desire to protect papers held in a private home. Other examples focused upon the purposes for which governments could use the information they held about individuals (Sweden) or prohibitions on the publication of certain types of personal information (France and Norway).[6]

In the twentieth century international legal standards defined privacy as a human right. The Universal Declaration of Human Rights (UDHR), 1948, contained the first attempt to protect privacy as a distinct human right. Article 12 of the UDHR provides that:

> "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."

While not legally binding, the UDHR proved immensely authoritative and the right to privacy can be found in many other human rights documents including the legally binding International Covenant on Civil and Political Rights (ICCPR) and the European Convention on Human Rights (ECHR). These are dealt with in more detail in Section 3 dealing with legal standards, The Global Legal and Regulatory Environment for Protection of Privacy.

In addition to these broad international provisions, many countries include a right to privacy in their constitutions, provide for it in specific laws or have had the courts recognise implicit constitutional rights to privacy, as they do in Canada, France, Germany,

---

4 Ibid

5 Beresford A. and Stajano F. (2003) Location Privacy in Pervasive Computing, IEEE Communications Society

6 Privacy International, (2006) Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments

Japan, and India.[7] Some census agencies have privacy policies to ensure the protection of personal information being collected.[8]

Despite the extensive protections in both basic constitutions and law, the right to privacy remains a somewhat nebulous concept and securing the right will depend largely on the circumstances of individual cases. The European Court has stated itself that "the Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of 'private life'".[9] The lack of clarity has led one commentator to state that the fact that something "feels wrong... is often the most helpful delineation between when an incursion into the private life of an individual is reasonable and when it is not".[10] Privacy International has attempted to bring some clarity to the issue by defining four different types of privacy: information privacy (e.g. personal data), bodily privacy (e.g. invasive procedures), privacy of communication (e.g. surveillance) and territorial privacy (e.g. home).[11] In relation to the Internet, information privacy and privacy of communication are the most pertinent.

The importance given to privacy by many legislators and thinkers in history indicates its significance, however, as Paul Chadwick (information commissioner for the Australian State of Victoria) puts it: "Privacy is the quietest of our freedoms ... Privacy is easily drowned out in public policy debates ... Privacy is most appreciated by its absence, not its presence".[12] The value of privacy has been articulated in terms of value to the individual, it is essential to human dignity and indeed to individuality, it is said that if all our actions are watched and catalogued, we are less able to be ourselves. The value of privacy has also been articulated in terms of its instrumentality. Democracy and liberty rely on individuals having a certain degree of privacy. The right to privacy underpins many human rights, the right to freedom of association, freedom of belief and freedom of expression being particularly significant examples. As one writer puts it "in one sense, all human rights are aspects of the right to privacy",[13] in that if privacy is protected then the integrity of the individual is assured and this is the foundation of other rights and freedoms designed to protect the dignity of the person.

However it should also be noted that while people are often concerned about privacy in the abstract, they seem less concerned about privacy in practice. It is clear from a cursory use of the Internet that people give out personal information to a frequently surprising degree. Many writers have noticed the gap between what people say they value and what they actually do online. It may be the nature of the Internet, which is often accessed privately and combines both a communication medium in the shape of e-mail (which may suggest to the user the privacy of the telephone call or private conversation) and a publishing medium as with an application like Facebook. There is some anecdotal evidence that people do not realise the implications of publishing online, of how it will be

---

7 Solove, D.J. (2008) Understanding Privacy Harvard University Press

8 United States Census Bureau, Data Protection and Privacy Policy http://www.census.gov/privacy/data_protection/our_privacy_principles.html

9 Niemietz v Germany (1992), 16 EHRR 97. Para 29

10 Hosein, G. (2006) "Privacy as freedom" in R. Jorgensen (ed.) "Human Rights in the Global Information Society" MIT Press, Cambridge.

11 Privacy International, 2006.

12 Ibid. Page 2

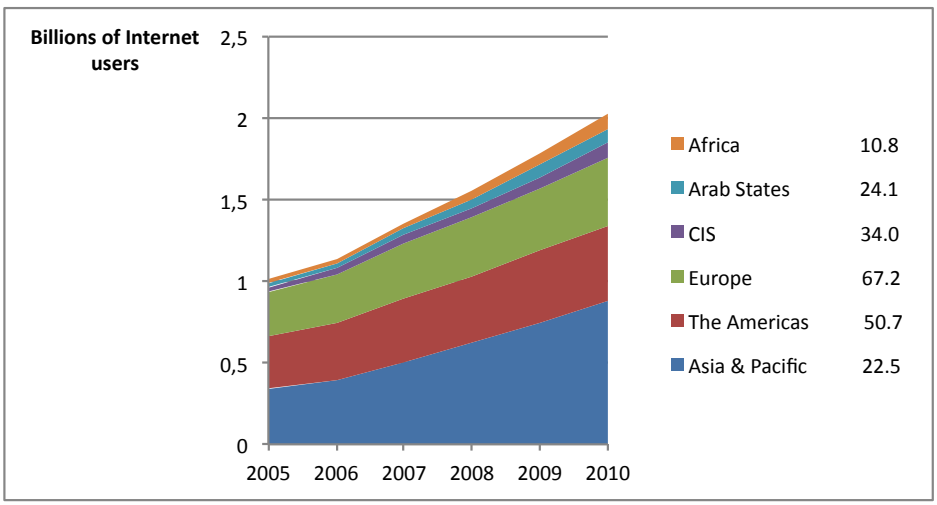
13 Volio, F. "Legal Personality, Privacy and the Family" in Henkin (ed), The International Bill of Rights (Columbia University Press 1981).

globally available and undeletable. For example, 57% of US adults who use the Internet at home believe incorrectly that when a website has a privacy policy, it will not share their personal information with other websites or companies.[14]

1.1 How has the Internet changed the nature of threats to privacy? What are the main threats in the digital age?

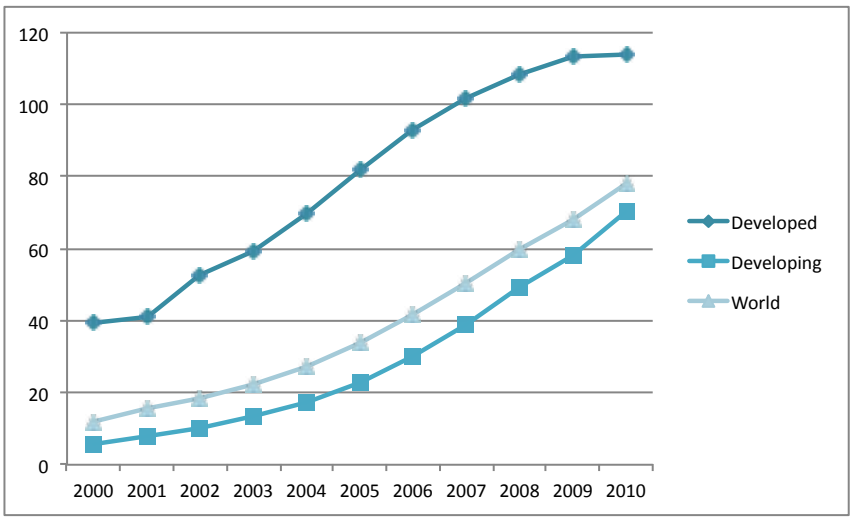
Internet access is expanding rapidly across most of the world. Statistics from the ITU, Figure 1, show that between 2005 and 2010 alone, the number of Internet users doubled. In 1995 only 0.4% of the world's population had access to the Internet, by March 2011 that percentage had erupted to 30.2%.[15] This corresponds to more than two billion Internet users, 1.2 billion of whom are in developed countries. The rise in usage of mobile phones has been even more extraordinary. Figure 2 shows the number of mobile subscriptions between 1998 and 2009. Today there are 5.3 billion mobile cellular subscriptions worldwide. Access to mobile networks is available to 90% of the world's population, and some commentators believe that universal availability may be achieved within the next five years.[16] In developed countries there are more mobile subscriptions than there are people (113.6 subscriptions per 100 inhabitants), and while the number is much lower in developing countries, it is still very high, with 56.8 subscriptions per 100 inhabitants.[17]

Figure 1[18] Internet users in different regions



14 Turow, J. Americans and Online Privacy: The System is Broken http://www.securitymanagement.com/archive/library/Anneberg_privacy1003.pdf
15 Internet World Statistics http://www.internetworldstats.com/emarketing.htm
16 See e.g. Sarrazin, T. (2011) Texting, Tweeting, Mobile Internet http://library.fes.de/pdf-files/bueros/africa-media/08343.pdf
17 ITU World Telecommunication, 2010a. The World in 2010. Pg4. [online] http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf
18 ITU World Telecommunication, 2010. Pg16.

Figure 2[19] Mobile cellular subscriptions per 100 inhabitants, 2000-2010



The combination of Internet and mobile phone has created a fast moving global digital communications environment. Though only a proportion of phones are Internet-enabled and an even smaller proportion are "smart", this is changing rapidly and in the next five to ten years most observers think that access to such phones will be very wide. While there were threats to privacy long before the digital age, the current challenges have changed significantly as the Internet has increased the capabilities of governments, businesses and individuals to intrude on the privacy of others. Many commentators note that much of the privacy we possessed in the past arose from default – the difficulties involved in monitoring people were too complex or expensive, technology could not cope and there was insufficient or too expensive man power. With the development of the Internet and the availability of cheap interactive digital communications the ability to monitor others has become easier, cheaper and more efficient. The Internet has enormously increased the potential impact upon the privacy rights a person has in both their identity and the treatment of their personal data. Internet use and transactions generate a large amount of personal information which is central to the business model of companies operating on the net – how these are understood, let alone regulated, in a fast changing transnational environment is a major challenge for policy makers.

In broad terms, the Internet:

- Enables the collection of new types of personal information
- Facilitates (and economically demands) the collection and location of personal information
- Creates new capacities for government and private actors to analyse personal information
- Creates new opportunities for commercial use of personal data
- Creates new challenges for regulation given the transnational nature of the Internet.

We examine the more detailed implications for each of these issues below.

19 ITU World Telecommunication, 2010. Pg16.

1.1.1 New types of personal information

Technological advances have developed the tools for collecting and understanding types of information which in the past would have been impossible or else unfeasible. For example, DNA's role in heredity was only confirmed in the 1950s, but nowadays progress in genetic sciences allows scientists to extract a person's DNA from ever more minute samples, and to determine ever more about an individual from their DNA. The digital storage of DNA is an enormous advantage in attempts to deal with crime as it has enabled a number of cold case murders to be revisited and at the same time has led to the freeing of a number of innocent people wrongly convicted of crimes. But the retention of DNA has significant privacy implications (among other issues) as it can contain a variety of sensitive personal information, such as a predisposition to certain diseases.

There are significant new developments in biometrics, such as facial recognition, finger scanning and iris-scanning, which are becoming increasingly popular as a method to secure identification. Such biometric devices have a wide variety of uses – they are used to prevent fraud by retailers and restaurant owners, to identify voters in elections, to provide immigration access (rather than use a passport), to maintain attendance records in workplaces or to gain access to high-security areas. While there is a great deal of social utility in these applications there are concerns about the control of such digital data, particularly questions of storage and access. There has been a particular controversy about whole body imaging used at airports following attempts by terrorists to smuggle bombs on planes inside their clothing. Many travellers dislike the use of technologies which penetrate clothing and produce what is essentially a nude image of an individual which is viewed by others. Many find this to be an invasion of their privacy. These images can reveal deeply personal information such as the fact that an individual has had cosmetic surgery or uses colostomy bags but in any case many people regard their clothing as an essential part of their bodily privacy. Against these privacy concerns must be balanced the safety of passengers of course but in these fast moving circumstances striking the right balance is fraught with difficulties.

1.1.2 Collection and location of personal information

Each computer, mobile phone or other device attached to the Internet has a unique IP address, which provides unique identifier for every device and which means in turn that they can be traced. The ability to locate any device creates significant new privacy challenges. Of the many tools that have been created to track Internet users, two common examples are cookies and web bugs. Cookies are small pieces of text which web browsers store on a user's computer. The cookie 'registers' with the web browser each time the user accesses that browser and can be used for session tracking, storing site preferences, authentication etc. Users can decide whether or not to accept cookies by changing settings on their browser software, but some sites become unusable without them. Web bugs are usually invisible to the user (they are typically only 1x1 pixel in size) and are embedded in web pages and emails. When the page/email containing the web bug is viewed, it sends information back to the server (including the IP address of the user, the time and date that the page/email was viewed and the browser it was viewed on).

An IP address can be tied to a person's physical identity in many ways. Many websites and ISPs have developed authentication systems which involve identity disclosure

(particularly during electronic commercial transactions); many applications require personal e-mail or other forms of identification, governments may require Internet users to register their IP addresses, or identity can even sometimes be deduced through a person's online actions (see below).

A key feature of the Internet is its interactivity when compared with "old" technologies such as the television, radio and telephones. Users are often required to provide information about themselves every step of the way – for example, what searches they make, what links they click on, what pages they look at and for how long. A series of technological tools and devices are designed to collect this information (e.g. TiVo, Xbox360, Google Books).[20] This is a central part of the economic model of the Internet. The digitalisation of information and expectation of free access makes traditional forms of income generation more complex on the Internet. Successful companies therefore consciously "mine" personal data in order to target advertising at users. There is therefore a direct and powerful economic incentive to secure, retain and share personal data. This also applies to non-Internet electronic activity. Computerised bar codes can be used to track individual purchases which in turn are then used to control stock levels and target incentives or marketing at those consumers. Computerised travel cards, such as the London Oyster card, create a digital picture of every journey that can be used to monitor city wide passenger movements – useful for transport planning, but also for tracking an individual's journeys. As the Internet is used in more and more everyday interactions including banking, shopping and socialising people are giving away more and more of their personal data, often unwittingly including sensitive information about their finances, heath and even their sexuality. These developments allow an ever greater amount of information to be gathered and, as Lawrence Lessig pointed out, "your life becomes an ever-increasing record".[21]

Watching and locating people offline has also become much easier using electronic surveillance. CCTV cameras and satellites are used to monitor public and private spaces, and are available to more and more people. Locational information is now extraordinarily cheap through private initiatives such as GoogleEarth. Global Positioning Systems (GPS) are incorporated into more and more consumer devices. Radio-Frequency Identification (RFID) tags are another example. Such RFID tags have been expensive, but prices are falling and ultimately they could identify, for example, not only the product that a consumer buys but how often it is used and where.[22]

1.1.3 New capacities for private actors to analyse personal information

Increased computing power means that vast quantities of information, once collected, can be cheaply and efficiently stored, consolidated and analysed. Technological advances allow databases of information to be connected together allowing even greater quantities of data to be processed. The potential for privacy violations increases exponentially as technologies are combined together, for example, linking facial recognition databases (as used on Facebook for example) with CCTV cameras would allow tracking of individuals on an unprecedented scale.

---

20 Privacy International, 2006

21 Lessig, L. (1999) "Code and the Laws of Cyberspace" Basic Books, New York. Page 152.

22 Martínez-Cabrera, A. (2010) Privacy concerns grow with the use of RFID tags http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2010/09/05/BUCE1F8C1G.DTL

The practice of merging and consolidating different informational databases is pervasive. Privacy issues clearly arise from matching data from different sources, for example tax data against health data or finance data against social security data. In addition personal data can be extracted from the various techniques and then matched with publicly available data to build a detailed personal profile.

The US-based privacy organisation EPIC states that "collectors of consumer information are willing to categorise, compile, and sell virtually any item of information". For instance, the Medical Marketing Service sells lists of persons suffering from various ailments. These lists are cross-referenced with information regarding age, educational level, family dwelling size, gender, income, lifestyle, marital status, and presence of children. The list of ailments includes: diabetes, breast cancer, and heart disease. Other companies sell databases of information relating to individuals' lifestyle habits, reading preferences, and even religion".[23]

Combined databases have numerous uses. They can be used for data mining, which is "the process of finding patterns in information contained in large databases"[24]. Data mining itself has many uses, many of them beneficial such as to identify patterns indicating fraudulent credit card use. While some commentators claim that data mining is neutral, it can have privacy implications. The mining of data or merging data often involves using people's information in a way that they did not consent to and are not even aware of. Furthermore, the wide array of data drawn upon often includes personal details and can easily be linked to individuals without their knowledge.

Another common use is data profiling which is the use of aggregated data to "identify, segregate, categorise and generally make decisions about individuals known to the decision maker only through their computerised profile"[25]. Companies and governments can use data profiling to build comprehensive profiles on individuals. EPIC give the example of a woman who sued the US-based Metromail after one of their data entry clerks stalked her based on information she submitted in a survey. During the case it emerged that Metromail maintained a 25 page dossier on the woman including "her income, and information on when she had used haemorrhoid medicine".[26]

In order to protect privacy (and circumvent privacy laws), companies often de-identify or anonymise the data. This is a process of stripping data of personal identifiers (such as name, social security number, and IP number). However, studies reveal that it is often possible to relate 'anonymised' information back to an individual. For example, a 1990 study in the United States of America found that data collected during a census (post code, birth date and gender) can be cross-referenced to uniquely identify 87% of their national population.[27] A more recent example occurred in 2006, when AOL released user search data which was supposedly non-identifiable; researchers were consequently able

---

23 Rotenburg M. And Hoofnagle C. "Submission to the House Government Reform Committee on Data Mining" March 25, 2003. http://epic.org/privacy/profiling/datamining3.25.03.html

24 Fayyad, U., Grinstein, G. and Wierse, A. (2001) "Information Visualization in Data Mining and Knowledge Discovery". Morgan Kaufman Publishers.

25 Netter, W. "The Death of Privacy" Privacy Module I: Data Profiling Introduction, University of Harvard, 2002 http://cyber.law.harvard.edu/privacy/Module2_Intro.html

26 EPIC, "Privacy and Consumer Profiling" http://epic.org/privacy/profiling/

27 Sweeney, L. "Strategies for De-Identifying Patient Data for Research" Carnegie Mellon University, Data Privacy Lab, 1998 http://www.ocri.ca/ehip/2005/presentations/Sweeney_bw.pdf Page 26.

to identify many users through the not unusual phenomena of vanity searches, where an individual searches their own name.[28]

Databases can be very hard to protect, especially where they can be accessed remotely and where many people are granted access. This leaves personal data in databases vulnerable to all sorts of cybercriminals. Additionally, information is often released into the public domain. This is often for legitimate reasons, but can raise privacy concerns. For example, the WHOIS database contains the personal contact details of the individual or organisation that registered each domain name. It is released publicly to allow network administrators to easily remedy problems on the Internet.[29] Another example is the movement, in many countries, to release public records in digitised format. Such information would have been available previously (such as birth, wedding and death certificates) but new formats make the information increasingly more accessible and easy to cross-reference.[30]

1.1.4 New capacities for governments to analyse personal information

Governments are attempting to harness the power of the Internet across their functions. There has been a dramatic move towards e-government as a way of providing more cost-effective and personalised services. As a consequence many countries are attempting to streamline and coordinate service provision through developing large databases containing personal information about citizens. Identity cards, for example, are in use in one form or another in virtually all countries of the world, and compulsory national identity cards are used in about 100 countries.[31] Increasingly, governments are moving towards capturing biometric data on the cards and storing this information on huge databases which can be used to certify access to, and monitor use of, for example, social security, health and travel.

There is a particularly important role for these technologies in the field of crime prevention and prosecution. Even before the so-called "war on terror" many governments were making great use of monitoring technologies such as CCTV cameras for these reasons. Since 9/11 the threat of terrorism has acted as a driver in many countries for increased use of monitoring mechanisms, often in ways which are intrusive and even in violation of existing privacy laws. A particularly pertinent example is that of air travel. As mentioned above, whole body imaging scanners are being used or trialled in the United States of America, the United Kingdom of Great Britain and Northern Ireland, India, Australia, Japan, the Russian Federation, and the Netherlands among others.[32] Another practice has been the use of secret watch lists, for example in Canada and the United States of

---

28 Soghoian, C. (2007) "The Problem of Anonymous Vanity Searches" Indiana University Bloomington – School of Informatics. Published online http://papers.ssrn.com/sol3/papers.cfm?abstract_id=953673 Page 1.

29 EPIC "WHOIS" accessed 15/03/10, published online http://epic.org/privacy/whois/

30 Privacy International, 2006.

31 Privacy International, 1996, ID Card Frequently Asked Questions https://www.privacyinternational.org/article/id-card-frequently-asked-questions

32 Cavoukian, A. "Whole Body Imaging in Airport Scanners: Building in Privacy by Design" Information & Privacy Commissioner, Ontario, Canada. June 2009 http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf Page 2.

America.[33] Personal data is submitted by travellers as a condition of travelling and this information is checked against databases of uncertain provenance. Data profiling is used to create a list of people who are judged to be a security threat, the list is circulated to other countries, and people on the list are either prevented from flying or are subjected to enhanced security measures. Watch lists sometimes become public; this has exposed errors, but stigmatised individuals; other times they have been kept secret which has meant that individuals have been refused a visa without necessarily having been convicted of anything or given the opportunity to defend themselves.[34] In one famous case in the United Kingdom of Great Britain and Northern Ireland, a prominent Muslim, Yusuf Islam (formerly the singer known as Cat Stevens) was prevented from travelling to the United States of America (his United Airlines flight from London to Washington's Dulles International Airport was diverted to Bangor, Maine, when US officials reviewing the passenger list discovered he was aboard). There were allegedly terrorist connections reasons but these were never made explicit, despite his record as a Muslim who promoted peace and reconciliation among communities. Subsequently the ban was lifted.

Some governments have been able to use these technologies to monitor the actions of their citizens, particularly dissidents, much more intensively. For example, the OpenNet Initiative reports that in China the most popular online instant messenger (QQ) records users' online communications and reports on these to the police. In 2006, the Chinese Ministry of Public Security announced the launch of the "Golden Shield" project, designed to become a national system of a digital surveillance. In 2008 a Chinese state-owned mobile phone company revealed that it had unlimited access to its customers' data and that it supplies this to the Chinese government on request. The most glaring example of this was the Chinese government's attempt in 2009 to insist that software known as Green Dam be built into all personal computers sold in China.[35] This software would have monitored individual computer behaviour by installing components in the operating system and would have given the authorities direct power to control access to content (as well as allowing remote control of the computer running the software).[36] The proposal was finally defeated through the WTO on trade grounds. More recently, there have been reports that Chinese authorities have tried to make cafes, hotels and other businesses in central Beijing install surveillance technology for those using Wi-Fi which has been seen as another instance of tightening controls on the use of the Internet.[37]

The Special Rapporteur on counter-terrorism and human rights has noted examples of surveillance practices in Germany, Colombia, Bangladesh and the United States of America that caused him concern.[38] A 2007 Privacy International study revealed an overall worsening of privacy protections and safeguards, together with an increase in the occurrence of surveillance across 47 countries.

---

33 Human Rights Council, Thirteenth session, Agenda item 3. 28 December 2009, A/HRC/13/37 http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf Page 17.

34 Ibid.

35 Opennet Initiative, China's Green Dam: The Implications of Government Control Encroaching on the Home PC http://opennet.net/chinas-green-dam-the-implications-government-control-encroaching-home-pc

36 Wolchok, S.; Yao, R. and Halderman, A. (2009) Analysis of the Green Dam Censorware System http://www.cse.umich.edu/~jhalderm/pub/gd/

37 Branagan, T. (2011) China boosts internet surveillance http://www.guardian.co.uk/world/2011/jul/26/china-boosts-internet-surveillance

38 Human Rights Council, 2009, 19, 20

Cybercrime is a growing problem on the Internet with estimates putting the cost of online theft at $1 trillion.[39] Lax security measures and security breaches can result in criminals stealing other people's data which can then be used to commit many crimes such as fraud, theft or stalking.

Finally, surveillance technologies are being used much more locally, to monitor behaviour of family members and of employees. Instead of monitoring employees who exhibit suspicious behaviour, there was evidence that many employers were instituting continuous systematic surveillance in the workplace.[40] Indeed a market is developing for new technologies assisting employers in monitoring their employees, as exemplified by the recent development of new technology that can detect complex employee behaviour and report back to the employer – the device can differentiate between actions such as "scrubbing, sweeping, walking, and even emptying a rubbish bin".[41]

1.1.5 New opportunities for commercial use of personal data

The Internet has generated a vast amount of economic activity. A recent study by McKinsey estimates that the direct and indirect economic effects of the Internet account for 3.4% of GDP in the 13 countries studied but 21% of the economic growth in the five mature economies, with 2.6 jobs created for every job lost.[42]

Internet companies such as Google, Yahoo and Facebook have access to an astronomical amount of data.[43] The biggest Internet companies have huge user bases (for example, Facebook has over 800 million users[44]) and are branching out to cover more and more interactions (for example, a user may use Google to locate information online, send emails, display videos, shop etc.) Many of the services provided by these companies are free and their business models rely on collecting user information and using it for marketing purposes. User data therefore has significant economic value. A 1999 study discovered that 92% of websites were gathering at least one type of identifying information from their users (for example their name, email address and postal address)[45] and it can be assumed that since then gathering of information has only increased. Companies also have a tendency to be very secretive about what information they gather and how; as noted in The Economist, this is as much to do with maintaining a competitive edge as it is with privacy concerns.[46]

---

39 Weber, T. Cybercrime threat rising sharply, BBC News, 31/01/09 http://news.bbc.co.uk/1/hi/business/davos/7862549.stm

40 Bonsor, K. Is your workplace tracking your computer activities? http://computer.howstuffworks.com/workplace-surveillance1.htm

41 Fitzpatrick, M. "Mobile that allows bosses to snoop on staff developed" BBC News 10/03/2010 http://news.bbc.co.uk/1/hi/technology/8559683.stm

42 McKinsey Global Institute, (2011) Internet matters: The Net's sweeping impact on growth, jobs, and prosperity http://www.eg8forum.com/fr/documents/actualites/McKinsey_and_Company-internet_matters.pdf

43 Massimino, E. (2012) Privacy, Free Expression And The Facebook Standard http://www.forbes.com/sites/realspin/2012/01/31/privacy-free-expression-and-the-facebook-standard/

44 Protalanski, E. (2012) Facebook has over 845 million users https://www.zdnet.com/blog/facebook/facebook-has-over-845-million-users/8332

45 Federal Trade Commission, (1999) "Self-regulation and Privacy Online: A Report to Congress" March 1999, Published online at http://www.ftc.gov/os/1999/07/privacy99.pdf Page 4.

46 Economist, (2010) "Clicking for Gold: How internet companies profit from data on the web", in "A special report on managing information" The Economist, Volume 394, Number 8671

Much of this economic activity depends upon Internet intermediaries – the range of actors, services and applications that facilitate transactions between third parties on the Internet, including for example search engines and ISPs. Internet-based communications are increasingly reliant on these intermediaries for accessing, processing and transmitting data. The increasing power of intermediaries and their control over personal data, has given rise to a number of concerns about whether current regulation is sufficient to protect privacy rights. Three types of intermediaries arouse particular concerns – social networking sites, cloud computing capacities and search engines.

Social networking sites

Social networking sites are websites that focus on building and/or reflecting social relations among people. Some facilitate virtual "friendships" with people who are already known to the user offline, allowing them to share photos and converse online. Others concentrate on allowing people to make new friends, often with a particular focus such as work relations (LinkedIn) or music tastes (Pandora). Each service is different, but the standard format allows users to create their own webpage containing various pieces of personal information (such as date of birth, location, interests, name). Users can then link to friends who will be able to see their information and vice versa. Social networking sites are very popular, with hundreds of millions of users between them. However there has been growing concern over privacy violations caused by such sites. Some concerns relate to media and communications literacy, with many users unaware of the risks involved in revealing personal information to others. Many users do not exercise restraint about who they allow to see their data, and many users are believed to befriend people that they do not know well. This can have considerable implications given, for example, that on Facebook the average user has 130 friends on the site.[47] This is discussed in more detail in the following section.

Cloud computing

Cloud computing is an emerging network architecture whereby data, processing power or software is stored on remote servers, as opposed to an individual's computer, and made accessible via the Internet. Different forms of cloud computing exist that provide a range of services. Individuals or organisations can effectively rent computing capacity from remote service providers. For example, Google's Apps service allows people to create and save spreadsheet and word processing documents online. Other services include collaborative platforms that allow users access to documents simultaneously, such as wiki platforms and Google docs.[48]

Cloud computing can yield a number of positive benefits. For example, it can reduce the costs of buying and updating software for small businesses and organisations, which can be particularly empowering for users with low levels of financial resources in developing countries. It can also improve convenience for users through allowing them to access documents anywhere in the world, and collaboratively author documents with people working in other geographical locations.

---

47 Facebook, (2012) " Statistics" published online http://www.facebook.com/press/info.php?statistics

48 EPIC "Cloud Computing" published online http://epic.org/privacy/cloudcomputing/

However, cloud computing also raises a number of concerns from a privacy perspective. As data is stored on a third party's software, the responsibility for protecting that information lies with the third party and users lose a degree of control. Additionally, laws covering cloud computing are not well defined so users are not assured of the privacy of their data. The terms and conditions (T&Cs) of use sometimes state that the service provider is able to terminate accounts or remove/edit content at their own discretion. For example, this is the case for Mozy.com, a service that allows users to back up the information stored on their PCs online[49]. This presents the danger that users could lose their personal information. Many T&Cs strictly limit the liability of the service provider, which could mean that should there be a breach in security and users lose their personal data, they may not have access to any compensation. Finally service providers often do not address what happens with a user's information once they have closed or deleted the account. This does not always mean that information is removed, potentially leading to privacy breaches[50]. The privacy implications of cloud computing are discussed in greater detail in the following section.

Search engines

Search engines fulfil a crucial role as intermediaries on the Internet, allowing individuals to find and access content. Examples include Google, Bing, Ask.com, and Yahoo! Search. Search engines typically collect a large amount of personal data including IP addresses, search requests, together with the time, date and location of the computer submitting the request. As discussed above, this information can be personally identifiable and can reveal particularly sensitive pieces of information such as a person's political beliefs, sexual orientation, religious beliefs and medical issues. This information is generally used for marketing purposes, however there are also risks of public disclosure of information, such as AOL's release of information in 2006 (discussed above). The risks regarding privacy and other human rights are all the more significant in countries with limited protections for human rights. This is discussed in more detail in the following section.

49 Ibid
50 Ibid.

2. GLOBAL OVERVIEW OF CHALLENGES AND OPPORTUNITIES FOR PRIVACY PROTECTION ON THE INTERNET

2.1 Key issues

2.1.1 Challenges and opportunities for maintaining control over personal data online

> "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." – Article 12, Universal Declaration of Human Right.

Protection of privacy has long been enshrined as a core human right. However with new technical developments in recent decades, particularly in information and communication technologies, this right has been increasingly challenged. In response to these difficulties there has been a wave of data protection laws in different parts of the world since the 1980s, which have attempted to safeguard the personal data of individuals. However legislation and public policy have had significant difficulty in keeping up with increasingly short technology development cycles. This problem has become most evident on the Internet, where it is highly questionable whether the European Union statement that "everyone has the right to the protection of personal data concerning him or her"[51] is respected. Do individual Internet users have control over their own personal data, including over how it is collected, retained, processed, used and disclosed?

In practice, many attributes of the Internet prove highly challenging for individual user rights to control their personal data. The transnationality of the Internet makes it difficult and at times impossible to judge across which countries, legal jurisdictions and regions their data is being transmitted. The speed and reach of Internet communications is so high that data may spread far beyond the actual control of an individual within less than a second. Moreover there is a substantial market on the Internet for personal data, which is driven by advertising-based business models in which users pay with their data instead of providing monetary payment. At the same time the cost of such data is extraordinarily low leading tens of thousands of records of personal user data to be exchanged at little or no cost. Advances in computerised processing technology allow for an increasing amount of

51 Art. 8.1, Charter of Fundamental Rights of the European Union, 2000.

personal data to be processed. The many different parties involved in displaying an Internet page on a user's screen complicate this process considerably. Increasing convergence of devices connected to the Internet also makes it particularly difficult to maintain control over personal data. Finally, many Internet users have become accustomed to clicking 'Accept' and consenting to providing their data without spending any meaningful amount of time reading the terms of service or privacy policy of the respective site.

The tension between rights and actual control capacity of Internet users over their personal data has led to extensive debates about privacy on the Internet. These debates typically focus on the lack of user control and empowerment in influencing how their data is used and processed, while emphasising the role of corporations in controlling and managing private data. Moreover the control of private actors is frequently contrasted with that of public authorities, which are seen as either unable or unwilling to enforce substantive protections of users' personal data.

These debates can be understood in the context of several basic questions. First and foremost, the question of informed consent of users and how it can be obtained, guaranteed or even revoked. Second, the question of the transparency and 'readability' of privacy policies to users. Third, the ability of users, private actors and public entities to effectively enforce their individual choices about personal data usage on the Internet. Even if most users, private actors and public entities are in agreement, diffusion of personal data is such that it may quickly move beyond the capacity of any one actor to control (see inset below for further details).

Fourth, user rights to control their personal data may conflict with other rights, such as the right of another individual to freedom of expression. As is discussed in the inset below about Visual Privacy and Edison Chen, there are frequent conflicts between media reporting about public figures and their rights to control their personal data. Fifth, the problematic role of public authorities' surveillance of the Internet remains difficult. Lastly, the appropriateness of anonymity and pseudonymity online represent an important component in the overall debate on privacy protection on the Internet. While all of these questions are intimately linked to information privacy, they also provide an answer to the broader challenge: what is the Internet we hope to create? Whichever stakeholder group, nation state or grouping of actors this 'we' may represent, considering a common vision of a future Internet may assist in understanding how to get there. Providing substantive answers to this question will fundamentally shape the global Internet as a whole.

(I) Visual privacy and Edison Chen

Edison Koon-Hei Chen was one of the leading actors from Hong Kong. He acted in numerous different regional and international films and was considered one of the leading actors in the area, also acting in Hollywood productions such as The Dark Night. In January 2008 sexual images of Chen together with other women from the film industry in China began to surface on the Internet and were extensively publicised in mainstream media. Although national and international police authorities were involved in attempting to stop the pictures spreading

further, they were seemingly unable to do so.[52] They continued to spread across the Internet and as a result the name of the actor was one of the top search terms in China in 2008.[53] A computer technician who repaired Edison Chen's laptop was eventually convicted for having stolen the pictures while repairing it in 2007.[54] Once the pictures had made their way online they became extremely difficult if not impossible to remove. In this context the massive public demand for the images ensured their widespread distribution. The widespread republication of and associated demand for images was clearly violating personal privacy and the massive public demand for such images raises questions about how to foster a culture of information privacy.

2.1.2 Initiatives to protect privacy and anonymity online

In response to many of these questions a variety of initiatives have sprung up on the Internet to protect the privacy of individuals. In this, there is extraordinary importance in civil society initiating and organising initiatives to protect privacy and anonymity online.

This role is reflected in the many important initiatives civil society has spearheaded. In this context one of the most important initiatives has been to raise awareness and education of users about the importance of their privacy and how it can be protected. Important examples include the 'Surveillance Self Defence' project created by the Electronic Frontier Foundation (EFF), Big Brother Inc.' a project profiling companies exporting surveillance technologies and 'Me and my own Shadow' which is an awareness raising campaign by the NGO TacticalTech.

(II) Citizens initiative on data retention

One of the most remarkable user initiatives for the protection of privacy and anonymity on the Internet is the German citizen initiative on data retention. Over 34,000 citizens initiated a mass constitutional complaint against the newly passed German data retention law with the German Constitutional Court in 2007.[55] This massive class action represents the largest joint case ever brought to the German constitutional court. The lawyers involved took several months to process the signatures and submit them to the court. The constitutional court initially issued a preliminary injunction against the new data retention law in 2008 and eventually declared the data retention law unconstitutional in 2010.[56] As very few constitutional complaints are even accepted by the German constitutional court and only around

52 Pang, D., Chen, B., & Lee, D. (2008). Eight now held in internet sex probe. The Standard. Retrieved December 13, 2011, from http://www.thestandard.com.hk/news_detail.asp?pp_cat=12&art_id=61125&sid=17431562&con_type=3#.

53 Google. (2008). Google Zeitgeist 2008. Retrieved December 13, 2011, from https://www.google.com/intl/en/press/zeitgeist2008/world.html#top.

54 Pomfret, J. (2009). Technician guilty in Edison Chen sex pictures trial. Victoria News. Retrieved December 13, 2011, from http://www.vicnews.com/entertainment/television/43998412.html.

55 Initiative Vorratsdatenspeicherung. (2011). Stoppt die Vorratsdatenspeicherung. Retrieved December 13, 2011, from https://www.vorratsdatenspeicherung.de/static/verfassungsbeschwerde_de.html.

56 BVerfG, 1 BvR 256/08 on the 2.3.2010, Paragraph-Nr. (1 - 345), http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

1-2% are successful, this successful joint complaint was a watershed moment. As such the initiative was successful, not just in having the German data retention law declared unconstitutional, but in bringing privacy and anonymity to the fore of the public debate in Germany. As the German data retention law translated an EU directive into national German law, the ripples of this decision have been felt far beyond German borders and have heavily influenced both debate and practice of data retention in Europe.

Each of these projects demonstrates the important role played by civil society in raising awareness about privacy issues, providing users with resources to defend their privacy and informing citizens about the workings of the surveillance industry. Both international and local civil society organisations have played a crucial role in this context in empowering the users of technology to make informed choices about their personal data.

Technical initiatives also play a valuable role protecting privacy and anonymity online. The development of free and open source tools for Internet users such as Tor, GnuPG or HTTPSEverywhere have contributed substantially to the privacy and anonymity of Internet users. These open source programs provide Internet users with a greater level of anonymity while using the Internet, allow them to secure their files and their emails or provide better security when accessing many websites.

All of these technical efforts have received extensive support and development from Internet users across the world and various civil society organisations. Notably most private sector initiatives focus on providing end users' access to strong encryption technologies, which provide an invaluable counterbalance to Internet surveillance technologies. It has repeatedly been suggested by academic, technical experts and civil society alike that a substantial expansion in the use of strong encryption technologies among Internet users would have a highly positive impact on privacy and anonymity on the Internet.

(III) Corporate initiatives promoting freedom of expression and privacy: the Global Network Initiative

Separately from citizen's initiatives, one of the most prominent self-regulatory initiatives among Internet corporations is the Global Network Initiative (GNI). It brings together several technology companies, NGOs and academics. While it has been successful in creating awareness about the role of companies in protecting and advancing the rights of privacy and freedom of expression, the number of companies who are GNI members remains limited, with only a few large corporations involved: Google, Yahoo and Microsoft.

Although many other Internet corporations have been called upon and/or invited to join the GNI, these calls have to almost all been unsuccessful. As the GNI is still relatively young, it remains to be seen how its reporting requirements will affect actual company practises in the medium and long term.

Aside from civil society initiatives, user initiatives have also played an important role in safeguarding privacy and anonymity online. User initiatives tend to focus on one specific issue, rather than the concept of privacy as a whole. Campaigns for changes to 'real name policies' by the users of social networks, awareness-raising about the danger of sharing personal data on the Internet and a petition of over 30,000 individuals to the German Supreme Court against the constitutionality of data retention laws represent several important examples of significant user initiatives to protect privacy and anonymity online.

Also important to mention are corporate initiatives to protect privacy, of which the Global Network Initiative is one of the best known (see inset above). However there are widespread debates on the effectiveness on corporate self-regulation on the Internet. Particularly in regard to privacy it is frequently argued that corporate actors profit from selling the data of their customers and have no interest in providing anything beyond 'fig leaf' corporate social responsibility projects to mask their actual motives. The most frequent response to this claim is that companies require user's trust and any substantial breach of their trust would be harmful for the company breaching this trust. Whichever statement is true, there are clearly conflicting incentives for companies engaging in such initiatives and it is highly questionable the extent to which self-regulatory privacy regimes can replace public legislation and regulation.

Finally, among many privacy and anonymity advocates there is a notable distrust of the effectiveness of regulatory, judicial or governmental solutions. There is a widespread fear that public privacy regulation may be counterproductive, captured by special interests, badly informed or at best ineffective. While advocates have consistently called for regulatory change on privacy issues and continue to seek remedies for privacy violations through the judicial system, there is an equally strong focus on empowering users to ensure that they are not dependent on public regulation. This approach focuses on providing users with the tools they need to protect their own privacy and raising awareness about privacy issues. The main strategy of empowering end users to protect their privacy suggests that many advocates are not convinced that states are able or willing to tackle some of the most difficult privacy issues.

2.1.3 The roles and responsibilities of service providers and intermediaries

Internet service providers and Internet intermediaries have a particularly important role to play on the Internet. Their role goes far beyond the typical role of a company providing a standard product in a typical marketplace. Because Internet service providers and Internet intermediaries deal in information, these companies are capable through their actions of safeguarding or destroying many of the rights and freedoms of users on the Internet. Moreover their role does not exist in a power vacuum and different national and international governance arrangements, political and corporate interests often compete for greater control over Internet intermediaries. Consequently shielding such corporations from 'intermediary liability' is not a given, rather it represents a specific political bargain which is consistently challenged in many different contexts.[57] In response to these demands human rights advocates have issued robust defences calling for intermediary

57 Mueller (2010) Networks and States, Mueller, M. L. (2010). Networks and States: The Global Politics of Internet Governance, pp. 138-139. MIT Press.

liability rules to be elaborated in accordance with the standards of international protections.[58]

However in many cases there are other mechanisms by which intermediaries are coerced into invading their users' privacy than simply legal liability alone. Particularly Internet service providers (ISPs) are frequently coerced into 'voluntarily policing' their users actions, thereby creating infrastructure and institutions which collect and manipulate personal user data far beyond any mechanisms necessary for the provision of Internet services alone. This is just one of many examples in which Intermediaries are coerced or co-opted into fulfilling the wishes of third parties to invade and restrict their users' privacy.

At the same time the more transnational and disconnected from any specific physical location those Internet intermediaries operate, the more flexibility they obtain in their dealings with the respective legislative authorities. A special role in this context is played by large transnational intermediaries such as Google, Microsoft, Facebook or Amazon who can negotiate with nation-states on seemingly equal terms due to their size and international reach. The fact that they mainly sell software or online services allows them a considerable level of flexibility with regard to their physical location. The result is an ability to 'pick and choose' jurisdictions.

Nation-states across the world compete to host the companies and there are numerous indications through the research process that many countries have chosen weak privacy regulations strategically. This is done to achieve a (presumed) competitive advantage towards other developed economies. In many cases these strategic choices are made by small countries which have chosen to become regional hubs for the high-tech industry. This competition would seem to confirm privacy policy competition between countries being at least indirectly fostered by transnational corporations.

Another area which has become extremely controversial from a privacy perspective is data retention legislation. Through such legislation Internet service providers are made complicit in wide-scale surveillance and storage of private Internet practises of their customers. These measures typically take place on a broad scale without any suggestion that ISP customers who are being observed have committed a crime. However it is often argued that such measures could nevertheless assist in the investigation of crimes that were committed on the Internet. Child protection (see inset for further details) and copyright enforcement is another area where Internet service providers and Internet intermediaries have been put under considerable pressure to interfere with the privacy of their customers,[59] in ways that fall short of protection principles such as transparency, due process and accountability.

The pressure on Internet intermediaries such as Google, Facebook or Amazon can also cause substantial negative effects on Internet privacy. Unlike offline interactions in which it is extremely difficult to see personal, economic or political interactions on a broad scale, online interactions leave a 'data trail.' Google has begun to respond to this pressure by publishing regular 'Transparency Reports' to inform users about the extent to which data

---

58 La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue to the U.N. Human Rights Council [A/HRC/14/23]. Geneva: United Nations.

59 Mueller (2010) Networks and States, Mueller, M. L. (2010). Networks and States: The Global Politics of Internet Governance, pp. 150-151. MIT Press.

about them is being requested by governments. While this is a valuable first step, it is insufficient to map many of the informal coercive interactions which take place in order to gain private data from private corporations, or to specify to a greater extent why these requests were made.

A particularly complex role in this context is played by state-owned Internet service providers (ISPs). The fact that they are in state ownership and typically control much of the underlying Internet infrastructure leads them to be less independent from the state than would otherwise be the case. This can often have a detrimental effect on users' privacy, particularly in countries where the state has little regard for privacy and more generally the human rights of Internet users. Conversely, privatisation of state-owned ISPs together with local loop unbundling (LLU) are likely to provide an ISP market structure more conducive of protecting privacy. Here specific policies such as privatisation of state-owned ISPs and LLU may provide a healthy competitive ISP market. A properly functioning ISP market should in turn contribute to protecting users' privacy, by preventing oligopolistic or monopolistic markets in which there are only a few control points.

More generally, ISPs are in a particularly difficult position to resist invasions on their users' privacy, as they are typically subject to licensing agreements requiring them to provide data to public agencies. While this may be perfectly legitimate in certain situations, this puts them at a disadvantage to other Internet intermediaries who are less vulnerable to being forced into providing user data. The evolution of ISPs business model into providing bundled additional services and content to Internet users means that particularly large ISPs are far more vulnerable to regulatory coercion than they were in the past.

This development is further accentuated by much of the additional bundled content ISPs can provide being subject to the contractual terms of copyright-holders, who then require ISPs to invade their users' privacy in return for exclusive access to additional Internet content. Some ISPs in the mobile sector even welcome this development, as they already have privacy-limiting Internet infrastructure in place and consequently have a 'first mover advantage' over other ISPs when providing their users' data to their parties. As one ISP representative remarked during an interview, it takes considerable determination to regularly resist the frequent demands for private user data from state authorities.

More generally, national and transnational governance arrangements have made it extraordinarily difficult to stem the highly privacy-invasive international trade in individuals' personal data, or to provide effective remedies for trans-border violations of privacy. Transnational intermediaries play many different roles in these initiatives and may not always be committed to a rights-based approach to privacy. Finding effective governance mechanisms for data protection and privacy represents one of the greatest challenges to safeguarding human rights in a global information society.

(IV) Privacy of children and young people

Concerns about privacy require different types of consideration for different individuals.[60] In a recent study the European Network and Information Security Agency (ENISA) suggested that protecting the privacy of young people is one of the key strategies of combating cyber-bullying and online grooming.[61] They identify improperly designed Internet platforms and unnecessarily high levels of complexity as well as a lack of awareness as key vulnerability for young peoples' privacy online. As a result, one the main ENISA recommendations is that "the generation and use of user profiles for underage persons should not be possible in general,"[62] together with stricter financial penalties for companies who break these laws. In the United States of America, the Children's Online Privacy Protection Act is designed to ensure that Internet sites receive parental consent before collecting data from individuals under 13. As a result, many Internet sites including Facebook choose to exclude individuals under 13 from their website. At the same time academic research suggests that many parents assist their children in getting around age restrictions in order to access Facebook.[63] This clearly raises questions about the capacity of current legislation to protect the privacy of children and young people on the Internet.

2.2 Specific challenges posed by different applications, communications platforms and business models

2.2.1 Cloud computing

Cloud Computing is a relatively recent development where increasing amounts of data – including personal data – are stored in an online "cloud". While being stored, personal data is transmitted across the Internet which may already pose a risk to individual control over that data. Once the data has been stored in the cloud, these risks continue, for example a "cloud provider may, without notice to a user, move the user's information from jurisdiction to jurisdiction, from provider to provider, or from machine to machine."[64]

Furthermore, users' personal data in the cloud may be subject to dynamic changes in terms of service as "it is common for an Internet company establishing terms of service or

60 Hilles, L., & Jugendschutz.Net. (2011). Verlockt - Verlinkt - verlernt? Werbung, Vernetzung und Datenabfragen auf Kinderseiten. Mainz, Germany.

61 Marinos, L., & European Network and Information Security Agency. (2011). Cyber-bullying and online grooming: helping to protect against the risks. Heraklion, Greece.

62 ibid. p.47.

63 Boyd, D., Hargittai, E., Schultz, J., & Palfrey, J. (2011). Why parents help their children lie to Facebook about age: Unintended consequences of the "Childrens Online Privacy Protection Act'. First Monday, 16(11).

64 Gellman, R., & World Privacy Forum. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Retrieved from http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf.

a privacy policy to reserve the right to change the terms or the policy without limit."[65] This important caveat means that in many cases even a privacy policy or a 'terms of service' which seems to be highly protective of personal data may be changed from one day to the next. Users are limited in their ability to react to these changes and in certain cases may be unaware of them or unable to understand the implications of these changes for their own personal data.

Protection of personal data is confronted with the business model of cloud computing itself, which inherently expects users (and in many cases their customers as well) to transfer their personal data onto the Internet. In doing so users will usually give up any 'data sovereignty', that is they will no longer be able to define under which jurisdiction(s) their personal data may fall. Moreover centralised control of this data by the cloud provider makes the data subject to computer-based algorithms which may reveal personal information that users did not want to disclose or were themselves not even aware of. It also leaves their personal data open to correlation by the cloud provider and the cross-referencing of the data within third party databases. Data stored in the cloud may also be subject to a court order, subpoena or discovery in any jurisdiction where the cloud provider employs staff or possesses assets. Particularly for large transnational companies acting as cloud providers, the number of governments able to request access data that is stored in the cloud can be expected to be very high.

Many of these issues could be remedied by providing strong encryption to users of services provided in the cloud, both in transit and where the data is stored. Such measures would ensure that only the user has access to their own personal data. However at present very few cloud providers offer this level of strong encryption of data – both in transit and while being stored in the cloud. At the same time there is an ongoing debate in the Internet community whether cloud providers are trustworthy. As some of the largest providers of email services continue to store personal information in the cloud without encrypting personal data, the suspicions of the Internet community do not seem unfounded. These suspicions would seem to be confirmed when large Internet services in the cloud are hacked and the amount of personal data becomes clear (see inset below for further details).

(V) 85% of Internet users' personal data lost in the Republic of Korea

In mid-2011 citizens of the Republic of Korea experienced by far the largest loss of personal data in the country's history. SK Communications Co. informed the public that personal information of 35 million customers had been hacked, with personal data stolen mainly from its Cyworld social networking site and its Nate search engine, two of the largest websites in the Republic of Korea. Personal information included user names, passwords, social security numbers, resident registration numbers, names, mobile phone numbers, email addresses and personal photographs.[66] According to the ITU there are approximately 40 million Internet users in the Republic of Korea which suggests that more than 70% of the

65 ibid.

66 Sung-jin, Y. (2011). 35m Cyworld, Nate users' information hacked. The Korea Herald. Retrieved December 13, 2011, from http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110728000881.

Korean population or almost 90% of all Internet users in the Republic of Korea had the personal information they stored in the cloud stolen.[67] Before the attack the the Republic of Korea's government had a 'real name' policy, which forced users of large websites to use their real names and provide their social security number to prove their identity, however the government announced that this policy would be changed following the attack and it was eventually struck down by the Korean Constitutional Court in August 2012. Nevertheless, the massive shock of the data breach in the Republic of Korea is a cautionary tale for the Internet industry where oligopolistic control of personal data is becoming increasingly normal.

In many situations, Cloud Computing providers are vulnerable to decisions made by Internet intermediaries. Regardless of the degree of protection promised by the cloud provider in their terms of service, the security and confidentiality of personal information is ultimately determined by the weakest link in the chain. As several intermediaries are typically involved in the transfer and storage of personal information in the cloud; only one of them needs to fail either intentionally or unintentionally for private information to be disclosed.[68] At the same time cloud providers are also vulnerable to governmental surveillance programs. This is because they transfer large amounts of personal data across the public Internet in order to store it in the cloud and in many cases may continue to transfer it across the public Internet between different parts of the cloud. These procedures make it almost impossible for an end user to say with absolute certainty across which jurisdictions their personal data will be routed. Consequently it also becomes very difficult for users of cloud computing to ascertain which governmental surveillance programs their data may be subject to.

Finally there are many unresolved legal issues regarding the protection of personal data in the cloud. As "the cloud may have more than one legal location at the same time, with differing legal consequences,"[69] it remains unclear how cloud providers will react in a specific context. Cloud computing is not inherently incapable of protecting personal data. However a business model, which is based on centralising personal data on a data processing platform across a distributed communications network, is going to raise significant questions about the protection of personal data.

2.2.2 Search engines

Search engines have historically served an important function on the Internet by helping users navigate the vast resources available online. Like many Internet services they are provided as a free service, with a business model based on advertising. In these business models, users do not pay monetarily but by providing their data and by viewing advertising based on this data. The better and more complete the personal data is, the more effective the advertising provided can be. Consequently it does not seem unreasonable to suggest that search engines on the Internet are geared towards collecting as much personal data as possible due to their business model.

---

67 Telecommunications Research Centre. (2011). World telecommunication. Geneva: ITU.

68 Filippi, P. de. (2011). Notes on Privacy in the Cloud.

69 Gellman, R., & World Privacy Forum. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Retrieved from http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

Internet search engines have often expanded their services to encompass other types of services such as email or picture sharing which can be provided to users. These additional services allow search engines to cross reference information between different services and thereby build more complete user profiles. While an integration effect makes the multiple integrated services easier to use and more valuable for users, they are also paying increasingly with their personal data by providing a 360 degree view of their personal lives. A similar conflict already exists in regard to customisation, where search engine users give up some of their privacy for a greater customisation of search services. Here, the value of the service may rise, but the user 'pays' for this improved service by sacrificing a little bit more of their personal data.

Another notable development has been the rise of so-called 'national search engines' in China, the Russian Federation and other parts of the world. These search engines have challenged the dominant international search engines with particular success in certain parts of the world, but there is substantial concern in the Internet community about their privacy practises. While transnational actors may be prepared to challenge more user restrictive privacy practices in different parts of the world, national search engines are bound to their key local markets. This leaves national search engines at the mercy of national regulatory frameworks in their respective local markets. Insofar as these are highly protective of privacy, this could be seen as a positive development, but this is generally not the case. At the same time there are also signs that 'competition based on privacy' may slowly be developing among search engines. Through a mixture of user, civil society and regulatory pressure, some search engines have begun to innovate in the area of privacy policies.[70] This is an encouraging sign, as it may be hoped that competition between search engines is driving an overall improvement in privacy policies. Yet it is unclear whether the associated practices of search engines are actually changing. Much of the information about privacy policies provided by search engines remains difficult to assess and hard to verify.

Still, search engines are consumer-facing businesses, which rely on user and customer trust in order to function. A substantial loss of trust could have immediate direct consequences on the ability of search engines to exist and operate profitable businesses. Insofar it can be hoped that as the search market increasingly matures, there will be ever-greater competition among search engines to actively demonstrate their commitment to user privacy. This is not to say that lock-in effects do not exist and users may become increasingly dependent on search engines. Certain functions of search engines such as speed, linkage to social networks or email accounts are likely to be seen as part of the search experience by consumers and will be increasingly expected from other providers of search engines, raising the bar for other entrants to the search engine market. At the same time lock-in effects seem heavily dependent on habitual search practises, which could be changed relatively quickly if a significant breach of trust becomes apparent.[71] Trusting search engines in many ways replaces a closer understanding of whether or not

---

70 Cooper, A. (2007). Competing on Privacy. Center for Democracy and Technology. Retrieved December 13, 2011, from https://www.cdt.org/blogs/alissa-cooper/competing-privacy.

71 See and Banwell, L., Ray, K., Coulson, G., Urquhart, C., Lonsdale, R., Armstrong, C., Thomas, R., et al. (2004). The JISC User Behaviour Monitoring and Evaluation Framework. Journal of Documentation, 60(3), 302-320 and Griffiths, J. (n.d.). Student searching behaviour and the web: use of academic resources and google. Library trends, 2005, vol. 53, no. 4, pp. 539-554, The Johns Hopkins University Press.

Internet content is relevant and trustworthy.[72] As media literacy slowly grows among the general population it could be hoped that dependence on search engines will lessen the current lock-in effect, thereby increasing competition on other key issues such as privacy.

2.2.3 Social networks

While the noted lock-in effects to certain search engines and their associated services are important, these effects may be even greater on social networks (see inset below for further details). If it is true that "Facebook may well have succeeded in becoming irreplaceable for many of its users,"[73] then this has substantial implications for privacy on the Internet. It makes users vulnerable to unilateral changes made by Facebook and also other social networks to their privacy policies and privacy practises. Users are sufficiently locked-in to the social network that even if they fundamentally disagree with social network privacy policies, they are unlikely to leave the network. This substantially increases the leverage of the social network over their users' privacy.

Like search engines, the business model of social networks is based on advertising and there is generally no direct financial relationship between users of social networks and the social networks themselves. However social networks take this logic one step further than search engines, as the content they produce is also contributed by users. As almost all of the content provided by the users of social networks is personal information and private data, it does not seem unreasonable to suggest that the users of social network are exchanging their private data in return for a 'monetarily free' service. Contractual financial relationships do, however, exist between the social networks and their advertising partners, who are responsible for funding the network. As a result, social networks have a natural business incentive in consistently improving the targeting of their advertising with the help of their users' personal data. While there may also be other means of generating revenue within social networks through subscription models or transaction models, the most important revenue stream for most large social networks remains advertising revenue.[74] Consequently the personal data of the users of social networks is still the key currency, a critical mass of which needs to be obtained in order for social networks to remain profitable.[75]

---

72 See Shaker, L. (2006, April 3). In Google we trust: Information integrity in the digital age. First Monday. Ghosh, Rishab Aiyer. Retrieved from http://frodo.lib.uic.edu/ojsjournals/index.php/fm/article/view/1320/1240 and Hargittai, E. (2010). Trust online: young adults' evaluation of web content. International Journal of Communication, 4.

73 York, J. C. (2010). Policing Content in the Quasi-Public Sphere. Boston, MA: Open Net Initiative Bulletin. Berkman Center. Harvard University.

74 For an extended discussion of social networking funding models see Enders, A., Hungenberg, H., Denker, H.-P., & Mauch, S. (2008). The long tail of social networking. Revenue models of social networking sites. European Management Journal, 26(3).

75 Mueller, P. (2011). Offene Staatskunst – Strategie für eine vernetzte Welt. Arbeitskreis Internet Governance. Munich, Germany: Münchner Centrum für Governance-Forschung (MCG).

(VI) The power of lock-in

"Having one place where we do all our communication leaves us at the mercy of the policies of the people who control the infrastructure we are chained to, that we are stuck using that we are locked into – You can't leave Facebook without leaving everybody you know – because everybody you know is on Facebook. I was not a Facebook user, I was against Facebook. I thought it was bad to centralise all our communication in one place. I didn't like the privacy implications. I didn't like Facebook's censorship of things like pictures of nursing mothers [...] I thought those were bad policies and I reacted to that by not joining Facebook for years while all my friends were on Facebook [...] I joined Facebook late last year [...] Because a friend of mine passed away. His name was Chuck, a brilliant man and he lived a lot of his life online. He was on Facebook and he shared things with his friends on Facebook – and when he passed away I realised that I hadn't communicated with him in a while [...] I wasn't meeting him where he was, I wasn't on Facebook. I was missing out on something huge. That's the cost of not being there – and so I joined because I decided that as strong as my beliefs were, it was more important to me to be there with my friends and to talk to my friends. That's the power of lock-in."[76]

It is often argued that users of social networks explicitly consent to these uses of personal data in the terms of service and privacy policy. While this argument may shield social networks from legal liability, 'meaningful' or 'substantive' consent would assume that users were (1) aware of the privacy policy, (2) able to understand the complex legal language used within these policies and (3) willing to spend time reading these policies (4) able to accept certain parts of the privacy policy while rejecting others. Even were users to do so, however, privacy policies can be changed at any time, making even the most informed user vulnerable to sudden, unexpected and unilateral changes in privacy by the social networking providers.[77] It has been suggested that this complete volatility in dealing with private data is as "if tenants had no rights to privacy in their homes because they happen to be renting the walls and doors. This week, you are allowed to close the door but, oops, we changed the terms-of-service."[78]

Equally there are issues associated with the 'publicness' practised in social networks that extend far beyond the actual social networks themselves. It has become common practise for automated programs to 'mine' publicly available personal data on social networking sites. Consequently it can be sufficient for personal data to be publicly available only for a short period of time before it is already distributed onto many other sites, online spaces

76 Vasile, J. (2011). Presentation of the FreedomBox. Elevate 2011 – Music, Arts and Political Discourse. Graz, Austria: Verein zur Förderung des gesellschaftspolitischen und kulturellen Austausches.

77 Electronic Privacy Information Center. (2011). Social Networking Privacy. Retrieved December 13, 2011, from https://epic.org/privacy/socialnet/.

78 Tufekci, Z. (2010). Facebook: The Privatization of our Privates and Life in the Company Town. Technosociology: Our Tools, Ourselves. Retrieved December 13, 2011, from http://technosociology.org/?p=131.

and technical systems.[79] While this risk may exist analogously for other Internet services as well, the sheer amount of personal data stored on social networking sites makes the risk of inadvertent public exposure of private data far greater than for other comparable services. These problems are exacerbated by the day-to-day operations of many social networking sites that are typically driven by computer scientists and engineers. In this context, products and services are developed following an engineering logic of providing customers with the most advanced new products and a privacy policy is then bolted-on at the last minute. Throughout the research conducted for this report, this internal organisational dimension within social networks kept reappearing as an important barrier towards providing greater privacy protections for users.

2.2.4 Mobile phones, smartphones and the mobile Internet

The explosion of the use of the mobile Internet in the 21st century has contributed to many of the existing concerns about privacy and data protection on mobile phone networks. In comparison with fixed line communications, mobile communications have several attributes which have a particularly negative effect on privacy. These include unique mobile device (IMEI) and SIM card (IMSI) identifiers, the ability to regularly ascertain the approximate geographic location of mobile device and the ability for third parties to intercept wireless mobile communications as they travel through the air.[80] These privacy concerns specifically related to the mobile Internet all need to be considered in addition to existing concerns about privacy on the Internet which all also apply to mobile Internet devices.

While it is frequently assumed that these concerns are only relevant for 'Smart Phones', they apply in equal measure to any mobile device which is capable of accessing the Internet through mobile phone networks. Consequently these privacy concerns need to be considered in the developing and the developed world for any device which is capable of accessing the Internet. They apply both to a farmer in Zimbabwe sending emails to his family on an old Nokia phone, as they do to a corporate lawyer in Hong Kong using an iPhone to send an email to a client. While these concerns already exist in regard to mobile telephony in general, they are further exacerbated by the use of the Internet on mobile devices.

However, beyond specific privacy concerns with mobile networks themselves, smartphones also raise additional privacy issues in comparison to 'less smart' mobile phones, often termed 'feature phones.' Smartphones are generally used as mobile Internet devices and are typically able to transfer far greater amounts of data than normal mobile phones through what are known as second (2G), third (3G) or fourth (4G) generation mobile networks. This means that they are also capable of transferring far more personal data onto the public Internet than a typical mobile phone. Furthermore, these phones are designed to be 'always on' the Internet. Moreover, a variety of services are built into smartphones, which regularly send data across the Internet, often without knowledge

---

79 For an overview of problems and solutions see Fuchs, C. (2009). Social networking sites and the surveillance society a critical case study of the usage of studiVZ, Facebook, and MySpace by students in Salzburg in the context of electronic surveillance. Salzburg: Forschungsgruppe Unified Theory of Information.

80 Electronic Frontier Foundation (EFF). (2011). Mobile Devices. Surveillance Self-Defense Project. Retrieved December 13, 2011, from https://ssd.eff.org/tech/mobile.

of the user of the phone. It has been documented that both Google Android and Apple iPhone smartphones regularly 'phone home', thereby transferring information about their location, their user and other potentially personal information such as Wi-Fi networks in range across the Internet.[81]

This further contributes to the overall trend in smartphone privacy, namely the fragmentation of control of personal data in mobile Internet platforms. The mobile Internet service provider, device manufacturer, operating system provider and app providers all have a certain level of control over user personal data. In the case of a typical smartphone user sending emails in Argentina, some of their personal data would conceivably be controlled by their mobile Internet device manufacturer (Samsung), mobile operating system provider (Google), mobile Internet service provider (Movistar), their email App (K-9 Mail), their email service provider (Yahoo) and the email service provider of the individual they were sending the email to (Microsoft). This does not even include data leakage issues when passwords and email content are sent unencrypted across Internet, potential additional access to personal data by local or international law enforcement or unauthorised third party access to personal data. Nor does it begin to consider the additional layer of complexity introduced by the installation of additional smartphones applications ('Apps'), which may also have access to users' personal data. Moreover smartphones combine a wide array of different sensors and communications chips and platforms, making it difficult for smartphone users to understand the privacy implications of each additional sensor or specific communications chip. The most recent iPhone4S includes communications chips capable of communicating across different types of mobile phone networks (GSM/CDMA/EDGE/ UMTS/HSDPA/HSUPA), 'Wi-Fi' wireless Internet networks (802.11b/g/n), GPS global positioning systems and Bluetooth technology, as well as a light censor, a proximity sensor, a movement sensor known as a gyroscope and multiple microphones.[82]

(VII) Internet devices storage exploited

In many repressive states across the world it is standard practise to force political prisoners who have been arrested to hand in their Internet-connected devices before being questioned. The authorities are particularly interested in smartphones, as these carry a great deal of additional private data not normally available on normal mobile phones. This personal information is then used to systematically gather information on the social networks that political prisoners inhabit. With this information other direct and indirect contacts of political prisoners can be targeted. These networks include the personal, professional and coincidental networks of individuals, who are themselves intimidated or imprisoned for little other reason than having – however briefly – met the wrong person. These methods do not necessarily solve any legitimate governmental purpose; rather they serve to intimidate individuals and their personal networks. They can be engineered to produce chilling effects and spread the shadow of state hierarchy far beyond

81 Angwin, J., & Valentino-Devries, J. (2011). Apple's iPhones and Google's Androids Send Cellphone Location. Wall Street Journal. Retrieved December 13, 2011, from http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html.

82 Higginbotham, S. (2010). iPhone 4 Sensors Highlight a Bright Spot for VCs. GigaOM. Retrieved from http://gigaom.com/2010/06/08/iphone-4-sensors-highlight-a-bright-spot-for-vcs/.

political prisoners themselves. Personal communications devices and the personal data they digitise and collect are fundamental to such intimidation strategies.

These sensors can be combined in unexpected ways, such as recent attempts to create a record of user typing using the gyroscope movement sensor.[83] Much of the data collected on smartphones is stored on the phone for an unspecified amount of time, with little user control over its existence or removal. Depending on the extent to which smartphones are used, smartphones can quickly become complete digital repositories of the lives of their owners. This means that if smartphones are lost, stolen or simply taken from their owners, the implications for the privacy of individuals can be severe (see inset for further details).

Finally the two dominant smartphone platforms, Google Android and Apple iPhone, also use their respective mobile platforms to target advertising at users. In many cases the data these companies have obtained about users from other Internet devices – through their Google search history, ITunes Store purchasing history, Apple/Google account usage history or similar – can be combined with data provided by the mobile platform such as geographic location data from the phone. This personal information about an individual – which may in many cases be more extensive than what the users know themselves – allows these platforms to target highly personalised advertising at their users. As with search engines and social networks, the developers of mobile Internet platforms have a business interest in getting as much personal information as possible from their users. The more they know about their users, the more valuable the targeted advertising shown on mobile Internet platforms is likely to be.

2.2.5 Unique citizen identifiers and eGovernment initiatives

Long before the public Internet came into being in the early 1990s, governments across the world have moved to standardise and centralise records about their citizens. As computing power increased and became cheaper, states were able to make increasing efficiency gains within their bureaucracies by centralising and standardising information about citizens.[84] In accordance with the views of James C. Scott, states have sought to make the societies they govern 'legible' in order to promote their policies.[85] They also serve to respond to persistent demands on public bureaucracies to cut costs by increasing efficiency through computerisation. These efficiency gains have often had the effect of negatively impacting on citizens' privacy and anonymity. Public initiatives to create large public databases about citizens have been met with scepticism by privacy advocates. The dangers of such databases are particularly evident when the information is lost (see inset for further details).

Such databases and identification services often include an online component, allowing citizens to access various government services via the Internet. Use of these services

83 Cai, L., & Chen, H. (2011). TouchLogger: inferring keystrokes on touch screen from smartphone motion. HotSec'11 Proceedings of the 6th USENIX conference on Hot topics in security. Berkeley, CA, USA: USENIX Association.

84 For a discussion on the importance of computing to modern states and societies see Robertson, D.S. (1998) The New Renaissance: Computers and the Next Level of Civilization. Oxford University Press, United States of America.

85 Scott, J.C. (1998) Seeing like a state : how certain schemes to improve the human condition have failed. New Haven: Yale University Press.

may provide many benefits to citizens, such as greater convenience and efficiency. But as has been noted by a US Government Privacy Working Group:

> "These benefits, however, do not come without a cost: the loss of privacy. Privacy in this context means 'information privacy,' an individual's claim to control the terms under which personal information – information identifiable to an individual – is acquired, disclosed and used."[86]

(VIII) Loss of 25 million citizens' personal data

One of the largest losses of citizen data in Europe occurred in the United Kingdom of Great Britain and Northern Ireland, where two CDs containing personal data of more than 25 million individuals were lost in the internal government postal system in 2007.[87] They were sent without any technical protection mechanisms from the British Revenue and Customs service (HMRC) to the National Audit Office (NAO). Furthermore, the level of actual governmental control over the transport of the CDs is questionable, as the transport was conducted by a private courier service. The personal information on the CDs was related to child benefits payments to all families in the UK. As the vast majority of families in the UK claim child benefits, the personal data loss affected almost all families with children under 16. It has been suggested in the UK that the majority of large scale personal data losses have taken place in the public sector.[88] This is typically attributed to a lack of "success in fostering a culture of security for personal data,"[89] both online and offline.

This prescient statement describes precisely the difficulty in ensuring that eGovernment is both effective and guarantees privacy. This tension can also be found in more recent forms of eGovernment. Typically these initiatives attempt to increase participation of citizens and the transparency of government operations, however here too there may be privacy concerns. For one, users participating in these initiatives are typically required to identify themselves as citizens in participative government initiatives, as non-citizen participation is typically not possible. Moreover they are expected to participate in these initiatives with their 'whole identity.' Anonymous or pseudonymous participation – even for individuals identified as citizens – is generally not an option.

Another important point is the tension between transparency and openGovernment or participatory government initiatives and privacy. Most participatory governmental initiatives require high levels of transparency to ensure the legitimacy of the process. However by doing so they run the danger of overly restricting the rights of individuals to

---

86 Gates, J., & Privacy Working Group. (1995). Privacy and the National Information Infrastructure: Principles for Providing and using Personal Information. Information Policy Committee, Information Infrastructure Task Force. Retrieved from http://aspe.hhs.gov/datacncl/niiprivp.htm.

87 Gorge, M. (2008). Data protection: why are organisations still missing the point? Computer Fraud & Security, 2008(6), 5-8.

88 Privacy International. (2011). United Kingdom – Privacy Profile. Privacy International. Retrieved December 13, 2011, from https://www.privacyinternational.org/article/united-kingdom-privacy-profile.

89 Ibid.

their personal data in order to safeguard transparency. Requiring citizens to sign petitions or participate in openGovernment using their real name solves authentication problems for the government using the system, but leads users to speak less openly than if they were speaking anonymously or pseudonymously through a trusted third party.

Finally, it is important to consider the close cooperation with the private sector in many eGovernment and openGovernment initiatives. As governments often do not have the capacity to perform these functions themselves, they frequently outsource processes and services integral to modern governments to private service providers. While this may be an effective way of cutting costs, it also provides additional privacy risks by involving third parties in the processing, transfer and storage of citizens' personal data. These interactions with the private sector do not necessarily harm citizens' privacy, but they do introduce an additional layer of complexity that needs to be governed appropriately.

2.3 Threats posed by different mechanisms of surveillance and data collection

2.3.1 User identification – unique identifiers, cookies and other forms of user identification

There is an enormous array of different ways in which Internet users are identified. From initial registration of Internet users through Internet service providers or at Internet cafes, to numbering and identification of Internet devices which are themselves often linked to Internet accounts, to individual IDs which are provided by browsers or stored as cookies, as well as the IP-Addresses which are assigned to Internet users through Internet protocols. All of these identification procedures may serve to make an Internet user less anonymous, but in some cases these identities may also be necessary for provision of services on the Internet. It is difficult to use the Internet without an IP-Address – although of course an IP Address can be assigned dynamically or anonymised – and many other Internet services rely on some form of identification.

Particularly in the developing world, but also in some parts of the developed world, Internet user registration, for both short and long term Internet usage, constitutes one important privacy concern. User identification may take place as part of registration procedures for an Internet café, as part of the signup procedure to a wireless network or during the purchase of a mobile phone contract. In each of these contexts, Internet user identification mechanisms contribute to restricting privacy and anonymity on the Internet. Another cause for concern is the resulting restriction of anonymous speech and the chilling effects that such identification mechanisms bring with them. Admittedly these identification procedures are at least relatively transparent to Internet users, which cannot be said for other user identification mechanisms.

Of the less transparent user identification mechanisms, cookies are perhaps the best-known. These are stored on the computer of an Internet user when they visit a website, and the user's Internet browser. Depending on how this website is constructed and the settings of the Internet user's browsers, anything from one to a dozen cookies can be stored or updated when visiting a website. By storing cookies on users' computers, each user can be tracked across the Internet. Particularly in the case of cookies which are set outside of the domain which the user is visiting – so-called third party cookies – these cookies can 'follow' users across most parts of the Internet.

Cookies also form a component of user analytics, a common practise for user tracking across the Internet. Credible estimates suggest that between 40 and 60% of the largest Internet websites use Google Analytics, a traffic tracking tool that allows website administrators to gauge their traffic.[90] Of all Internet websites, similar estimates suggest that close to 70% use some kind of user tracking based on various different Internet analytics packages.[91]

Technical implementations of cookies have long evolved beyond the point where users have any meaningful control over being tracked by them. Cookies are often set for years on a user's computer and are extended automatically each time the user visits an associated website. They can also be set by browser add-ons such as the 'Adobe Flash' independently of the main browser. Should a user attempt to remove their cookies from one of the many locations in which they can be stored, they are recreated from other storage areas or using other identification mechanisms such as session IDs, browser add-ons, cookie caching scripts or any number of other methods which allows for cookies to be recreated without the consent of individual users.[92] Although there were extensive debates about the privacy concerns associated with cookies relatively early in the evolution of the public Internet, many of the associated issues have yet to be resolved.[93]

Cookies are, however, just one of many components of user identification on the Internet. They are driven by the advertising-funded model which permeates much of the Internet and thrives on the identification of users for the purpose of targeting advertising. While website customisation and more relevant advertising are frequently mentioned as incentives for users to accept or even support Internet tracking, the fact that users are tracked across the Internet follows a clear profit motive. Fierce responses by the Internet advertising industry to recent DoNotTrack legislation in different parts of the world are just another example of such business interests.[94] While a substantial part of the Internet industry relies on advertising revenues for funding, finding ways of avoiding privacy-invasive user identification and tracking online will remain highly challenging.[95]

2.3.2 Adware, spyware and malware conduct covert data logging and surveillance

Further threats to the privacy of users on the Internet arise from adware, malware and viruses. In some cases these programs collect personal user information for criminal purposes, such as stealing money from individuals, hijacking their Internet accounts or otherwise misusing their personal information. Another prevalent use of spyware is the user who wishes to covertly observe other users he or she knows personally. This 'spyware'

---

90 BuiltWith. (2011). Google Analytics Usage Statistics - Websites using Google Analytics. Retrieved December 13, 2011, from http://trends.builtwith.com/analytics/Google-Analytics.

91 W3Techs. (2011). Usage Statistics and Market Share of Traffic Analysis Tools for Websites. Q-Success Web-based Services. Retrieved December 13, 2011, from

92 Mayer, J. (2011). Tracking the Trackers: Microsoft Advertising. Center for Internet and Society (CIS), Stanford Law School. Retrieved December 13, 2011, from http://cyberlaw.stanford.edu/node/6715.

93 Further details can be found in RFC 2109: https://www.ietf.org/rfc/rfc2109.txt.

94 Clarke, G. (2011). Do-Not-Track laws gain US momentum. The Register. Retrieved December 13, 2011, from http://www.theregister.co.uk/2011/05/06/senate_do_not_track/.

95 Rooney, B. (2011). U.K. Publishes EU "Cookie" Directive Guidelines. Wall Street Journal. Retrieved December 13, 2011, from http://blogs.wsj.com/tech-europe/2011/05/09/u-k-publishes-e-u-cookie-directive-guidelines/.

is often used by stalkers, who wish to invade the personal lives of their victims. It may include relaying details of the individual's physical location, their communications, other personal information and passwords.[96] What is perhaps surprising is that it is completely legal to buy and sell these technologies in many parts of the world. It is therefore relatively easy for individuals wishing to misuse these technologies to gain access to them.

Adware also fits into the category of privacy-invasive and consent-ignoring software, which is inadvertently stored on computers. This software is very difficult for users to recognise, as the software tends to masquerade as an anti-virus program, a search tool or a similar 'useful' technology that the user would want to use. It is often also bundled with software that seems to be free. However it is instead used to show unwanted advertisements to the user and track their computing behaviour.

Increasingly relevant in this context are law enforcement authorities using Trojan horse technology to gather information from remote computers. Such uses have been the subject of great controversy in many parts of the world, as they frequently involve taking over the entire computer. This technology is then used as a form of so-called 'legal intercept'; however civil society considers it malware while vendors of antivirus software classify it as a virus.[97] Such uses leave little room for private personal data, which is stored on computers, even though this space of 'deep intimate personhood' is explicitly protected as an important part of human dignity in many jurisdictions across the world. Finally malware, spyware and adware are increasingly being targeted at converged mobile devices such as smartphones, tablets and other Internet connected devices such as smart TVs. Here, it is the users' expectation that they are safe and have no requirement for any additional protection which is exploited. Having your personal data lost through a device which is not obviously a personal computer is frequently unexpected (see inset for further details).

The various different communications protocols used by these devices allow for many different distribution mechanisms for malware. A virus downloaded over the Internet via 3G mobile phone signal can be redistributed via Wi-Fi wireless networking or Bluetooth to other devices in the immediate proximity. As common operating systems in mobile devices such as iOS and Android proliferate, it becomes easier for these devices to spread malware to devices with similar operating systems. The multiple communication methods and unclear security procedures make new Internet devices an obvious target for malware and adware. As the number of devices connected to the Internet grows rapidly, from gaming consoles to smart televisions, cars, microwaves, fridges, and the "Internet of Things"[98] becomes normality, users find it increasingly difficult to maintain control over their personal data. Internet-connected cars and televisions do not typically provide privacy settings or allow users to install an anti-virus program or a firewall. These developments pose serious challenges for user privacy and individuals' ability to exercise control over their personal data.

---

96 Electronic Privacy Information Center. (2011). Personal Surveillance Technologies. Retrieved December 13, 2011, from https://epic.org/privacy/dv/personal_surveillance.html.

97 Chaos Computer Club. (2011). Chaos Computer Club analyzes government malware. Retrieved December 13, 2011, from http://ccc.de/en/updates/2011/staatstrojaner.

98 Gershenfeld, N., Krikorian, R., & Cohen, D. (2004). The Internet of Things. Scientific American, 291(4), 76-81. Springer.

(IX) Gaming console network hacked

In April 2011 the Sony 'Playstation Network' which is linked to the Sony Playstation console was broken into by unknown attackers. As a result it has been suggested that the personal data of 77 million users of the Playstation Network has been compromised, including their name, address, country, email address, date of birth and credit card number as well as the login, password and password security answers used in the network.[99] Aside from the scale of the personal information stolen, it took over a week for Sony to inform users of the network that their personal data was at risk. As the use of the same password across multiple Internet sites is common, this left users of the Playstation Network not just at risk on the network itself but across the Internet.

2.3.3 Deep packet inspection (DPI)

Deep packet inspection technology is pervasive and used as a generic Internet control technology in many parts of the Internet. The technology itself has the capacity to 'look inside' packets which travel through the Internet, inspect their content and react to the content in various different ways. Historically, technologies that scan and sometimes modify Internet traffic have only done so on the basis of their header information. By contrast, deep packet inspection looks 'inside' the packet and scans it for certain keywords, patterns or other attributes that are not evident from studying the packet header.[100] While DPI combines "many features of internet technologies that have been around for a long time [...] the combination of these elements into a scalable, widely implemented set of practices is generally seen by industry, technologists and policy critics as a new technology."[101] It is also a technology that has been mired in controversy since the first public debates about it began. During these debates, the technology was associated with some of the greatest invasions of privacy on the Internet. One DPI vendor – when asked during an interview conducted by the author what it was like selling DPI equipment – suggested that it was like having a sexually transmitted disease.

Two of the first uses of deep packet inspection technology which garnered significant public attention were targeted advertising by Phorm and NebuAd. The technology was used to build extensive advertising profiles about the users of several Internet service providers and in some cases even went as far as to insert additional adverts into websites. This active manipulation of users' websites and collection of their data without their consent caused such a scandal that it was eventually abandoned by the Internet service

99 Stuart, K. (2011). PlayStation Network hack: what every user needs to know. The Guardian. Retrieved December 13, 2011, from http://www.guardian.co.uk/technology/gamesblog/2011/apr/27/psn-security-advice.

100 For an extensive discussions of types of Deep Packet Inspection technology see Mueller, M. (2011). DPI Technology from the standpoint of Internet governance studies: An introduction. Syracuse University. Retrieved from http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf.

101 Mueller, M. (2011). DPI Technology from the standpoint of Internet governance studies: An introduction. Syracuse University. Retrieved from http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf.

providers involved and became part of legal proceedings.[102] It also did little good to the public perception of deep packet inspection technology, which has since been closely associated with violations of privacy in public debates. In the context of widespread public protests in the Islamic Republic of Iran and the MENA region in 2009, 2010 and 2011, deep packet inspection technology was also widely reported as being used by the government to monitor and censor their citizens.[103]

Since these initial reports, there has been continued publication of well documented evidence linking deep packet inspection technology to some surveillance regimes in the MENA region. Beyond the MENA region deep packet inspection is commonly part of governmental surveillance systems, which are sometimes termed 'lawful intercept.' They effectively make all unencrypted information passing through communications networks visible to the operators of the equipment, allowing them to store and in some cases even modify the information in the network.[104]

Another common use of deep packet inspection technology is to profile users on communications networks. While it is unclear how extensive this profiling is, it is clear that it takes place for commercial purposes. However in some cases, these profiles can just as well be used for advertising purposes to target particularly relevant advertisements at users of the network. Another potentially privacy invasive form of DPI-usage is the filtering of content on the Internet, typically because it is considered illegal. In many cases this also allows for the monitoring of users who wish to access filtered content.

Notably DPI can be used for bandwidth management by ISPs, to block spam at a network level and to protect ISPs from certain types of Internet attacks. In this sense it is not as 'inherently bad' as some of the public debate suggests, but it does pose significant ethical questions when implemented. Some vendors have attempted to mitigate these problems by developing types of 'privacy by design' for DPI, although these developments are still at an early stage.[105] In the context of ethical questions regarding privacy, deep packet inspection's status as a generic communications control technology does lend itself to misuse in many different contexts. As the DPI industry matures, it remains to be seen how different companies within it will position themselves to these potential misuses of DPI technology and how possible convergence between different DPI usages affects the industry as a whole.

---

102 European Commission. (2010). Digital Agenda: Commission refers UK to Court over privacy and personal data protection [IP/10/1215]. Retrieved December 13, 2011, from http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215.

103 See Silver, V., & Elgin, B. (2011). Torture in Bahrain Becomes Routine With Help From Nokia Siemens. Bloomberg. Retrieved August 28, 2011, from http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html and Sonne, P., & Coker, M. (2011). Foreign Firms Helped Gadhafi Spy on Libyans. Wall Street Journal. Retrieved September 23, 2011, from http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html.

104 European Commission. (2010). Digital Agenda: Commission refers UK to Court over privacy and personal data protection [IP/10/1215]. Retrieved December 13, 2011, from http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215.

105 This is based on interviews by the author in July 2011.

2.3.4 Pervasive geo-location technology: an emerging threat to Internet privacy

Historically geo-location data has been an integral part of the Internet. Systems with the ability to locate Internet users with a relatively high degree of accuracy have been used for both advertising and legal purposes. These services provide a geography location of the IP addresses of Internet users and allow ISPs to develop a relatively accurate estimate in which country a user is located and in many cases even in which city. As Internet usage has increased and data on Internet usage has increased, so too has the precision of these services and thereby the ability of websites and intermediaries to geographically locate Internet users.

However technical developments in Internet connected devices have meant that many Internet users now have GPS location technology attached. This technology is far more precise, allowing for a specification of the physical location of an Internet user within a few meters. At the same time it is embedded in numerous different devices and users are typically not aware of the consequences that activating or deactivating the function may have on their privacy, which programs or applications have access to GPS location information.

The provision of GPS information is driven by several online business models. Users of FourSquare and Facebook are actively encouraged to provide location information when they visit the website, primarily as a social function. This is also common in other forms of social networks such as 'CouchSurfing', whereby the location provided here is generally less precise than FourSquare or Facebook. Notably these are all social networking sites in some shape or form, but for FourSquare and Couchsurfing it could perhaps be argued that providing location information is inherently part of the concept of the network. Users expect when joining these social networks to have their private information shared and may even be joining precisely for this reason. This argument would seem less evident in the case of Facebook.

Geo-location systems clearly raises issues related to user consent and control over their personal location data. Users have little control over the actual users of their data and forms of data processing, which can make informed consent particularly difficult. Moreover, geo-location data is heavily processed and may – as discussed above – be generated out of other information the user provides without the users' knowledge or consent of this process. Furthermore, geo-location via GPS systems built into handsets are also technically far more precise than the geo-location of mobile masts, creating a far more precise picture of the movements of an individual.

Geographic location data collected in this manner can then be used to create a movement profiles of individuals. One of the most evocative recent examples is Malte Spitz, a German Green politician who sued his mobile phone provider in order to gain access to his private data in order to understand what they knew about his movements. The data he received was later visualised by a German newspaper and represents a complete movement profile over months of his life, some of which was published online to demonstrate the scale of the problem.[106] Clearly, while geo-location technology and services are still developing massively, it is hard to say how its on-going developments will affect privacy on the Internet. Yet a cautionary glance at some of the issues geographic location information

106 Biermann, Kai. 2011. "Data Protection: Betrayed by our own data." ZEIT Online. Retrieved March 1, 2012 (http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz).

is already being used for suggest that – while geo-location is an emerging issue – there are unlikely to be 'quick fixes' for many of the problematic privacy issues associated with geo-location.

2.3.5 Data processing and facial recognition

"Facial recognition technology (FRT) has emerged as an attractive solution to address many contemporary needs for identification and the verification of identity claims. It brings together the promise of other biometric systems, which attempt to tie identity to individually distinctive features of the body, and the more familiar functionality of visual surveillance systems."[107]

(X) Reprocessing faces

In order to demonstrate the dangers associated with publicly sharing information, a group of artists downloaded over a million publicly available Facebook pictures, associated personal information and relationships.[108] They then used this information to categorise faces and (re-)aggregate them on a separate website. While this is a public project designed to raise awareness about the malleability and replicability of public data, there are many other 'Internet bots' which spend their time 'scraping' Internet sites in private and using this information to feed private databases. This also means that accidental choices to publicise information by Internet users can have irreversible consequences, with their data 'scraped' from the website they published it on and replicated within split seconds. Lack of user awareness about the potential scope of their privacy choices and lack of control over their own information once publicly provided (for whatever reason) has substantial negative effects on user privacy on the Internet.

Although there have been extensive debates in recent years on the impact of face recognition technology on an individual's privacy, these debates need to be seen in a wider context. While there are novel aspects to the debate, in many respects face recognition technology represents a new form of data processing and identification.

There are several reasons why advances in data processing can have such threatening effects for the privacy of individuals on the Internet. The first is that they re-contextualise data, processing it into a form that was neither wanted, nor expected or even conceivable. In a different context processed data may have a very different meaning. Indeed this may lead to data processors possessing information about an individual's personal life of which the individual is now aware.

Here, facial recognition technology serves to make what was previously personal data individually identifiable information. The increasing power of face recognition technology is increasingly elevating the face to a unique identifier, which can be linked across private

107 Introna, L. D., & Nissenbaum, H. F. (2009). Facial Recognition Technology: A Survey of Policy and Implementation Issues. SSRN eLibrary. SSRN.

108 Cirio, P., & Ludovico, A. (2011). Face-to-Facebook. Face-to-Facebook. Retrieved from www.face-to-facebook.net/theory.php.

and public profiles across the Internet (see inset for further details). It is increasingly becoming the key token of data linkage and identification. As a result users are only beginning to realise that information they expected to be effectively anonymous may be associated with their online profiles or searchable under their name. In a world where the number of camera lenses is constantly increasing, this can have substantially chilling effects on freedom of expression and an equally negatively effect on privacy.[109]

Face recognition has also been used by law enforcement as part of surveillance operations at large public events, such as the 2001 Superbowl in Florida, United States of America.[110] As similar reports have continued since, there is reason to believe that law enforcement and other public authorities are using similar face recognition technologies on the Internet. Despite widespread doubts about the effectiveness of face recognition technology as a law enforcement tool, continued investment in these technologies by public authorities across the world suggests that the technology is expected to develop rapidly in the near future.[111]

Another development with substantial privacy implications in this context is the significant transfer of personal data between the public and private sector. Personal data which has been pre-processed by the private sector (such as a search profile or social networking history) is increasingly requested by the public authorities.[112] At the same time, personal data such as individual 'intelligence profiles' which are pre-processed by the public sector are increasingly shared with the private sector.[113] This sharing of processed personal data is a large risk to individual control over their personal information. Users of social networks do not expect that the data they have ever entered into a social network, or that profiles of their movement stored by their mobile provider, will be shared with law enforcement. Nor do citizens typically expect that information collected by their intelligence services or law enforcement authorities will be routinely shared with private contractors.

Sharing personal information in both directions has become commonplace on the Internet. Indeed it seems possible to suggest a more general merging of public and private Internet surveillance infrastructure. Intelligence fusion centres, PNR, SWIFT and more generally data retention legislation are just a few examples where private actors collect data which is then used by public actors and vice versa. Here, the overlap of private and public privacy regimes makes it very difficult for individuals to consent to the use of their data by third parties, to know how and under which conditions their data is being stored, let alone be able to withdraw consent from digital storage of their data.

In this context data processing and face recognition technology become part of a wider surveillance infrastructure, which fundamentally threatens privacy. This is driven both by the public sectors' desire to know more about citizens and the private market which

---

109 Padania, S., Gregory, S., Alberdingk-Thijm, Y., & Nunez, B. (2011). Cameras Everywhere Report 2011. Retrieved from http://www.witness.org/cameras-everywhere/report-2011.

110 Privacy International. (2006). Privacy International 2006 – Executive Summary. Retrieved December 13, 2011, from https://www.privacyinternational.org/article/phr2006-executive-summary.

111 Electronic Privacy Information Center. (2011). Face Recognition. (EPIC). Retrieved December 13, 2011, from https://epic.org/privacy/facerecognition/.

112 Google. (2011). Google Transparency Report. Google. Retrieved December 13, 2011, from https://www.google.com/transparencyreport/.

113 Carter, D. L., & Carter, J. G. (2009). The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement. Criminal Justice and Behavior, 36(12), 1323-1339.

has quickly sprung up to satisfy this demand.[114] In conclusion, it seems reasonable to suggest that there has been "an explosion in the dissemination of images, in domains from photo-sharing to surveillance and medical imaging, with a corresponding increase in the potential for privacy intrusive uses of those images. Thus far, controls on the privacy intrusions that these technologies bring have been very limited."[115]

2.3.6 Internet surveillance technology

Moving from data processing and face recognition to the market for such equipment, one of the greatest threats to privacy on the Internet stems from the rise of the Internet surveillance industry. Although Internet surveillance technology is often discussed in the context of Deep Packet Inspection (DPI), the types of technologies used for Internet surveillance technology are far broader. The technologies in use range from software installed on individual computers by law enforcement such as 'Trojan horses', monitoring devices which are attached to computing systems or personal electronic devices, through to surveillance technologies attached to the communications networks linked to these devices.

Of particular concern for privacy are those surveillance technologies which attempt to harness the personal data uploaded and organised by Internet users, thereby typically processing an enormous amount of personal information. Advances in computer processing power have meant that modern Internet surveillance technology is capable of indexing, cross-referencing and profiling the personal user data of individuals. The diversity, scope and usage of Internet surveillance technologies have expanded massively since the beginnings of the public Internet.[116] These technologies are typically provided to governments and large corporations around the world regardless of mistreatment of information privacy or other human rights concerns. The result is a surveillance technology market where companies compete to provide the most privacy invasive technologies. Companies in this market have little or no interest in protecting the privacy of individuals; indeed they have a clear interest in removing user privacy to the greatest extent possible.

The international trade in surveillance technology and services has also increased the transmission of personal data across communications networks. Most modern surveillance technologies are designed to 'phone home', 'report back' or otherwise transmit their findings to their operators. As the operators and technicians are seldom located in the same physical location as the surveillance equipment, personal information being collected by the surveillance devices needs to be transmitted across communications networks to their operators. At the same time many Internet surveillance technologies have the capacity to update themselves across communications networks and may also provide remote access to the surveillance technology vendor. This remote access capability and associated transmission of personal data evidently threatens the privacy of

---

114 Silver, V., & Elgin, B. (2011). Torture in Bahrain Becomes Routine With Help From Nokia Siemens. Bloomberg. Retrieved August 28, 2011, from http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html.

115 Senior, A., & Pankanti, S. (2011). Privacy protection and face recognition. In S. Z. Li & A. K. Jain (Eds.), Handbook of Face Recognition. Springer.

116 King, E. (2011). Our response to EU consultation on legality of exporting surveillance and censorship technology. Privacy International. Retrieved December 13, 2011, from https://www.privacyinternational.org/article/our-response-eu-consultation-legality-exporting-surveillance-and-censorship-technology.

personal data. There are numerous well documented cases of surveillance technologies being compromised by third parties (see inset for an example).

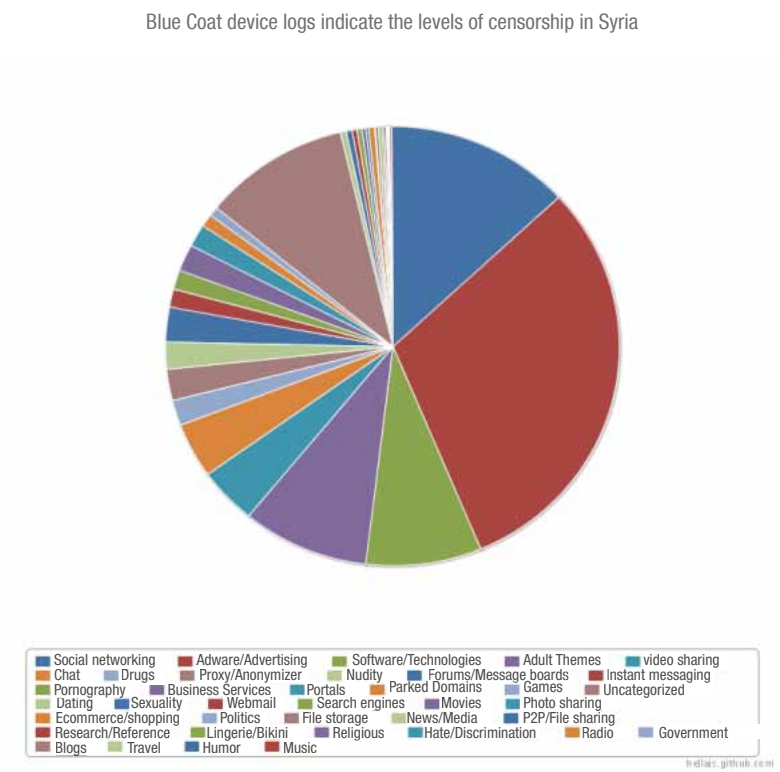
Moreover, the addition of surveillance technologies to technical devices, systems and networks adds an additional layer of vulnerability. These vulnerabilities are particularly pronounced as surveillance technology is designed to extract and prepare personal data for operators. Consequently third party access to surveillance systems is likely to be a far greater threat to privacy than access to the actual devices, systems or networks that are being surveyed. As will be discussed in chapter 3 in greater detail, there are a limited number of situations in which the use of surveillance technologies could be justified within a clear legal framework based on human rights and the rule of law. However, even in these situations surveillance technology is fundamentally privacy invasive, making their extensive use extremely threatening for privacy on the Internet.

(XI) Surveillance logs published

In October 2011 the Internet activist group Telecomix released extensive log files from Internet surveillance equipment in the Syrian Arab Republic.[117] The surveillance data published also provides an extraordinary picture from the inside of an Internet surveillance regime. It provides an insight into how users have both effectively and ineffectively attempted to protect their privacy and anonymity using Internet tools. It catalogues users on social networks, going shopping, looking at advertising, using search engines and video or photo sharing sites. More than anything else it gives an insight into the extraordinary power of surveillance equipment designed to breach personal privacy, beyond any and all boundaries of private space, anonymity or human dignity. The day to day personal activity of individuals is chronicled and catalogued and expressions of their personal hopes and dreams not destined for public view are laid out for display. A brief overview can be found below.

117 Valentino-Devries, J., Sonne, P., & Malas, N. (2011). Blue Coat Acknowledges Syria Used Its Gear for Internet Censorship Amid Arab Spring. Wall Street Journal. Retrieved December 13, 2011, from http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

Figure 3 – Surveillance logs overview[118]



118 Filastò, A. (2011). Blue Coat device logs indicate the levels of censorship in Syria. Retrieved December 13, 2011, from http://hellais.github.com/syria-censorship/.

3. THE GLOBAL LEGAL AND REGULATORY ENVIRONMENT FOR PROTECTION OF PRIVACY

The right to privacy is an ancient right, with roots in various religious traditions – including the Jewish, Christian and Muslim traditions – as well as in ancient Greece and China. Some sorts of protection for privacy existed in England as far back as 1361, with the Justices of the Peace Act criminalising eavesdropping and peeping toms.[119] Privacy has found protection as an international human right from the outset, being included in the Universal Declaration of Human Rights (UDHR),[120] as well as the International Covenant on Civil and Political Rights (ICCPR).[121]

At the same time, it has proven difficult to forge consensus on the specific content of this right. It is clear that it has at its essential core some notion of the right to be free of external intrusion, but beyond that various authors have come up with different definitions. Thus, the report by the government of the United Kingdom of Great Britain and Northern Ireland on privacy, known as the Calcutt report, stated that the authors could not find a "wholly satisfactory definition" of privacy.[122]

In their seminal piece on the topic in 1890, Warren and Brandeis defined privacy as the "right to be left alone".[123] Leading court decisions in the United States of America have subsequently identified four different types of privacy interests: unreasonable intrusion upon the seclusion of another, appropriation of one's name or likeness, publicity which places one in a false light and unreasonable publicity given to one's private life.[124] The South African Constitutional Court recently defined privacy as the "right of a person to live his or her life as he or she pleases".[125] The Canadian Supreme Court has defined it as "the narrow sphere of personal autonomy within which inherently private choices are made".[126] The European Court of Human Rights has eschewed the definition, stating: "The Court does not consider it possible or necessary to attempt an exhaustive definition

---

119 Electronic Privacy Information Center and Privacy International, Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments (Electronic Privacy Information Center and Privacy International: 2007), p. 5.

120 UN General Assembly Resolution 217A(III), 10 December 1948.

121 Adopted by UN General Assembly Resolution 2200A (XXI), 16 December 1966, entered into force 23 March 1976.

122 Calcutt, D., et al., 1990. Report of the committee on privacy and related matters, Chairman David Calcutt QC, London: HMSO (Cmnd. 1102), p. 7.

123 "The Right to Privacy" (1890) 4 Harvard Law Review 193, pp. 195.

124 See, Lake v. Wal-Mart-Stores Inc., 30 July 1998, Minnesota Supreme Court, C7-97-263. See also, Restatement (Second) of Torts, § 652B-E (1977).

125 NM and Others v. Smith and Others, 2007(7) BCLR 751, para. 33.

126 Godbout v. Longueuil (City) [1997] 3 SCR 844, para. 97.

of the notion of 'private life'."[127] In the case of Ponzetti de Balbín, Indalia vs Editorial Atlàntida S.A., the Argentine Supreme Court also relied on an extremely broad definition of privacy.[128]

Furthermore, it is reasonably clear that the content of the right has a subjective element, inasmuch as one may, by treating something as public in nature, effectively render it so, or perhaps cede parts of one's privacy. Thus, one's sexual orientation is private, but one might change this by making it public repeatedly through advocacy. In this regard, it may be contrasted with other personal rights, such as to reputation or to freedom of expression, which have much clearer and more objective boundaries. It may thus be assimilated to "hard core pornography" of which Justice Stewart of the United States Supreme Court noted that it was difficult to define the concept, "But I know it when I see it".[129] The problem of definition is exacerbated by the role of the notion of the public interest, also notoriously difficult to define, in defining the scope of privacy protection. The lack of a clear definition has contributed to difficulties in applying and enforcing the right to privacy.

The idea of data protection, which is of particular relevance to the concept of privacy and the Internet, is of far more recent vintage, essentially finding its genesis in the increasing collection of personal data about individuals by government. The advent of computers, and then of the Internet, greatly spurred on the development of the concept of data protection. The very first data protection law has been attributed to the Land (or state) of Hesse in Germany in 1970, and Sweden is credited with having adopted the first national law in 1973.

The core concept behind data protection is that individuals have a right to control the collection and use of data through which they may be identified (personal data). Like privacy, data protection is subject to certain constraints, of which an obvious one is police investigations into crime. Data protection may be contrasted with privacy inasmuch as the core notions underpinning it are fairly clear and garner wide consensus, albeit with some important variations.

An important issue for Internet privacy in general is the precise relationship between privacy and data protection or, to put it differently, the extent to which data protection principles find protection as part of the established human right to privacy. It is clear that the two issues are different and that data protection is not entirely subsumed into the concept of privacy.[130] However, important data protection principles can be derived directly from the human right to privacy, and this finds support in international jurisprudence. This is less clear of other principles, and certainly of the systems that are used to give concrete protection to data protection.

---

127 Niemietz v. Germany, 16 December 1992, 16 EHRR 97, para. 29. See also Workman, R., who in 1992 wrote: "[A] solid definition of 'privacy' has eluded commentators". "Balancing the Right to Privacy and the First Amendment" (1992) 29 Houston Law Review 1059, p. 1063.

128 Decided 11 December 1984, Corte Suprema de Justicia de la Nación (CS), para. 8. Available at: http://www.fallodelderecho.com.ar/jurisprudencia-argentina/ponzetti-de-balbin.

129 Jacobellis v. Ohio, 378 US 184 (1964), at. 197.

130 In recognition of this, the Charter of Fundamental Rights of the European Union includes protection for both privacy and data protection (see note 208). The European Commission's new proposals for a data protection regulation also reflect this idea, stating: "Data protection is closely linked to respect for private and family life". Note 217, p. 7.

3.1 International protection for privacy and personal data

3.1.1 Privacy

3.1.1.1 Global standards

Privacy finds direct and explicit protection under international human rights law. Article 12 of the UDHR states:

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.

The right was given formal legal protection in Article 17 of the ICCPR, which states:

(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 and reputation.

(2) Everyone has the right to the protection of the law against such interference or attacks.

These two definitions are similar, albeit with some important differences. The UDHR only protects against arbitrary, but not unlawful, interferences with privacy. In practice this is likely to be of limited importance, since an unlawful interference will always qualify as arbitrary. As far as honour and reputation go, the ICCPR only protects against unlawful attacks, while the UDHR protects against all such attacks. This may be more significant in nature, although this remains untested in the jurisprudence.

The UN Human Rights Committee has made it clear in a General Comment on Article 17 that the right to privacy encompasses the right to protection "against all such interferences and attacks whether they emanate from State authorities or from natural or legal persons."[131] The Committee's General Comment provides little guidance, however, as to what either 'arbitrary' or 'privacy' mean. Regarding the former, the Committee stated that an interference that was provided by law could still be arbitrary, and that all such interferences would need to be "in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, reasonable in the particular circumstances."[132] This ultimately provides very little guidance as to what may be considered to be 'arbitrary', although it would at least rule out interferences with privacy that were established by laws which ran against the aims of the Covenant or which were not reasonable.

The General Comment also includes fairly expansive, if general, statements on data protection, stating that the gathering and holding of personal information, whether by public or private bodies, must be regulated, that individuals have a right to ascertain what information about them is held, and for what purposes, and by whom.[133]

The jurisprudence of the Committee in this area has also been sparse. In the case of Hulst v. the Netherlands, the Committee had to assess whether or not interception of the telephone calls by the author, who was a lawyer, which were used to convict him of

131 General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), adopted 4 August 1988, para. 1.
132 Ibid., para. 4.
133 Ibid., para. 10.

a crime, represented an unwarranted invasion of his privacy. In deciding that there had been no interference, the Committee quoted the standards noted above in its General Comment, and held that the interference was authorised by law and was reasonable.[134]

3.1.1.2 African and Inter-American System

There is no explicit protection for privacy in the African Charter on Human and Peoples' Rights.[135] Protections for privacy are also found in the American Convention on Human Rights (ACHR),[136] at Article 11, and the European Convention on Human Rights (ECHR),[137] at Article 8.

The relevant provisions of the ACHR state:

> (2) No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
>
> (3) Everyone has the right to the protection of the law against such interference or attacks.

These provisions are very similar to those found under the UDHR and ICCPR. There has been little direct jurisprudence on this issue before the Inter-American Court of Human Rights. An important recent case on privacy, decided in November 2011, is *Fontevecchia & D'Amico v. Argentina*.[138] In that case, the Inter-American Court held that the publication of certain private information about Menem, the former President of Argentina, was not an invasion of his privacy. It gave as reasons that the information was already well known, it had not even been treated confidentially by Menem and there was considerable public interest in the information.

The Inter-American Court has dealt with privacy on a number of other occasions as well. In the case of *Tristán Donoso v. Panama*, the Court found a breach of the right to privacy when State officials disseminated a recording of a private telephone conversation, which had apparently been made by a private party, to church officials and members of the bar association.[139] In the case of *Escher et al. v. Brazil*, the Court came to a number of important conclusions regarding privacy in the context of telephone surveillance. First, it held that while the burden proof of the facts of a human rights violation normally lay with the complainant, it was legitimate to draw reasonable conclusions where it was impossible for the complainant to prove these facts conclusively, due to secrecy on the part of the State.[140]

---

134 Communication No. 903/1999, 1 November 2004.
135 Adopted 26 June 1981, OAU Doc. CAB/LEG/67/3 rev. 5, 21 I.L.M. 58 (1982), entered into force 21 October 1986.
136 Adopted 22 November 1969, O.A.S. Treaty Series No. 36, entered into force 18 July 1978.
137 Adopted 4 November 1950, E.T.S. No. 5, entered into force 3 September 1953.
138 29 November 2011, Series C, No. 238.
139 27 January 2009. Series C, No. 193, para. 83.
140 6 July 2009, Series C, No. 200, paras. 127-128.

Given the intrusive nature of telephone interception, the Court held:

> [T]his measure must be based on a law that must be precise and indicate the corresponding clear and detailed rules, such as the circumstances in which this measure can be adopted, the persons authorised to request it, to order it and to carry it out, and the procedure to be followed.[141]

In this case, the rules had not been followed properly, and so the invasion of privacy did not meet the requirement of legality, as stipulated in the ACHR.[142] The dissemination of some of the private material by State agents represented a further breach of the right to privacy.[143]

In terms of data protection, the Inter-American Commission has made it clear that it believes that a right of *habeas data* exists under the ACHR, which gives individuals the right to know what information the State and private actors have collected on them, to access that data and to modify, correct or remove it, as appropriate.[144] The Inter-American Court has never directly addressed the issue of *habeas data*.

3.1.1.3 ECHR: an overview

Article 8 of the ECHR formulates the right in rather different terms that the ICCPR or ACHR, as follows:

> (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 characterisation of the right here is more positive; a right to respect for one's privacy rather than to be protected against interferences. Another difference is that the protection is restricted to interference by public authorities, although the European Court of Human Rights has not interpreted the provision in such a limited fashion (see below). Finally, the standards for restrictions are set out in a much clearer form. Instead of vague terms such as 'arbitrary', 'unlawful' and 'abusive', we have a clear three-part test: a) in accordance with the law; b) necessary in a democratic society; and c) to protect one of the listed interests (national security, public order and so on).

In terms of the scope of the notion of privacy, the European Court has identified a number of specific types of State actions that may breach the right, such as interception of private

---

141 Ibid., para. 131.
142 Ibid., para. 146.
143 Ibid., para. 164.
144 Inter-American Commission on Human Rights, *Report on the Situation of Human Rights Defenders in the Americas*, para. 89. Available at: http://www.cidh.org/countryrep/defenders/defenderschap1-4.htm.

communications or telephone tapping, regardless of the content of the communication,[145] allocation of rights over children,[146] interference with sexual life,[147] compulsory medical treatment[148] and access to certain types of State-held information.[149] The Court has refrained from proposing a generic definition of privacy, holding instead, as noted above, that this is not possible.[150]

The Court has, however, indicated a number of features of the right. In the case of *Von Hannover v. Germany*, for example, the Court held that privacy covers "aspects relating to personal identity, such as a person's name, or a person's picture" and "a person's physical and psychological integrity". Furthermore, the right is intended to "ensure the development, without outside interference, of the personality of each individual in his relations with other human beings."[151] In *Niemietz v. Germany*, it held that "it would be too restrictive to limit the notion to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world". Instead, "private life must also comprise to a certain degree the right to establish and develop relationships with other human beings."[152] Business and professional relations came within the scope of the concept, so that a search of a business premises did represent an interference with private life.[153]

The Court has noted that "a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor."[154] Even information collected in public situations may, through the unexpected use to which it is put, raise private life issues. Thus: "Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain."[155]

In practice, the Court has tended to recognise a fairly wide scope of the right, while also recognising the possibility of restrictions, along with a wide margin of appreciation to States, particularly in cases involving protection of children. For example, in the case of Keegan v. Ireland, the Court stated that States "enjoy a wide margin of appreciation in the area of adoption."[156] The case involved a father seeking guardianship over his child, whom the mother, who was estranged from the father, had put up for adoption. In *Von*

---

145 See, for example, Iordachi And Others v. Moldova, 10 February 2009, Application No. 25198/02. See also Halford v. the United Kingdom, 25 June 1997, Application No. 20605/92, para. 44.

146 See, for example, Elsholz v. Germany, 13 July 2000, Application No. 25735/94.

147 See, for example, Dudgeon v. the United Kingdom, 22 October 1981, Application No. 7525/76. See also Mosley v. The United Kingdom, 10 May 2011, Application No. 48009/08.

148 See, for example, Acmanne and others v. Belgium, 10 December 1984, Admissibility Decision, Application No. 10435/83.

149 See, for example, Gaskin v. United Kingdom, note 167.

150 See *Niemietz v. Germany*, note 127. In *Costello-Roberts v. the United Kingdom*, the Court held that the notion of private life "is not susceptible to exhaustive definition". 25 March 1993, Application No. 13134/87, para. 36. The case involved corporal punishment at a private school which the Court held in the circumstances did not infringe private life.

151 24 June 2004, Application No. 59320/00, para. 50. Cross references to other legal cases and texts have been removed here and also from other quotations in the text.

152 16 December 1992, Application No. 13710/88, para. 29.

153 See also *Von Hannover v. Germany (No. 2)*, 7 February 2012, Applications Nos. 40660/08 and 60641/08, para. 95.

154 *P.G. AND J.H. v. United Kingdom*, 25 September 2001, Application No. 44787/98, para. 57.

155 Ibid. For example, information collected openly by security services may be covered. See Rotaru v. Romania, 4 May 2000, Application No. 28341/95.

156 26 May 1994, Application No. 16969/90, para. 47.

Hannover v. Germany (No. 2), which involved the publication of pictures alleged to be private, the Court stated: "Contracting States have a certain margin of appreciation in assessing whether and to what extent an interference with the freedom of expression protected by this provision is necessary".[157]

3.1.1.4 ECHR: restrictions

The Court has developed a fairly clear methodology for applying the three-part test for restrictions in cases involving interferences with privacy. In a number of cases, especially regarding telephone tapping and other forms of surveillance, the Court has noted that due to the particularly invasive nature of these activities, they must "be based on a 'law' that is particularly precise … especially as the technology available for use is continually becoming more sophisticated."[158] In the case of *Kruslin v. France*, the Court held that this part of the test was not met because the conditions on telephone tapping were not sufficiently precise. In particular, there was no restriction on the categories of person who might have their telephones tapped, no obligation on judges to set a time limit on tapping, no procedures for drawing up reports on intercepted conversations or procedures for destruction of recordings, and no requirements that recordings be kept intact.[159]

In the case of *Malone v. United Kingdom*, the European Court examined the practice of 'metering' of phone calls (i.e. recording the numbers called and length of the calls). It distinguished this from actual interception of calls, but noted that while this was legitimate (presumably on the basis of consent) for purposes of billing and monitoring of proper use of the service, passing this information on to the police represented an interference with private life. There was no law that required the Post Office, which conducted the metering (a public body which had become British Telecommunications by the time of the case), to pass the records over to the police, but in practice they did so in cases where this information was "essential to police enquiries in relation to serious crime" and could not be obtained from other sources". This practice did not meet the standard of being "in accordance with the law" for purposes of Article 8(2) of the ECHR.[160] This is clearly relevant for other cases in which private actors – such as Internet service providers – engage with public bodies in areas which impact on privacy rights.

In terms of the second part of the test, in general, the Court has no problem recognising a legitimate aim which requires protection in privacy cases, often the rights of others or public order. Thus, in *Leander v. Sweden*, the Court held in one short paragraph that a law allowing police to keep secret information gathered on job applicants for certain positions was necessary in the interests of national security,[161] while in *Murray v. the United Kingdom* the Court similarly devoted only one paragraph to recognising the prevention of crime as a legitimate aim.[162]

In assessing the necessity part of the test, the Court has stated: "[R]egard must be had to the fair balance that has to be struck between the competing interests of the

---

157 Note 153, para. 104.
158 See, for example, *Kruslin v. France*, 24 April 1990, Application No. 11801/85, para. 33. See also Rotaru v. Romania, note 155, para. 62. This latter case involves the collection of personal data.
159 Ibid., *Kruslin v. France*, para. 35.
160 *Malone v. United Kingdom*, 2 August 1984, Application No. 8691/79, paras. 83-86.
161 26 March 1987, Application No. 9248/81, para. 49.
162 28 October 1994, Application No. 14310/88, para. 89.

individual and of the community as a whole".[163] Furthermore, "the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued" and that the "reasons adduced to justify the interferences at issue are 'relevant and sufficient'".[164] As with national courts, the European Court has relied upon the idea of the overall public interest when assessing restrictions on privacy, especially when competing human rights come into play, as is clear from the box below on the Von Hannover case.

3.1.1.5 ECHR: private actors

The European Court has addressed the question of interference with privacy by private interests on a number of occasions. It has stressed that "the object of [Article 8] is 'essentially' that of protecting the individual against arbitrary interference by the public authorities".[165] The Court has recognised that privacy interests may impose positive obligations on States to take action to safeguard privacy. Sometimes, the Court uses positive obligations in cases in which "it is not that the State has acted but that it has failed to act" to protect privacy.[166] Some of these cases deal with the relationship between individuals and the State, or the 'vertical' application of rights. *Gaskin v. United Kingdom* is an example of this. In that case, the Court held that a public authority was obliged to release certain personal information relating to the applicant to protect a privacy interest.[167]

At the same time, the Court has in some cases referred to States' positive obligation to regulate relations between non-State actors, the 'horizontal' application of rights. In such cases, it is not the relationship between the State and an individual – either because of an action the State has taken or the failure of a State to act – that is in issue. Rather, the claim is that the effective protection of private life requires the State to regulate relations between non-State actors, for example by providing a legal remedy against privacy invasions.

In some of these cases, there has been an element of State involvement in the privacy breach. For example, in *López Ostra v. Spain*, the Court held that the failure of the authorities to take action to prevent the detrimental effects of severe environmental pollution arising from a waste-treatment plant breached Article 8. However, the Court specifically noted that the legality of the plant under Spanish law was in question and focused on the fact that the authorities had not only failed to protect Mrs. López Ostra but had also contributed to prolonging the situation.[168] In *X and Y v. the Netherlands*,[169] the Court held that a civil remedy was insufficient to protect individuals against sexual assault and that a criminal remedy should be available. The Netherlands did normally provide a criminal law remedy for sexual assault; it was not applicable in this case because of certain procedural issues relating to the fact that the victim was mentally handicapped.

---

163 *Keegan v. Ireland*, note 156, para. 49.
164 *Olsson v. Sweden*, 24 March 1988, Application No. 10465/83, paras. 67-68.
165 *See Marckx v. Belgium*, 13 June 1979, Application No. 6833/74, para. 31.
166 *Airey v. Ireland*, 9 October 1979, Application No. 6289/73, para. 37.
167 *Gaskin v. United Kingdom*, 7 July 1989, Application No. 10454/83, paras. 41 and 49.
168 9 December 1994, Application No. 16798/90, paras. 54-6.
169 26 March 1985, Application No. 8978/80.

In other cases, however, the Court has held that States were in breach of the right to privacy purely due to actions between private parties (see box).

(XII) Cases of Von Hannover v. Germany

Two decisions, in 2004 and in 2012, by the European Court of Human Rights, Von Hannover v. Germany and Von Hannover v. Germany (No. 2), set out clear rules regarding privacy. That first case involved a number of photos of Princess Caroline of Monaco, including her riding on horseback, on a skiing holiday and tripping over something on a private beach. The photos were published in private magazines in Germany and the case was, therefore, about the horizontal application of rights. The German courts, for the most part, upheld the publication of the pictures (with the exception of certain pictures taken in places where the princess had a reasonable expectation of privacy and some pictures involving her children).

The situation was largely the same in the second case, with the exception that the photos in question focused mostly on the issue of the illness of the reigning Prince of Monaco, Prince Rainier, and the way his family were looking after him during his illness.

In the first case, the European Court stated:

> In the cases in which the Court has had to balance the protection of private life against the freedom of expression it has always stressed the contribution made by photos or articles in the press to a debate of general interest.[170]

The Court also stipulated:

> The Court considers that a fundamental distinction needs to be made between reporting facts – even controversial ones – capable of contributing to a debate in a democratic society relating to politicians in the exercise of their functions, for example, and reporting details of the private life of an individual who, moreover, as in this case, does not exercise official functions.[171]

The domestic courts had held that Princess Caroline was a figure of contemporary society "par excellence" and therefore had no right to privacy unless she was in a secluded place out of the public eye. The European Court held that this standard might be appropriate for politicians exercising official functions, but was not applicable in the present case. As the Court noted in relation to the applicant, "the interest of the general public and the press is based solely on her membership of a reigning family whereas she herself does not exercise any official functions."[172]

- In the second case, the Court set out a number of principles to be taken into account in balancing freedom of expression and the protection of privacy, including:
- the extent to which the publication contributed to a matter of public interest (para. 109);

170 Note 151, para. 60.
171 Ibid., para. 63.
172 Ibid., para. 72.

- the degree of fame of the person involved and the subject of the report (para. 110);
- the prior conduct of the persons involved (para. 111);
- the content, form and consequences of the publication (para. 112); and
- the circumstances in which the photos were taken (para. 113).

In general, the Court appeared to be prepared to allow wide latitude, even to photos, which made some contribution to debate on a matter of public interest. The complete lack of such contribution in the first case – perhaps best exemplified by the photo of Princess Caroline tripping on the beach – mandated the particular conclusion reached, while in the second case, the Court held that "articles about the illness affecting Prince Rainier III, the reigning sovereign of the Principality of Monaco at the time, and the conduct of the members of his family during that illness" did bear on a matter of public concern.[173]

3.1.1.6 ECHR: data protection

The Court has never recognised a general right to data protection under Article 8 of the ECHR, at least in the sense in which that term is generally used. However, in a series of cases, it has recognised various aspects of the rights generally associated with data protection.

First, in a number of decisions the Court has held that the collection of private information engages concern for private life. For example, in the case of *Murray v. the United Kingdom*, the government did not contest, and the Court accepted, that collection of personal information(including a photograph) upon arrest represented an interference with private life, although it was justified as a restriction on that right in the circumstances of that case.[174]

In the case of *Leander v. Sweden*, the Court held that both the storing and the release of information relating to private life represented an interference with privacy.[175] In that case, the Court discussed in some detail the procedural safeguards that were required to ensure that the collection of information – in this case about suitability for employment in a naval museum – met the requirement of necessity in a democratic society. The Court accepted that the collection of this sort of information could be necessary to protect national security. However, the Court stated that there must be "adequate and effective guarantees against abuse".[176] It noted that the relevant law contained provisions to limit the use of the information to a minimum, especially outside of matters of control of personnel, where it might be used only for purposes of prosecution and obtaining citizenship. The Court placed particular emphasis on the role of external players in exercising oversight over the system, including parliamentarians, the Chancellor of Justice, the Parliamentary Ombudsman and the Parliamentary Committee on Justice.

173 Note 153, para. 117.
174 Note 162, para. 86.
175 Note 161. See also Rotaru v. Romania, note 158.
176 Ibid., para. 60.

Second, the Court has held that dissemination of private information by public bodies engages privacy concerns. In *Z. v. Finland*, the issue was the disclosure of certain information about the applicant, including the fact of being HIV positive, through the judicial process. The Court had no problem deciding that this was an interference with the applicant's right to private life. Indeed, the Court held that protection of this personal data, and especially medical records, was "of fundamental importance to a person's enjoyment of his or her right to respect for private and family life".[177] Given the particularly sensitive nature of the medical information in question, "any State measures compelling communication or disclosure of such information without the consent of the patient call for the most careful scrutiny on the part of the Court, as do the safeguards designed to secure an effective protection".[178] In upholding the disclosure of certain evidence on a limited basis, the Court focused on the fact that the applicant had been given adequate opportunities to object to the disclosures and the importance of the information as evidence in a serious criminal case.[179] The Court did, however, indicate that public disclosure of the information after ten years, as well as its disclosure in the judgment of the Court of Appeal, when other options were available (such as omitting to mention her name), were breaches of the right to private life.[180]

Even internal disclosures (i.e. disclosures within the public sector) raise privacy issues. *M.S. v. Sweden* involved the disclosure of certain medical information by a public medical clinic to the Social Insurance Office, in the context of a claim to the Office for benefits relating to the applicant's medical condition. There was no question that the matter engaged private life issues. The Court rejected the government's claim that by submitting the claim, the applicant had consented to the disclosure, in part because the scope of the disclosure of information was not determined by her.[181] In holding that the interference was justified, the Court noted the necessity for the Office to access the information to be able to assess the insurance claim and strong protections for confidentiality, such as robust sanctions for disclosures outside of the strict framework of the law.[182]

Third, in a number of cases – including *Leander v. Sweden*,[183] *Gaskin v. United Kingdom*,[184] *Guerra and Ors. v. Italy*,[185] *McGinley and Egan v. United Kingdom*,[186] *Odièvre v. France*[187] and *Roche v. United Kingdom*[188] – the Court has upheld a right of individuals to access information held by public authorities which relates to them. In each of these cases, the Court found that to deny access to the information in question was an interference with the right to private and/or family life, albeit allowing in some cases that refusing access might be a legitimate restriction on these rights.

---

177 25 February 1997, Application No. 22009/93, para. 94.
178 Ibid., para. 96.
179 Ibid., paras. 101-109.
180 Ibid., paras. 111-113. See also Rotaru v. Romania, note 158.
181 22 August 1997, Application No. 20837/92, para. 35.
182 Ibid., paras. 42-43.
183 Note 175.
184 7 July 1989, Application No. 10454/83, 12 EHRR 36.
185 19 February 1998, Application No. 14967/89.
186 9 June 1998, Application Nos. 21825/93 and 23414/94.
187 13 February 2003, Application No. 42326/98.
188 19 October 2005, Application No. 32555/96.

(XIII) Cases before the European Court of Human Rights on access to private information

In the first case on access to private information before the European Court, *Leander*, the applicant was dismissed from a job with the Swedish government on national security grounds, but was refused access to information about his private life, held in a secret police register, which had provided the basis for his dismissal. The Court held that the storage and use of the information, coupled with a refusal to allow the applicant an opportunity to refute it, was an interference with his right to respect for private life. The interference was, however, justified as necessary to protect Sweden's national security.[189] It is interesting to note that it ultimately transpired that Leander was in fact fired for his political beliefs, and he was offered an apology and compensation by the Swedish government.

In *Gaskin*, the applicant, who as a child had been under the care of local authorities in the United Kingdom of Great Britain and Northern Ireland, had applied for but was refused access to case records about him held by the State. The Court held that the applicant had a right to receive information necessary to know and understand his childhood and early development, although that had to be balanced against the confidentiality interests of the third parties who had contributed the information. Significantly, this placed a positive obligation on the government to establish an independent authority to decide whether access should be granted if a third party contributor was not available or withheld consent for the disclosure. Since the government had not done so, the applicant's rights had been breached.[190]

In *Guerra*, the applicants, who lived near a "high risk" chemical factory, complained that the local authorities in Italy had failed to provide them with information about the risks of pollution and how to proceed in event of a major accident. The Court held that severe environmental problems may affect individuals' well-being and prevent them from enjoying their homes, thereby interfering with their right to private and family life. As a result, the Italian authorities had a positive obligation to provide the applicants with the information necessary to assess the risks of living in a town near a high risk chemical factory. The failure to provide the applicants with that essential information was a breach of their Article 8 rights.[191] The decision was particularly significant as it appears that the State did not hold the information requested, so that it would actually need to go out and collect it.

In *McGinley and Egan*, the applicants had been exposed to radiation during nuclear testing in the Christmas Islands, and claimed a right of access to records regarding the potential health risks of this exposure. The Court held that the applicants did have a right to access the information in question under Articles 6 and 8 of the ECHR, regarding, respectively, the right to a fair hearing and respect for private and family life. However, the government had complied with its positive obligations through the establishment of a process by which access to the information could be obtained, which the applicants had failed to make use of.[192]

189 *Leander*, note 183, paras. 48, 67.
190 *Gaskin*, note 184, para. 49.
191 *Guerra*, note 185, para. 60.
192 *McGinley and Egan*, note 186, paras. 102-103.

> In *Odièvre*, the issue was access to information about the natural mother of the applicant. The Court accepted that this was an interference with the right to private life, as guaranteed by Article 8, but held that the refusal by the French authorities to provide the information represented an appropriate balance between the interests of the applicant and the interests of her mother, who had expressly sought to keep her identity secret.[193]
>
> In *Roche*, which like *McGinley and Egan* involved claims of medical problems resulting from military testing, the Court held that there had been a breach of the right to privacy since the government did not have reasonable grounds for refusing to disclose the information. Significantly, the Court held that the various disclosures that were made in response to requests by the applicant did not constitute the "kind of structured disclosure process envisaged by Article 8".[194]

Fourth, in at least some cases, notably *Rotaru v. Romania*, the Court has referred to the right to refute information which was apparently false.[195] The case involved information held by the security services, and which was apparently false, and to which the applicant had been denied access or an opportunity to correct.

It is clear from these decisions that the collection and dissemination of private information, including within the public sector, will almost always raise issues of relevance to private life. Furthermore, in assessing whether or not such collection and dissemination is necessary in a democratic society, the Court will assess the use to which the information is put. The Court has also made some reference to the right to refute (and perhaps by implication correct) information where the subject of that information believes it is incorrect. The Court has at least recognised the importance of independent oversight bodies, and may even require them to be available to decide data protection issues.

However, when it comes to access to information, even personal information which relates to the applicant, the Court has proceeded cautiously. The Court has refused to recognise a general right to access one's personal information, instead limiting its decisions to the case at hand. In each case, it first undertook an assessment of whether or not access to the information was needed to protect the applicant's right to privacy and/or family life. In other words, access was granted where needed to protect another privacy interest, but access itself has not been recognised itself as a privacy interest. Furthermore, in each of these cases, the information was held by a public body. It is far from clear that the Court would apply the same reasoning, via a positive obligation on the State, to require private bodies to release information.

There have been a few cases at the European Court of Human Rights based directly on privacy and the Internet. These suggest that the complex and rather different nature of the Internet may throw up some challenging privacy issues. Thus, in the case of *K.U. v. Finland*, the issue was whether an ISP should be forced to reveal the identity of someone who had used its services to post an advertisement purporting to be someone else, namely a 12-year-old boy, "linking" to the boy's picture and claiming he was looking for

193 *Odièvre*, note 187, paras. 44-49.
194 *Roche*, note 188, para. 166.
195 Note 158, para. 46.

an "intimate relationship with a boy of his age or older "to show him the way".[196] The ISP refused and this was upheld by the domestic courts since, under Finnish law, the police could only force disclosure of such information in certain types of cases, not including this case, which was one of malicious misrepresentation.

In deciding the case, the European Court reviewed a wide range of international authorities from the Council of Europe, the United Nations and the European Union. It easily held that the case involved private life, "a concept which covers the physical and moral integrity of the person."[197] The Court noted that States have a positive obligation under Article 8 to criminalise offenses against the person, particularly when these involve children and other vulnerable individuals, but that such offenses had limited deterrent effect if the offender could not be identified. The availability of a claim for damages against the ISP was also not sufficient, since only a direct remedy against the actual offender would create the necessary deterrent effect.

The Court noted the need for adequate protections for the presumption of innocence and the fact that "freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected." However, by simply ruling out disclosure of the information, the State had not put in place "the framework for reconciling the various claims which compete for protection in this context", and was thus in breach of its Article 8 obligations.[198] The Court thus recognised the complex balancing of rights that would be needed to decide this case, but did not actually undertake that balancing exercise itself.

3.1.2 Data protection

3.1.2.1 Global standards

Regimes on data protection are directly relevant to the protection of privacy on the Internet, given that they were specifically designed to address data collection and privacy issues of the sort that modern technologies have enabled. At a very general level, these regimes place conditions on the collection, use and storage of personal data (rules governing data controllers), give certain rights to the individuals to whom the data relates (data subjects), and provide for a system of oversight to ensure respect for the rules and to address breaches. A central aspect of almost all data protection systems is the identification of key principles governing these issues and, in particular, the collection, use and storage of personal data.

Within the United Nations, General Assembly Resolution 45/95, Guidelines for the regulation of computerised personal data files,[199] sets out ten key principles on data protection. These are relevant primarily to national legislation but are also binding on inter-governmental organisations, with appropriate modifications. They apply to publicly and privately held computerised files containing data on individuals, and may be extended to cover manual files and/or data on legal persons.

---

196 2 December 2008, Application No. 2872/02, para. 7.
197 Ibid., para. 41.
198 Ibid., paras. 46-50.
199 Adopted on 14 December 1990, A/RES/45/95.

The Guidelines include a number of principles governing the collection and use of personal data that are found in many data protection regimes. The key principles may be summarised as follows:

Lawfulness and Fairness: collection of data should be fair and lawful and not contrary to the purposes and principles of the Charter of the United Nations.

Accuracy: data controllers are responsible for checking data regularly to ensure its accuracy and relevance, and that it is as complete as possible for the purpose it was collected, to avoid errors of omission.

Purpose-Specification: the purpose for which data is collected should be legitimate and brought to the attention of the data subjects, the data should not be used for other, incompatible, purposes, and the data should only be kept for as long as necessary to serve this purpose.

Interested-Person Access: data subjects have the right to know when their data is being collected or processed, to access that data in an intelligible form, without undue delay or expense and to make appropriate rectifications or deletions.

Non-Discrimination: any exceptions to these principles may not be discriminatory in nature.

Security: appropriate measures should be taken to protect data against both natural and human risks, including unauthorised access, misuse or physical contamination.

The Guidelines recognise that there may be a need for exceptions from the first five principles, but only as necessary to protect national security, public order, health and morals, or the rights and freedoms of others. They call for the designation of an independent supervisory authority with responsibility for ensuring respect for the principles, along with systems of sanctions for breach of the rules. They also call for limits on circulation of information to countries which do not offer comparable safeguards.

(XIV) Regional standards on data protection

There are numerous regional standards on data protection. The main systems that currently exist are as follows:

- Organisation for Economic Co-operation and Development (OECD): the 1980 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[200]
- Asia-Pacific Economic Cooperation (APEC) forum: the 2005 *APEC Privacy Framework.*
- Economic Community for West African States (ECOWAS): the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS.[201]
- Organisation of American States (OAS): General Assembly Resolution 2661 on Access to Public Information and Protection of Personal Data.[202]

200 Adopted by OECD Council Recommendation on 23 September 1980.
201 Adopted on 16 February 2010.
202 Adopted on 7 July 2004, AG/RES. 2661 (XLI-O/11).

- Council of Europe (COE): the 1981 *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*,[203] as amended by the 2001 Additional Protocol to the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder Data Flows.[204]
- European Union: Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data.[205]

3.1.2.2 APEC standards

The 21 members of Asia-Pacific Economic Cooperation (APEC) bring together countries such as Canada, Chile, Peru and the United States of America on one side of the Pacific, with a number of Asian economies, including major economies such as China, Japan and the Russian Federation, as well as Indonesia, Viet Nam and Thailand, and countries such as Australia and New Zealand.

The main APEC rules on privacy are set out in the APEC Privacy Framework.[206] The preamble to the Framework grounds the motivation for its adoption clearly in the need to maintain consumer trust so as to foster the economic benefits from electronic commerce. It notes that the Framework is consistent with the OECD Guidelines, while balancing the need for information privacy with business needs. It also recognises the need to allow individual countries flexibility in relation to implementation.

The core principles are roughly similar in nature to the UN Guidelines, as well as European and OECD standards. A certain degree of flexibility is built into the Framework, which may be contrasted with the more detailed European standards, where exceptions are spelt out in more detail. This is also reflected in the provisions on implementation, which grant wide discretion to Member Economies to decide on the best approach.

The Principles define 'personal information' broadly as all information about an identified or identifiable individual and a 'personal information controller' similarly broadly as a person who exercises control over the collection or use of personal information (paragraphs 9-10). As noted, the Framework specifically incorporates a degree of flexibility in being applied based on social, economic and cultural differences, as well as the need to protect national security, public safety and public policy (paragraphs 12-13).

The first substantive principle is 'Preventing Harm', which calls for measures to prevent misuse of personal information which are proportionate to the likelihood and severity of the risk of harm (paragraph 14). Controllers are required to provide notice, where

203 Adopted on 28 January 1981, E.T.S. No. 108, entered into force 1 October 1985.
204 Adopted on 8 November 2001, E.T.S. No. 181, entered into force 1 July 2004.
205 Adopted on 24 October 1995, OJ L 281, p. 31, as supplemented by Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, p. 37, and Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105, p. 54.
206 Available at: http://publications.apec.org/publication-detail.php?pub_id=390.

possible in advance or at the time of collection, to individuals about the fact of collection of personal information, the purposes for which it is being collected, the types of persons to whom it may be disclosed and how to contact the controller (paragraphs 15-17). Only information relevant to the stated purpose should be collected, and this should be done by lawful and fair means (paragraph 18).

Information should only be used for the purposes for which it was collected, or for compatible purposes, except with consent or where necessary to provide a service requested by the individual (paragraph 19). Individuals should also be provided with choice regarding the collection, use and disclosure of their information (paragraph 20). Information should be accurate and kept up-to-date, and stored in a manner that minimises the risk of unauthorised access, modification and so on (paragraphs 21-22).

In line with core data protection principles, individuals should have the right to access and to correct information about themselves, subject to cost and various other constraints (paragraphs 23-25). Finally, controllers should be held accountable for complying with these principles, including by ensuring that those to whom information is transferred undertake to respect the principles (paragraph 26).

3.1.2.3 European standards

Significant differences exist between the different regional data protection regimes, although the system of the European Union is very similar to that of the Council of Europe, as amended. We provide a more detailed outline here of the European Union system, as an example of a strong data protection approach and also of a system that has had a lot of global influence.

The system put in place by the European Union is widely recognised both as being very progressive, in the sense of providing strong protection for data protection, and as playing a leadership role in this area, in the sense of exerting influence over data protection laws in other countries. The rules are formally binding on the 27 members of the European Union, but their influence is far wider than that. In a recent study, Greenleaf compares the European systems with those of the OECD and APEC, and identifies ten key differences between them, all reflecting higher standards in the European systems. Analysing all 29 data protection laws outside of Europe, he concludes that 13 incorporate at least nine of these ten characteristics, 19 have at least seven and fully 23 have at least five, or one-half, of them.[207] This extremely strong correlation suggests that the European systems have been quite dominant globally.

The European Union adopted a *Charter of Fundamental Rights of the European Union* in December 2000,[208] which contains strong protections for both privacy in general (Article 7) and data protection in particular (Article 8). The latter require data processing to be fair, for a specific purpose and based on consent. Subjects have a right to access and rectify their data, and oversight shall be by an independent body. Although this was adopted after the main provisions of the data protection framework were adopted, the latter must be seen in light of these overriding guarantees.

---

207 See, for example, Greenleaf, G. The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, University of New South Wales Faculty of Law Research Series, Paper 42, 2011.

208 2000/C 364/01.

The basic approach of Directive 95/46 is to apply the rules extremely broadly and then apply limitations or exceptions. The definitions in Article 2 thus define personal data as any data relating to an identified or identifiable natural person, processing as any operation on personal data (including collection, storage and so on), the controller as any natural or legal person who determines the purposes and means of processing of data.

Pursuant to these definitions, any individual who stores telephone numbers on a mobile phone or computer is a controller. However, Article 3 provides that the directive does not apply to data processing for purposes outside of the scope of Community law (which include security and activities relating to the criminal law) or to processing by a natural person for "purely personal or household" activities. It also limits the scope of the Directive to processing wholly or partly by automated means (i.e. mostly electronically), or to data which are part of a filing system, thereby excluding data stored in an ad hoc or informal manner.

The data protection principles are set out in Article 6 (see box). These are essentially the same as the first three principles listed above from UN General Assembly Resolution 45/95. Most of the principles are reasonably clear. As a rule of thumb, the rule on incompatible processing is not breached if the information is used in a "way in which those who supplied the information would expect it to be used and disclosed."[209]

(XV) EU Data Protection Directive Principles

EU Directive 95/46 sets out the basic data protection principles in Article 6. They require that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

209 Irish Data Protection Commissioner, Data Protection Rule 3: Use and further processing of personal information. Available at: http://dataprotection.ie/viewdoc.asp?DocID=25.

Article 7 of Directive 95/46 sets conditions on when data may be processed, which include with the subject's consent, for purposes of entering into a contract with the subject, where necessary to comply with a legal obligation of the controller, where necessary to protect the "vital interests" of the subject (such as collection of blood after an accident), where necessary in the public interest or in the exercise of official authority, or where necessary to protect the controller's or a third party's legitimate interests, subject to a test of proportionality with the subject's interests. For the latter two grounds, the subject may object to the processing on "compelling legitimate grounds", and a separate right of objection is provided for in relation to processing of data for direct marketing purposes (Article 14). It will immediately be clear that this list is both inherently wide and subject to broad and potentially varying interpretation.

Consent of the subject is a key part of the system and it must be unambiguous. However, specifically ticking off an agreement with terms and conditions, such as one often does for Internet-based services, meets this standard. This is the case even though in most cases subjects do not read, and perhaps would have difficulty understanding if they did read, those terms and conditions. This could be criticised for placing an undue burden on subjects, although at the same time the whole idea of control over one's data almost inevitably leads to this.

Articles 10 to 12 of the Directive define certain rights of the data subject. Pursuant to Articles 10 and 11, he or she must be informed of the identity of the controller (or his or her representative), the purposes of the data processing and, as necessary to ensure fair processing, various other information, such as the recipients of the data and the right to access and rectify the data. The rigour of this is mitigated partly by the rule that the information does not need to be provided if the subject already has it and, as with consent, general terms and conditions may be used to 'impart' this information to the subject. Furthermore, where processing is done by an entity which did not collect the data, this information does not need to be provided in case of historical or scientific research, where this would be impossible or disproportionate, or where processing is required by law.

Pursuant to Article 12, subjects have the right to obtain from the controller, at reasonable intervals and without excessive delay or expense, the following:

- confirmation as to whether data is being processed, the purposes thereof, the categories of data and the recipients of the data;
- the data, in an intelligible form, along with their source; and
- the logic involved in any automatic processing, at least where this may lead to a decision affecting him or her.

Controllers are also required to rectify, erase or block data where the Directive has not been complied with, in particular because the data is incomplete or inaccurate, and notify relevant third parties of this. Articles 16 and 17 provide for data to be kept and processed in a secure manner.

Article 13 allows States to restrict the obligations of Articles 6, 10, 11, 12 and 21 (see below) where necessary to protect national or public security, to prevent criminal or professional breaches, for important economic reasons, for purposes of a monitoring or regulatory function, or to protect the subject or the rights or freedoms of others.

Another apparently onerous rule, once again mitigated by exceptions, is the obligation of controllers to notify the oversight body(before processing data) of the purpose, categories of data subjects, recipients and any proposed transfers to third countries. A register of all processing operations which have been notified in this way must be maintained by the oversight body and be open to the public.[210] States may carve out broad exceptions to this, including for non-profit organisations, where controllers appoint data protection officials, for registers which are by law intended to provide information to the public, and for certain categories of processing which are unlikely to harm rights or freedoms. For processing that is covered by an exception, key information must be made available to anyone on request (Articles 18, 19 and 21).

(XVI) Overview of the European Union data protection system

The main elements of the system are:

- Broad definitions of personal data and processing of data
- Principles governing personal data: processed fairly, for specific identified purposes, adequate, relevant and not excessive for those purposes, accurate and up-to-date, and kept no longer than necessary
- Rights of the data subject: to be informed of the controller and purpose of processing, to obtain the data in an intelligible form, to require rectification or deletion of the data
- Obligation of controller to notify the oversight body and for this to be kept in a public register
- Remedies available to subjects
- Transfers of data only where adequate protection is ensured
- Oversight by an independent body

Various remedies are available including the right of subjects to receive compensation from a controller where they have suffered damage due to unlawful processing of data (Article 23) and to a judicial remedy for breaches of their rights (Article 22). Sanctions shall also be established for those who breach the rules (Article 24).

A key part of the Directive is the limitations it establishes on transfers of data undergoing processing to third countries (i.e. outside of the European Union) (Article 25). This may be done only if the third country offers an "adequate level of protection" for the data. Once again, exceptions apply, and States may provide for transfers to non-adequate countries on grounds which are largely the same as those that apply to legitimate data processing in the first place, with the exception of the first one (i.e. the interests of the controller or a third party) (Article 26).

210 An example is the register of data controllers in the United Kingdom, available in a searchable format at: http://www.ico.gov.uk/what_we_cover/register_of_data_controllers.aspx.

Whole countries may be certified by the Commission as providing adequate protection. This has been done for countries like Switzerland, Canada and Argentina.[211] In the case of the United States of America, which does not generally qualify as 'adequate' because of its lack of central legislation governing data protection for private actors, the Department of Commerce has developed an International Safe Harbor Privacy Principles Certification Program.[212] This is a voluntary programme, whereby companies can apply for certification where they comply with the seven Safe Harbor Principles. These are along the lines of European data protection rules, and include providing notice about the purposes of collecting data, the right of individuals to refuse onward transfer of the data to third parties or use for other purposes, requirements of security for data and so on.[213] Once they receive certification, they are accepted as providing adequate personal data protection for purposes of the EU rules.[214]

The Directive provides for two types of institutional structures. First, each party must establish an independent supervisory or oversight body with various powers, such as to investigate, to intervene, including by banning data processing, to engage in legal proceedings and to hear complaints (Article 28). Second, there is the so-called Article 29 Working Party, composed of representatives of the oversight bodies, whose role is primarily advisory in nature (Articles 29 and 30).

There is little question that the Directive plays a very important role in the protection of personal data. It is widely lauded for being technology neutral (i.e. it applies regardless of the technology used to process data), for imposing high standards which are based on flexible principles, and for harmonising rules across the European Union and to some extent more widely.

At the same time, it has been criticised for being out-of-date (understandable given the rapid pace of change in terms of processing personal data), excessively bureaucratic, rigid and prescriptive, insufficiently focused on risk as opposed to procedures, and even unrealistic (for example in relation to international transfers in the context of massive and increasing global data flows).[215]

The need to renew the Directive is widely accepted and consultations are ongoing with a view to achieving this. The European Commission describes the objectives of this exercise as being to modernise the system to meet the challenges of globalisation and new technologies, to strengthen rights while reducing administrative formalities, to ensure a free flow of data, to improve the clarity and coherence of the rules, and to achieve consistent and effective implementation.[216]

---

211 See http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

212 See http://export.gov/safeharbor.

213 A full list of the principles is available at: http://export.gov/safeharbor/eu/eg_main_018475.asp.

214 The system was approved by the European Commission in Decision 2000/520/CE. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.

215 See, for example, Robinson, N.; Graux, H.; Botterman, M. and Valieri, L. *Review of EU Data Protection Directive: Summary*, prepared for the UK Information Commissioner's Office, May 2009, Foreword. Available at: http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive_summary.pdf.

216 See http://ec.europa.eu/justice/policies/privacy/review/index_en.htm.

On 25 January 2012, the Commission released its 'final' proposals for what it proposes to transform into a regulation (i.e. instead of a directive) on data protection.[217] The main importance of this is that the rules would have direct legal force in each Member State.[218] The proposals include a number of provisions to tighten up the rules in the existing Directive, to clarify areas of uncertainty and certain definitions, and to "beef up" various systems, such as the information to be provided to data subjects, procedures for exercising subjects' rights, remedies and oversight powers and cooperation.

The draft regulation also proposes a number of new rules. The information to be provided to subjects must be transparent, easily accessible and understandable. Another rule is the right of data portability, including the right to obtain a copy of one's data in a commonly used format. Controllers are required to put in place internal policies and mechanisms to ensure compliance with their obligations, to notify subjects of data breaches and to carry out assessments prior to risky processing. Public bodies and large private bodies are required to appoint data protection officers. The proposals would also establish a new body, the European Data Protection Board, to replace the Article 29 Working Party, with expanded powers. The rules on establishing 'adequacy' for purposes of third country transfers are also clarified.

Some of the proposals are perhaps more controversial. For example, the new regulation proposes to apply to data processing operations based outside of the European Union, "where the processing activities are directed to such data subjects, or serve to monitor the behaviour of such data subjects". It would establish a 'right to forget', including a right to require erasure of all data and an end to further processing.

3.1.2.4 Supplementary rules

Directive 95/46 is supplemented by two directives, Directive 2002/58 concerning the protection of privacy in electronic communications (e-Privacy Directive) and Directive 2006/24 on the retention of data (Data Retention Directive).[219] The former provides for a number of special rules regarding privacy in the context of electronic communications, requiring confidentiality of communications and various other types of data (traffic data and location data), except for limited purposes – such as billing, marketing and added value services – and providing for user rights in relation to various communications-related issues – such as itemising billing, caller identification services, call forwarding, directories of subscribers and unsolicited communications. States may, by legislative measures, override the rules on confidentiality for purposes of national and public security and the investigation of crimes – all of which fall outside the competence of the European Union – including by providing for data retention.

The Data Retention Directive essentially rides roughshod over these rules by requiring the wholesale retention of a large number of categories of communications data – not including the content of communications – for between six months and two years, in derogation from the relevant provisions on non-retention in the e-Privacy Directive.

---

217 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Brussels, 25.1.2012, COM(2012) 11 final, 2012/0011 (COD).

218 Directives, in contrast, only oblige Member States to bring their law into compliance with their provisions.

219 Note 205.

(XVI) Constitutional rulings on the EU Data Retention Directive[220]

Courts in three countries – the Czech Republic, Germany and Romania – have struck down as unconstitutional on privacy grounds national rules seeking to implement the EU Data Retention Directive. In October 2009, the Romanian Constitutional Court ruled that the Directive breached Article 8 of the ECHR. Among other things, the Court noted the comprehensive nature of the requirement of retention of data, which applies to everyone, regardless of whether they have committed, or are even under suspicion of having committed, a crime. It noted that the scope was ambiguous and that the rules lacked sufficient safeguards against abuse.[221] The decision is particularly important inasmuch as it purports to be based on Article 8 of the ECHR. If the European Court of Human Rights were to uphold this interpretation, it would mean that European Union countries would be caught in a legal catch-22.

In March 2010, the German Federal Constitutional Court followed suit, holding that the German implementing provisions violated the constitutional right to secrecy of telecommunications. It noted that the rules would create a sense among citizens of being watched, which would undermine their enjoyment of various fundamental rights. While limited retention of data to safeguard important security interests might be justifiable, the current rules were far too overbroad. The Court also made reference to the lack of safeguards and, in particular, the lack of proper oversight.[222]

The Czech Constitutional Court similarly ruled, in March 2011, that given the intensity and breadth of the interference with privacy, the rules could not be justified as a necessary limitation on the right to privacy. It noted, in this regard, that retention of the sort required by the rules did not impact significantly on crime statistics, especially given new technological possibilities to avoid identification. As with the German Court, the Czech Court noted that the purposes that would justify retention were too broad and that insufficient safeguards were in place.[223]

According to the European Commission: "Cases on data retention have also been brought before the constitutional courts of Bulgaria, which resulted in a revision of the transposing law of Cyprus, in which court orders issued under

220 The information in this section is drawn from EDRI's Shadow evaluation report on the Data Retention Directive (2006/24/EC), 17 April 2011, available at: http://www.edri.org/files/shadow_drd_report_110417.pdf and the official Report From the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011 COM(2011) 225 final.

221 Decision no 1258 from 8 October 2009 of the Romanian Constitutional Court, Romanian Official Monitor No 789, 23 November 2009. Available at: http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

222 Judgement of the Bundesverfassungsgericht 1 BvR 256/08, of 2 March 2010. Available at: http://www.bverfg.de/en/press/bvg10- 011en.html.

223 Official Gazette of 1 April 2011, Judgment of the Constitutional Court of 22 March on the provisions of section 97 paragraph 3 and 4 of Act No. 127/2005 Coll. on electronic communications and amending certain related acts as amended, and Decree No 485/2005 Coll. on the data retention and transmission to competent authorities. Available at: http://www.concourt.cz/clanek/GetFile?id=5075.

the transposing law were held to be unconstitutional, and of Hungary, where a case concerning the omission in the transposing law of the legal purposes of data processing is pending.[224, 225]

This Directive has been subject to massive criticism from both civil society and formal Commission organs. For example, the European Data Protection Supervisor has described the Directive as "the most privacy invasive instrument ever adopted by the EU".[226] European Digital Rights (EDRI) has stated: "Over the past five years, the Data Retention Directive has proved to be an unnecessary and unprecedented violation of the fundamental rights of 500 million Europeans."[227] Courts in three countries – Croatia, Germany and Romania – have struck down as unconstitutional implementing legislation for the Directive, and it is under constitutional attack in other countries as well (see box). EDRI has recommended, instead, "a system of expedited preservation and targeted collection of traffic data that assists in a specific investigation ('data preservation'), as has been agreed internationally in the Council of Europe's 2001 Convention on Cybercrime."[228]

The Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC), the Commission's formal evaluation of the Directive, disagrees. It states: "[T]he evaluation has demonstrated that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU" and: "[T]he EU should continue through common rules to ensure that high standards for the storage, retrieval and use of traffic and location data are consistently maintained."[229] As a result, it intends to propose revisions to, rather than the repeal of, the current data retention framework.

In 2009, a new Directive was adopted amending and extending certain provisions in the e-Privacy Directive.[230] The 2009 Directive enhanced the rules on security and notice to users in case of security breaches, and enhanced the remedies and sanctions for breaches of the rules. But the most important change was hidden in a few words in Article 5(3), which meant that the activities of storing or accessing information on the terminal equipment of the user are permitted only where the user has given his or her consent. Previously, it was enough to provide users with clear and comprehensive

---

224 Bulgarian Supreme Administrative Court, decision no. 13627, 11 December 2008; Supreme Court of Cyprus Appeal Case Nos. 65/2009, 78/2009, 82/2009 and 15/2010-22/2010, 1 February 2011; the Hungarian constitutional complaint was filed by the Hungarian Civil Liberties Union on 2 June 2008.

225 *Report From the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, note 220, pp. 20-21.

226 See his speech of 3 December 2010. Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf.

227 Shadow evaluation report on the Data Retention Directive (2006/24/EC), note 220, p. 2.

228 Ibid., p. 6.

229 Note 220, p. 1.

230 Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L337, p. 11.

information about terminal storing and accessing, and to give them an opportunity to reject these activities.

The directive is informally being called the "cookie directive", because of the enormous impact implementation of this rule will have on the way cookies work. It has caused a significant backlash from industry, who believe it will be difficult, costly and impractical to implement.[231] The rule has also raised a lot of questions as to what, exactly, constitutes consent. For example, would setting an Internet browser to accept cookies, which is basically what has happened in the past, qualify? Presumably not, but requiring users to accept every attempt to place a cookie on their devices would also be impractical.

The Directive remains law and countries are moving ahead to implement it (the deadline was May 2011; see below on the French efforts). In the United Kingdom of Great Britain and Northern Ireland, a law has been adopted – indeed the United Kingdom was one of the first countries to adopt such a law – but the Information Commissioner's Office, which is responsible for implementation, has indicated that it will give companies a year to bring themselves into compliance (i.e. that it will not prosecute breaches for a year).[232] The real impact of the measure thus largely remains to be seen.

3.2 National protection for privacy

3.2.1 China

There is limited protection for privacy in China, with no fully-fledged constitutional guarantee, no proper privacy law and no data protection law. In general, the Chinese authorities exercise a considerable degree of control over the Internet and individuals have very few privacy protections against them.[233]

However, there is increasing pressure for change, particularly in relation to threats to privacy from private quarters. This has been driven in significant part by abuses of private data in the form of targeted marketing approaches following on from commercial transactions, such as purchasing a car or insurance or opening a bank account. These have often taken the highly intrusive form of targeted text messages or even follow-up calls.

The response has been a number of legal and regulatory proposals having been mooted or adopted in recent years. Amendments to the criminal and tort laws have established independent actions in favour of privacy, and there have been various proposals regarding data protection.

Unlike many constitutions, the Chinese Constitution does not include a general, freestanding right to privacy. Article 40 of the Constitution states:

---

231 See http://online.wsj.com/article/SB10001424052748704444304575628610624607130.html.

232 See http://econsultancy.com/us/blog/8210-q-a-lbi-s-manley-on-preparing-for-the-eu-cookie-laws.

233 See, for example, the reporting on this by Reporters Without Borders, at http://en.rsf.org/china.html; the IFJ Press Freedom in China Campaign Bulletins, at: http://asiapacific.ifj.org/en/pages/asia-pacific-china-bulletin-2008; and the chapter on China, and especially on surveillance, in Privacy and Human Rights 2006, note 119, p. 335.

> Freedom and privacy of correspondence of citizens of the People's Republic of China are protected by law. No organisation or individual may, on any ground, infringe upon citizens' freedom and privacy of correspondence, except in cases where, to meet the needs of State security or of criminal investigation, public security or procuratorial organs are permitted to censor correspondence in accordance with the procedures prescribed by law.[234]

This establishes a limited sectoral right to privacy in relation to correspondence. This is, however, subject to wide-ranging exceptions, which are only bounded by the constraint that they be established by law. Article 38 of the Constitution provides general protection for the personal dignity of citizens, providing that "[i]nsult, libel, false accusation or false incrimination" are prohibited. This has been interpreted by courts as providing a general basis for the right to privacy, as linked to the wider notion of reputation. Protection for reputation, found at Article 101 of the 1986 General Principles of the Civil Law,[235] has been used as a basis for protection of privacy as well. However, this is done only where there has also been a primary breach of reputation, so that the scope of protection for privacy per se is rather limited.

The Seventh Amendment to the Criminal Law introduced certain criminal provisions on privacy. Employees of public bodies, or financial, telecommunication, transportation, education or medical organisations, are prohibited from selling or otherwise unlawfully disseminating personal information which they obtained in the course of their employment. Offenders shall be sentenced to a minimum of three years' imprisonment, provided that the behaviour reaches a certain level of severity. Anyone who obtains such information by theft or other unlawful means shall be subject to the same punishment, again provided that the behaviour reaches a certain level of severity. Organisations committing these offences shall be subject to monetary penalties, and their directors and other responsible officers subject to the same punishment as individuals committing these offences.[236]

This is significant inasmuch as it represents the first independent action for breach of privacy in China. At the same time, in common with many national laws in China, it is drafted at a very general level, leaving key terms undefined. These include 'personal information', other illegal means of dissemination, and the level of severity which would engage responsibility. The first conviction under these provisions was reportedly entered on 3 January 2010, by a court in Zhuhai, for the purchase and subsequent sale of a log of telephone calls made by a senior government official.

Another significant development came with the adoption of the Tort Liability Law on 26 December 2009, which came into force on 1 July 2010. This established a separate tort relating to privacy, giving rise to a private right of action for damages. The party claiming breach of privacy may claim any profits which the plaintiff may have made, as well as damages for emotional harm. A website operator who becomes aware or is informed that another party's privacy or other rights have been infringed as a result of content hosted on their website and fails to remove that content is jointly and severally liable

---

234 Available at: http://www.npc.gov.cn/englishnpc/Constitution/node_2825.htm.

235 Adopted 12 April 1986. Available at: http://en.chinacourt.org/public/detail.php?id=2696.

236 Unofficial translation of the text by McKenzie and Milner, China Update, March 2009: Recent Developments in Data Protection, 9 March 2009 (Morrison Foerster). Available at: http://www.mofo.com/international/CN_en/news/15332.html.

with the person who posted the content. Furthermore, if the offended party asks for the registration information of the posting party, the website operator must either provide that information or become directly liable for the content. These rules are problematical from a freedom of expression perspective because (amongst other things) they do not require any proof that the material does breach a privacy right before it may be removed. Finally, medical institutions may be sued for damages if they are responsible for unauthorised disclosures of patients' medical records.[237]

This represents an important extension of the criminal protections adopted earlier. Of particular relevance is the fact that they vest a right of action in individuals to protect their own privacy rights.

There have been proposals to introduce a fully-fledged data protection law in China, although these have not yet come to fruition. In 2006-7, a Personal Information Protection Act, drafted by the Institute of Law at the Chinese Academy of Social Sciences, was being considered by the Informatics Committee of the State Council. However, that Committee no longer exists. Greenleaf describes the situation as follows:

> In China data privacy laws have for the last five years been in what could be called the 'warring states' period, where the states in question are the many fiefdoms in the labyrinthine bureaucracies of the PRC.[238]

(XVIII) Republic of Korea: real names rule

In July 2007, the Republic of Korea adopted the Real Name Verification Law. In its current version, it requires all websites with daily traffic of over 100,000 visitors to identify users who upload material or post comments by their real names, in practice usually through Resident Registration Numbers (RRNs). The law aims to address problems such as the growing number of libellous and fraudulent accusations made online, invasions of privacy and cyber-bullying.

Technically, the rules do not require companies to create databases of personal information, since they have the option of requiring users to provide the data each time they log on. Yet this is impractical, since most users will not be prepared to do this. Google has refused to comply, and has instead prevented users from uploading content to the Korean version of YouTube, on the basis that real name verification rules do not "fall in line with Google's principles".[239]

---

237 See Hunton & Williams, Client Alert, January 2010. Available at: http://www.hunton.com/files/News/4bfa5361-4d8f-4c7e-af03-75055a82202c/Presentation/NewsAttachment/7d2612ba-40d6-4884-83de-c01965341d41/new_chinese_tort_liability_law.pdf. See also McKenzie, P. and Milner, G. Data Privacy in China: Criminal Law Developments, 25 January 2010 (Morrison Foerster). Available at: http://www.mofo.com/data-privacy-in-china-civil-and-criminal-law-developments-01-25-2010/.

238 Greenleaf, G., "Asia-Pacific data privacy: 2011, year of revolution?" [2011] UNSWLRS 30, p. 5. Available at: http://law.bepress.com/unswwps/flrps11/art30/.

239 See Reuters, South Korea's net nirvana spawns good, bad and ugly results, 5 December 2011. Available at: http://www.msnbc.msn.com/id/45562846/ns/technology_and_science-tech_and_gadgets/t/south-koreas-net-nirvana-spawns-good-bad-ugly-results/#.Tw6t7Jj6QTM. See also http://www.zdnet.com/blog/foremski/google-refuses-compliance-with-korean-real-name-law-but-imposes-it-on-g-users/1920.

> The occurrence of massive data breach in July 2011, in which hackers allegedly stole the personal details of a reported 35 million Koreans from the company SK Communications (see box above) has led to renewed calls to repeal the law, which exacerbated the effects of the leak. In late December 2011, the country's Internet regulator, the Korea Communications Commission, said that it would review the policy and the consensus seems to be that it is likely to revoke it.[240]

Another significant development was the issuance, in February 2011, of the draft Information Security Technology Guidelines for Personal Information Protection. The Guidelines were issued jointly by the Ministry of Industry and Information Technology (MIIT) Standardisation Administration of China (SAC) and the General Administration for Quality Supervision, Inspection, and Quarantin; these constitute a non-binding set of data protection rules.

The Guidelines, which apply to information processed on computers, define personal information broadly as any information which, alone or in combination with other information, may be used to identify an individual. The purpose of processing (including collecting) personal data must be clear and reasonable, and the subjects should be notified about the purpose and the entity processing the data, as well as their rights (which include how to access the data, to correct the data and to object to further processing) and how to complain. Only data which is relevant to the purpose may be collected. Data must be kept confidential and must only be used for the stated purpose, unless another purpose is provided for by law or clearly agreed to by the subject. Special rules apply to certain types of particularly sensitive data. Consent from a guardian is required before data from individuals under 16 years of age may be processed.

The Guidelines have strict rules on transfer of data. Transfer to third parties is allowed only with the consent of the subject, where provided for by law or where the oversight body authorises it. Unlike in most systems, no exceptions to this are provided for, making it a very strict, and perhaps even unworkable, scheme.

The rules on foreign transfers are even more rigid, as this is allowed only where authorised by law or approved by the oversight body (and not even when consent of the subject is provided). Given that there are currently no laws authorising such transfers (perhaps understandable since the matter has not come up before), and no exceptions to the need for specific authorisation (either by law or as authorised by the oversight body), this represents a very strict constraint on the cross-border flow of data.

As the Guidelines are not binding, they may to some extent be soft tested in practice, perhaps as a prelude to the adoption of legally enforceable standards. This is just as well, given that, in their current form, they are considered by some as being impractical.[241]

---

240 See http://www.hancinema.net/real-name-internet-law-on-way-out-36915.html

241 See McKenzie, P.; Dicker, A. and Fang, J. China Issues New Guidelines on Data Privacy Protection, 11 April 2011 (Morrison Foerster), available at: http://www.mofo.com/files/Uploads/Images/110411-China-Data-Privacy-Guidelines.pdf; Fernández, China Publishes Draft Privacy Guidelines, 14 April 2011 (Hogan Lovells), available at: http://www.hldataprotection.com/2011/04/articles/international-eu-privacy/china-publishes-draft-privacy-guidelines/; Ross, L., Gao, K., and Zhou, A., China Issues *Draft Guidelines on Online Privacy, Announces new Agency to Supervise the Internet*, 19 May 2011 (Wilmer Hale).

A number of provisions in Chinese laws and guidelines adopted since 2009 provide sectoral protection for personal data in the areas of money laundering, medical records, insurance, consumer protection and credit reporting.[242] There has also been some legislative/regulatory activity at the local (provincial and municipal) level to protect privacy, for example in consumer laws and in relation to computer systems.[243]

3.2.2 India

Until recently, South Asia was decidedly behind in terms of giving protection to data protection and privacy more generally, leading one author to describe it in 2009 as the "final frontier" for data protection in Asia.[244] A couple of years later the situation in India, at least, had changed significantly.

The Indian Constitution does not include a freestanding right to privacy. However, the Supreme Court has read in a right to privacy mainly as part of the Article 21 right to life and liberty, which reads as follows: "No person shall be deprived of his life or personal liberty except according to procedure established by law." Thus, in a 1994 case, the Supreme Court stated:

> The right to privacy is implicit in the right of life and liberty guaranteed to the citizens of this country by article 21. It is a "right to be left alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood and education among other matters. None can publish anything concerning the above matters without his consent. If he does so, he would be violating the right to privacy of the person concerned and would be liable in action for damages.[245]

There is still no independent civil law on privacy in India, although one has been under discussion for a number of years. As a result of the 1994 case noted above, however, courts have had to find a remedy for privacy invasions since the Supreme Court in that case held that publication of private matters, "whether truthful or otherwise" would be a breach of the right to privacy. To do so, courts have looked mainly to general common law rules, such as breach of confidence.

A comprehensive Privacy Bill has been under discussion in India for some time, although at the time of writing one has still not been adopted. A draft dated 19 April 2011, and titled "Third Working Draft (For Discussion and Correction) Legislative Department", was originally leaked but is now available online.[246] The Bill would create a broad freestanding privacy right, along with a strong mechanism to address breaches of the right, called the Data Protection Authority of India (DPAI).

The Bill defines privacy broadly to include such things as privacy of communications, private and family life, banking and medical information, data protection and various

---

242 See Greenleaf, note 207, p. 7.

243 See McKenzie and Milner, note 236.

244 Greenleaf, G., "Twenty-one years of Asia-Pacific data protection" (2009) 100 *Privacy Laws & Business International Newsletter 21*.

245 *R. Rajagopal v. State of Tamil Nadu* (1994) 6 SCC 632. This case extended the right of privacy by placing an obligation on the State to prevent private intrusions. The right was first recognised by the Supreme Court in Govind v. State of Madhya Pradesh & Anr (1975), SCR (3) 946.

246 Available at: http://bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf.

protections against State actions, for example in the areas of search and surveillance. Importantly, the scope of the law is limited to Indian citizens, thereby leaving the very significant Indian outsourcing activities outside of its scope. Certain pre-existing legal regimes, including those addressing the right to information and corruption, are specifically exempted from the application of the law, but it seems that the Bill would preserve all pre-existing laws in the area (see section 3).

The DPAI would have extensive powers including to act as the registrar of data controllers, to investigate abuses, and to require data controllers to take certain actions to bring abuses to an end. The DPAI would also have the power to receive some (as yet unspecified) complaints. Individuals would also be able to complain to the Cyber Regulations Appellate Tribunal, which is established under Section 48 of the Information Technology Act, 2000,[247] which would have the power, among other things, to impose compensation for breaches.[248] As noted, however, this remains a Bill which could be subject to significant change before being passed into law.

Various Indian laws provide protection against privacy invasions by the State, for example in the area of law enforcement although, as in all countries, these are subject to overrides. Thus, the Penal Code requires police to obtain warrants before conducting a search. These rules are modified by constitutional jurisprudence at the Supreme Court which has, for example, held that wiretaps are a serious privacy invasion which, as a result, requires a high level of justification.[249]

Telecommunications are generally protected pursuant to the Indian Telegraph Act, 1885,[250] as well as the Information Technology Act, 2000. The latter, as amended, has introduced a limited criminal offence for certain violations of privacy online.[251] Amendments to the latter in 2008 provided for the interception of telecommunications where necessary or expedient to protect the sovereignty, integrity or security of India, friendly relations with other States, public order, incitement to crime or the undermining of investigations into offences.[252] The Telecommunications Regulatory Authority of India (TRAI), established by the Telecommunications Regulatory Authority of India Act, 1997,[253] also has broad powers in this area, and has issued various legal orders to protect privacy of communication.[254]

Mention should also be made here of the Right to Information Act, 2005,[255] which provides for access to all information held by public authorities, to the exclusion of any other law

---

247 No. 21 of 2000.

248 For more information on the Privacy Bill see Gupta, A., "Analysis of the Privacy Bill, 2011" on India Law and Technology Blog, 27 June 2011 and Greenleaf, G., "India's U-turns on Data Privacy" a series of four papers published in (2011) 110-114 *Privacy Laws & Business International Report*.

249 See *People's Union for Civil Liberties (PUCL) v. Union of India and Anr*. (1997) 1 SCC 301.

250 No. 13 of 1885. See, for example, sections 5 and 7.

251 See section 66-E.

252 The Information Technology (Amendment) Act, 2008, No. 10 of 2009, section 34, amending section 69 of the original act and introducing new sections 69A and 69B.

253 No. 24 of 1997.

254 See, for example, Direction under section 13, read with sub-clauses (i) of clause (b) of sub-section (1) of section 11 of the Telecom Regulatory Authority of India Act, 1997 (24 of 1997) to ensure compliance of the terms and conditions of the licence by the service providers regarding confidentiality of information of subscribers and privacy of communications, 26 February 2010.

255 No. 22 of 2005.

which prevents such access, subject only to the exceptions it provides for. Section 8(j) of the Act protects privacy in the following terms:

> [I]nformation which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information:

Provided that the information which cannot be denied to the Parliament or a State Legislature shall not be denied to any person.

This incorporates a strong public interest override for privacy.

Last, but by no means least, on 11 April 2011, the Indian Ministry of Communications and Information Technology adopted the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, pursuant to section 43A of the Information Technology Act, 2000. These are essentially a mini-data protection regime with much of the flavour of similar regimes in other countries. One interesting twist is that they apply exclusively to the private sector, a difference from most other countries where these rules apply first and foremost to the public sector and then perhaps also to the private sector.

In terms of substance, the rules require data controllers to have in place data protection policies which provide a clear statement of their practices and policy, indicate the type of data collected, the purposes of that collection, the disclosure of the information and the security protection in place to protect it (section 4). Many of the rules are limited in scope to sensitive personal data, such as medical or financial information, but also including information on sexual orientation. The rules also, however, require reasonable notice of collection and purposes of collection of personal data, as well as the intended recipients. Data may only be used for the stated purposes and there are also rules on access and correction of data, and security (section 5). Compliance with IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security Management System – Requirements" is deemed to provide sufficient information security (section 8).

While the precise scope of these rules remains to be determined, and while they are somewhat limited compared to many countries, it is at the same time true to say that the adoption of these rules has vaulted India to a new level of protection for personal data.

3.2.3 Egypt

Historically, protection for privacy has not been a priority in Egypt. The security forces were able to access significant amounts of personal information, whether online or offline, although formally this was regulated by the Criminal Procedure Code. There is no dedicated law providing for protection for privacy. It remains to be seen whether this will change with the revolution and the broad democratic changes it has brought.

At the time of writing, the constitution of Egypt was the Constitutional Declaration which was proclaimed by the Supreme Council of the Armed Forces on 23 March 2011, following a referendum on 19 March 2011 regarding nine transitional articles. The

Declaration contains, in addition to these nine articles, 49 articles carried over from the 1971 Constitution, including (now) Article 11, which states:

> The inviolability of the private lives of citizens is protected by law. Correspondence, telephone calls and other private and confidential means of communication may not be confiscated or investigated or monitored except with a judicial warrant and for a specific issue, in accordance with the provisions of law.

At the time of writing, there was no comprehensive privacy law or any data protection law. Privacy rules are found in a number of pieces of sectoral legislation, but they tend to be contradictory in nature. A good example of this is the privacy rules in the law on telecommunications.[256] Article 13, describing the role of the regulator, the National Telecommunication Regulatory Authority (NTRA), provides that it shall monitor the execution of telecommunications licences to ensure that the rights of users, and "especially their privacy rights", are guaranteed.

However, Article 64 provides that all telecommunications service providers must ensure that their systems include the technical potential to "enable the Armed Forces, and National Security Entities to exercise their powers within the law". Formally, this shall be done with "due consideration to inviolability of citizens private life as protected by law", but the generality of Article 64, as well as the overall focus of the legal framework, meant that this was largely ignored in practice in the past.

Article 58 of the law requires the NTRA to maintain a database of those who have been licensed to use the frequency spectrum, providing that this "database shall be classified in order to protect the privacy" of licensees. In most countries, such information is made public, on the basis that the frequency spectrum is a public resource and that the public has a right to know who has been given a licence to use it.

3.2.4 France

France is a country which prides itself on its strong protections for privacy. While there is generally strong national support for this, the system came under increasing scrutiny in the aftermath of the Strauss-Kahn affair, where it was considered that undue protection in France of the private lives of the rich and famous prevented the media exposure of Dominique Strauss-Kahn's historically (and allegedly) immoral acts.[257]

Surprisingly, given this, the 1958 French Constitution does not provide for explicit protection for privacy. However, in 1995 the Constitutional Court (Conseil Constitutionnel)

256 Telecommunication Regulation Law, Law No 10 of Year 2003.

257 See, for example, Gopnik, A., D.S.K.: French Lives, French Laws, 16 May 2001. Available at: http://www.newyorker.com/online/blogs/newsdesk/2011/05/dsk-french-lives-french-law.html.

ruled that the right was implicit in the constitution,[258] and this was confirmed in a decision in 1999.[259]

Article 9 of the Civil Code, added in 1970,[260] provides protection for privacy, stating simply: "Everyone has the right to respect for his private life." The second paragraph of this article makes it clear that, in addition to compensation, courts may order "sequestration, seizure and others, appropriate to prevent or put an end to" the invasion of privacy, and on an interim basis in an emergency. These rules are applied via Article 1382 of the Civil Code, which establishes the general principles of liability for civil wrongs.

In practice, French courts have applied these rules robustly, interpreting private life to include, among other things, love life, friendships, family circumstances, leisure activities, political opinions, trade union or religious affiliation, and state of health.[261]

France also has strong criminal provisions on privacy, found at Articles 226-1 to 7 of the Penal Code. Pursuant to Article 226-1, it is a crime, punishable by up to one year's imprisonment and a fine of up to Euro 45,000, wilfully to violate the private life of another person without their consent by:

(1) intercepting, recording or transmitting words uttered in confidence or in private circumstances;

(2) taking, recording or transmitting the picture of a person in a private place.

Consent is, however, presumed where these actions are performed in the sight and knowledge of the person and he or she did not object, despite being in a position to do so. These provisions, which are limited to private places and confidential utterances, are widely understood as being aimed primarily at the paparazzi.

Article 226-2, aimed more at the media, applies the same penalties to the keeping, bringing to the knowledge of the public or using in any manner documents or recordings obtained in breach of Article 226-1. Article 42 of the Law on the Freedom of the Press of 29 July 1881 assigns liability for these crimes, when committed in the press, normally to the editorial director (or editor-in-chief). Pursuant to Article 226-6, criminal proceedings under these articles may only be initiated upon receipt of a complaint from the victim.

Law n° 91-646 of 10 July 1991, entitled relative to secrecy of correspondence emitted by way of electronic communications, protects, as the name suggests, the secrecy of electronic communications. Pursuant to Article 3, interception of communications can, exceptionally, be authorised for purposes such as maintaining security, combating terrorism or crime, or protecting essential economic or scientific interests of the country. Strict procedures govern the authorisation of such interceptions, pursuant to Article 4

---

258 Décision n° 94-352 DC du 18 janvier 1995, Recueil, p. 170 – Journal officiel du 21 janvier 1995, p. 1154. Available at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1995/94-352-dc/decision-n-94-352-dc-du-18-janvier-1995.10612.html.

259 Décision n° 99-416 DC du 23 juillet 1999, Recueil, p. 100 – Journal officiel du 28 juillet 1999, p. 1125. Available at: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/1999/99-416-dc/decision-n-99-416-dc-du-23-juillet-1999.11847.html. See, in particular, para. 45.

260 Act no 70-643 of 17 July 1970.

261 See ambafrance-us.org/spip.php?article640.

(they must ultimately be authorised by the Prime Minister or one of two other specially authorised people).

France also has a long-standing and strong regime for the protection of personal data, in the form of the 1978 Data Protection Act.[262] As amended, the Act fully implements the EU Data Protection Directive, including by establishing the "Commission nationale de l'informatique et des libertés" (CNIL) as an independent administrative oversight body. One interesting feature of the French law is that it requires data controllers to define a retention period compatible with the intended purpose (Article 30(I)(5)).

France has also implemented the EU Data Retention Directive, requiring telecommunications providers to retain traffic data for one year. This is currently being challenged before the State Council (Conseil d'État), France's highest administrative court, by some 20 Internet companies active in France.[263]

France has moved to implement EU Directive 2009/136, or the 'Cookies Directive'. An Ordinance giving effect to the Directive was adopted by the French Council of Ministers on 24 August 2011. Users will now have to be informed about the installation and use of cookies, which under the rules needs to be done before the first cookie is installed. However, under the French rule, if browsers are set up to allow programmes to install cookies, the default situation on most computers is that users are not required to provide express consent.[264] This would seem to be a solution that veers towards satisfying industry interests, rather than forging a strong privacy path, and it remains to be seen whether it will be deemed acceptable as a means of implementing the Directive.

(IXX) Constitutional guarantees for data protection in Latin America

A relatively unique feature of Latin American countries is the strong prevalence of explicit constitutional guarantees for data protection or for the more limited right of habeas data. In most other countries, privacy guarantees are rather generic in nature but, according to some estimates, nearly two-thirds of Latin American constitutions include such explicit protection. Some examples are:

Mexico: Section 6 of the Constitution states: "Everyone has the right to the protection of their personal data."

Brazil: Article 5(0)(LXXII) of the Constitution states: "the right to habeas data is granted:

(a) to ensure knowledge of information relating to the person of the petitioner, contained in records or data banks of government entities or of public entities;

---

262 Act n° 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, as amended by Act n° 2004-801 of 6 August 2004 relating to the protection of individuals with regard to the processing of personal data.

263 See News Wires, Internet giants challenge French data law over privacy, 6 April 2011. Available at: http://www.france24.com/en/20110406-internet-giants-challenge-france-data-law-privacy-google-facebook-ebay. It is not clear where proceedings are in this case at present.

264 See http://www.privacysecuritysource.com/2011/09/09/france-implements-the-cookies-directive-and-strengthens-its-privacy-laws/.

(b) for the correction of data, if the petitioner does not prefer to do so through confidential, judicial, or administrative proceedings;

Uruguay: Article 66(19) of the Constitution states: "The following rights of persons are recognised and guaranteed: The right to protection of personal information, including access to and decision about information and data of this nature, as well as its corresponding protection. The gathering, filing, processing, distribution or dissemination of these data or information shall require authorisation from the holder or a court order."

3.2.5 Argentina

The Constitution of Argentina includes a freestanding right to privacy, along the lines found in many constitutions, in Article 19, which states:

> The private actions of men which in no way offend public order or morality, nor injure a third party, are only reserved to God and are exempted from the authority of judges. No inhabitant of the Nation shall be obliged to perform what the law does not demand nor deprived of what it does not prohibit.[265]

It also, in line with many Latin American constitutions, provides for a right to habeas data, in Article 43, as follows:

> Any person shall file this action to obtain information on the data about himself and their purpose, registered in public records or data bases, or in private ones intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired.

The Civil Code also provides protection for privacy, at Article 1071bis,[266] which provides broadly for protection of privacy, where this is not a criminal offence. In case of a breach of a privacy right, the court shall order the cessation of the invasive activity, if this has not already happened, and may also order payment of damages. Where this would be equitable, the court may also require the publication of the judgment in a journal or newspaper. This article is frequently applied in Argentina to protect various sorts of privacy interests.

In a series of cases, courts in Argentina have issued preliminary injunctions against the search engines operated by Google and Yahoo!.[267] In all of these cases, personal data of the plaintiff(invariably a celebrity or well-known figure), such as the name or an image, was being posted on third party websites without their consent, usually to promote the sale of sexual content or services. Instead of pursuing those directly responsible, the

---

265 See also the *Ponzetti de Balbín* case, note 128.

266 Added by Article 1 of Law N° 21.173, published in the *Official Gazette* on 22 October 1975.

267 Much of the information about these cases comes from Compa, E. and Bertoni, E., Emerging Patterns in Internet Freedom of Expression: Comparative Research Findings in Argentina and Abroad (Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE)). Available at: http://www.palermo.edu/cele/libertad-de-expresion-en-Internet.pdf.

plaintiffs went after the search engines. This was undertaken presumably in the hope of cutting off access in a more systematic way.

In many cases, preliminary injunctions were issued against the search engines, on the basis that they had exacerbated this breach of the plaintiffs' privacy rights. They were often ordered not only to sever their links to the specific websites cited in the cases, but also to similar websites. Not only is this either extremely difficult or perhaps technically impossible to do, but it also represents a breach of international law.[268]

It remains unclear how this will eventually play out, although some of the early decisions have now been overturned. Thus, in the case of Virginia da Cunha c/ Yahoo de Argentina y Otro,[269] decided in July 2009, damages of ARS50,000 (approximately USD12,000) were assessed against both Google and Yahoo!. However, in August 2010, the decision was overturned by a 2-1 decision of the Court of Appeal.[270]

The Argentine Penal Code, as amended by Law N° 26.388 on violations of electronic communications and other norms,[271] provides sanctions for various information technology crimes. This law has been renamed Title V of Chapter III of the Penal Code as "Violation of Secrets and Privacy". Article 153, which addresses violations of electronic communications, makes it a crime to access and obtain, without consent, any electronic communication, letter, attachment, fax or telegraph. It is also a crime for any unauthorised person to delete or divert electronic communications, or to intercept or record them. Unauthorised access to private or public databases and information technology systems, and providing information from them to third parties, was also made a crime.

Argentina was one of the early countries in Latin America to adopt a data protection law, in the form of the 2000 Personal Data Protection Act.[272] That the law provides strong protection for personal data can be seen in the fact that Argentina is the only country in Latin America that has been generally approved as providing an adequate level of protection for personal data by the European Commission.[273] It appears that the law draws from European data protection standards.[274]

3.2.6 Mexico

The Mexican Constitution provides extensive protection for privacy at Article 16, which provides, in relevant part:

> Nobody can be disturbed in his or her person, family, residence, papers, or possessions, except by virtue of a written order by a competent authority, that is founded in and motivated by legal procedural cause.

---

268 See, for example, the 2011 Joint Declaration on the Internet and Freedom of Expression of the four special international mandates on freedom of expression, available at: http://www.law-democracy.org/wp-content/uploads/2010/07/11.06.Joint-Declaration.Internet.pdf.

269 Da Cunha Virginia c/ Yahoo de Argentina SRL y otro s/ Daños y perjuicios (Juz. Nac. En lo Civil nø 75, Expte. Nø 99.620/06), 29 July 2009.

270 See http://www.nytimes.com/2010/08/20/technology/internet/20google.html.

271 Published in the *Official Gazette* on 25 June 2008.

272 Law 25.326, promulgated on 30 October 2000.

273 See http://ec.europa.eu/justice/policies/privacy/thridcountries/index_en.htm.

274 In his survey, Greenleaf assesses the Argentine law as having nine of the ten attributes of the European system that are lacking in the OECD system. Note 207, p. 10.

> In all search orders, which only the judicial authority has the power to execute, and which will be written, the place to be inspected will be stated, and also the person or persons to be apprehended and the objects to be looked for. Care shall be taken to limit the search to be conducted as a circumscribed act, in the presence of two witnesses designated by the occupant of the searched place; or in their absence or refusal, the searching authorities will practice care.
>
> Private communications are inviolable: The law will sanction criminally any act committed against their liberty and privacy. Only the federal judicial authority, upon petition to the federal authority that enforces the law or to the head of the Public Ministry of the corresponding federated entity, may authorise the interception of any private communication. For this, the appropriate authority, by writing, must establish and justify the legal causes for the application. It must, besides, give the type of interception, its subjects, and its duration. The federal judicial authority may not grant these authorisations in electoral, fiscal, mercantile, labor, or administrative matters, or in the case of communications by an accused with his or her defender.
>
> Authorised interceptions will conform to the requirements and limits given by the laws. The result of interceptions that do not comply with them, will lack all investigative value.
>
> Administrative authority may visit residences only to ascertain that they comply with sanitary and police regulations, and to require the showing of those books and papers that are indispensable for verifying that the residents are paying attention to the financial arrangements subject in those cases to the respective laws and formalities prescribed for searches.
>
> Correspondence that is covered by the mail shall be free from all examination, and its violation will be punished by the law.

It thus provides strong protection for privacy generally, against searches and for privacy of communications.

The Federal Civil Code provides for civil protection for the right to privacy. Specifically, it provides remedies against moral damage suffered by an individual as a result of illegal acts affecting his or her "sentiments, affections, beliefs, decorum, honour, reputation, private life, configuration or physical aspects, or the opinion that others have of [him or her]". There is some litigation under these provisions.[275]

Since 2002, there has been protection for personal data held by at least Federal public authorities through the Federal Transparency and Access to Public Government

---

275 See, for example, *Solís v Radiomovil Dipsa SA de CV* (Case 642/99), cited in Schmidt, L. and Arceo, A. "Image and publicity rights in Mexico" in World Trademark Review, September/October 2008.

Information Law,[276] which is the Mexican right to information or freedom of information law. Although this is a right to information law, it includes as one of its purposes to "Guarantee the protection of the personal information possessed by subjects compelled by the Law" (Article 4(III)). Chapter IV of the Law establishes a data protection regime for personal information, which includes such rules as using personal data only for the purposes for which it was collected, guaranteeing the security of this data, making available a policy statement on the use of the data, keeping the data up-to-date and accurate, not disclosing it to third parties (except in certain circumstances), informing the oversight body of the fact that personal data is being collected, and providing for access to and correction of personal data by the subject. Oversight is provided by the Federal Institute of Access to Information (IFAI, now the Federal Institute for Information Access and Data Protection).

The scope of the right to information law is largely limited to federal public bodies. However, a general data protection law, binding on private bodies, was adopted in 2010 in the form of the Federal Law on the Protection of Personal Data Held by Private Parties. According to Greenleaf, this law conforms to only five of the ten key European data protection principles, not including the following:

- collection of data is limited to what is necessary for the declared purposes;
- a requirement to notify the data protection agency when collecting data;
- the obligation to anonymise or destroy data after a given period;
- limits on automated processing of data; and
- a requirement to provide an opt-out for direct marketing uses of data.[277]

At the same time, the law does institute most of the key data protection principles found in other systems.[278] Oversight is again provided by the IFAI.

3.2.7 United States of America

The United States of America is a crucial player in global privacy issues not only because of its general global weight and importance, but also because of its vast dominance in terms of companies providing Internet services. Indeed, of companies that provide Internet services that have become household names globally – such as Google, Facebook, Yahoo!, YouTube, Twitter and Wikipedia – almost all are based in the United States of America.

The United States of America has a long and strong history of providing protection for privacy, characterised by active and often innovative legislative initiatives. Against

---

276 Available at: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB68/laweng.pdf. Available in Spanish, as amended, at: http://www.diputados.gob.mx/LeyesBiblio/pdf/244.pdf.

277 Note 207, p. 11.

278 See, for example, Orantes, J., Cruz, C. and Morales, P., "Legal Update: Decree Enacting the Federal Law for Protection of Personal Data in Possession of a Person, and Amending Paragraphs II and VII of Article 3, and Article 33, as Well as the Heading of Chapter II, of the Second Title, of the Federal Law of Transparency and Access to Public Governmental Information", available at: http://www.theworldlawgroup.com/files/file/docs/Mexico%20DP.pdf, and Blackmer, S., "Mexico's New Data Protection Law", 28 July 2010, available at: http://www.infolawgroup.com/2010/07/articles/data-privacy-law-or-regulation/mexicos-new-data-protection-law/.

this, however, it also has a very strong conception of free speech, including freedom of commercial speech, which has been juxtaposed against privacy claims in many cases. Furthermore, lawmakers have demonstrated a reluctance to legislate specifically for Internet privacy issues out of concern for undermining the enormous vitality of online commerce and/or creating an unworkable regulatory regime. This has led to an interesting overall legal framework which in some areas is globally cutting edge while in others, most notably in the area of data protection, is decidedly not so.

There is no direct guarantee for privacy in the United States Constitution, although a limited right has been derived from a number of other constitutional provisions. The most significant of these is the derivation from the Fourth Amendment – which protects against unreasonable searches and seizures – of a right of privacy against the State by the United States Supreme Court in the 1967 case of *Katz v. United States*.[279] The core concept here is the idea of a zone where individuals have an expectation of privacy, which comprises both subjective (i.e. an actual expectation) and objective (i.e. a reasonable expectation) elements. The fact that this aspect of the right is grounded in the Fourth Amendment prevents it being extended, along the lines of Article 8 of the ECHR, to apply to private actors. There has been a wealth of jurisprudence under these rules. In a recent case, the United States Supreme Court held that attaching a GPS device to a vehicle amounted to a search, which fell within the rules relating to searches (i.e. normally requiring a warrant).[280]

The tort of invasion of privacy, which gives a right of action against both private and public actors, has been recognised in law for over a century, and is now recognised in almost every state. Four different privacy actions are generally protected, including unreasonable intrusion upon an individual's seclusion, appropriation of one's name or likeness, publicity which places one in a false light and unreasonable publicity given to one's private life.[281]

The 1974 Privacy Act establishes a system of data protection, but only for public authorities. Private bodies are, for the most part, free to determine privacy standards for themselves.[282] In many respects, the basic data protection values and principles behind the Privacy Act are similar to those of the EU Data Protection Directive, despite their very different scope of application.[283] At the same time, the institutional arrangements are quite different. Thus, there is no independent data protection oversight body, as required by the EU Directive. Instead, the Office of Management and Budget (OMB) plays a far more limited policy role.

In addition to these two central privacy systems, there are a large number of statutory schemes in the United States of America which focus on various sectors and areas of concern. The 1986 Electronic Communication Privacy Act (ECPA), which essentially brought traditional wiretapping legislation into the online era, provides protection for

---

279 389 US 347 (1967).

280 United States v. Jones, No. 10–1259, 23 January 2012.

281 See, Lake v. Wal-Mart-Stores Inc., 30 July 1998, Minnesota Supreme Court, C7-97-263. See also, Restatement (Second) of Torts, § 652B-E (1977).

282 The implications of the tort of privacy on data protection have been limited. See The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108, note 207, p. 5.

283 Written Statement of Professor Peter P. Swire Moritz College of Law of the Ohio State University Center for American Progress Submitted to the House Energy & Commerce Committee September 15, 2011 "Internet Privacy: The Impact and Burden of EU Regulation". Available at: http://www.americanprogressaction.org/issues/2011/09/pdf/swire_testimony.pdf.

electronic communications. It is divided into three parts or titles, known as the Wiretap Act, the Stored Communications Act and the Pen Register Act. Roughly speaking, the first title ensures confidentiality of communications while they are in transit and the second, as the name implies, does the same for stored communications. The third prohibits the tracing of incoming and outgoing messages. All three may be overridden for various reasons, and the first provides the strongest protection for confidentiality. The 2002 Homeland Security Act (or PATRIOT Act as it is commonly called) has weakened the privacy protections in the ECPA, in particular by expanding security and law enforcement interception powers.

The 1999 Gramm-Leach-Bliley Act effectively facilitates information sharing among financial institutions, while establishing special standards to ensure appropriate protection of privacy.[284] The 1994 Driver's Privacy Protection Act was adopted in response to the sale of motor vehicle records, including a lot of sensitive personal data – such as phone numbers, addresses, personal details and medical information – which had led to a number of high-profile crimes, including the murder of a famous actress. The Telephone Records and Privacy Protection Act of 2006 makes it a crime to use a false pretext to obtain, buy or sell personal telephone records, while the Fair and Accurate Credit Transactions Act of 2003 created certain new privacy rights, for example the right to obtain a free credit report from credit bureaus once a year. It was also part of an overall strategy to address identity theft.[285] The 2000 Children's Online Privacy Protection Act (COPPA) requires parental consent before information is collected from children under the age of 13. It also requires websites to have privacy policies, thus working in tandem with a self-regulatory approach.

The 2004 Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) was an attempt to set standards for spam, although it is largely considered to have had little impact. It does not require recipient consent for spam, but it does require senders to indicate that the message is an advertisement and to provide a valid postal address of the sender. Recipients are also given the right to opt out via a notice provision.

The United States of America has so far refused to adopt data retention rules along the lines of those required by the EU Data Retention Directive. Bills along these lines have been proposed, such as the 2009 Internet Stopping Adults Facilitating the Exploitation of Today's Youth or SAFETY Bill, which was proposed in 2009 but never adopted. It would have required communication service providers to retain for least two years "all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user."[286]

In addition to these federal laws, there has been a lot of activity at the state level focusing on the issue of privacy and the Internet.[287]

---

284 The Electronic Privacy Information Center and Privacy International describe these as "weak". Note 119, p. 1009.

285 See http://www.money-zine.com/Financial-Planning/Debt-Consolidation/Identity-Theft-Regulations/.

286 http://www.wired.com/threatlevel/2009/02/feds-propose-st/

287 Some of these are listed at: http://www.ncsl.org/default.aspx?tabid=13463.

3.2.8 Nigeria

Section 37 of the 1999 Constitution of the Federal Republic of Nigeria provides: "The privacy of citizens, their homes, correspondence, telephone conversations and telegraphic communications is hereby guaranteed and protected." Section 45, however, provides that this shall not invalidate any law that is "reasonably justifiable in a democratic society (a) in the interest of defence, public safety, public order, public morality or public health; or (b) for the purpose of protecting the rights and freedom or other persons." There has, however, been very little constitutional jurisprudence on these issues, which might provide guidance as to the scope of these limitations in practice.

There is no explicit protection for civil invasions of privacy in Nigerian law, but the common law remedy of breach of confidence presumptively applies in Nigeria and may therefore be relied upon for civil protect.[288] As with the constitutional guarantee, however, there would appear to have been very little if any local jurisprudence on this issue.

At the moment, Nigeria does not have any law specifically governing the interception of private communications. Two draft bills on this issue are pending before the parliament, namely the Interception and Monitoring Bill 2009 and the Telecommunications Facilities (Lawful Interception of Information) Bill 2010.[289] Pursuant to the Nigerian Communications Act 2003,[290] there is a presumption that communications are private, but the Act also provides for interception of communications. Thus, section 147 states: "The Commission may determine that a licensee or class of licensee shall implement the capability to allow authorised interception of communications and such determination may specify the technical requirements for authorised interception capability." Section 148 also provides for the interception of communications in case of a public emergency.

Two other bills have been under consideration specifically relating to information protection on computers and the Internet, namely the Computer Security and Critical Information Infrastructure Protection Bill, 2005 and the Cybersecurity and Information Protection Agency Bill, 2008. Section 13 of the former would prohibit the unlawful interception of any communication, but provides a broad authorisation for lawful interceptions, for example for purposes of detection and prevention of crime. The latter similarly prohibits unlawful interception, but requires service providers to have the capacity to intercept communications for purposes of assisting law enforcement agencies (sections 16-17).[291]

Nigerian law does not include any comprehensive data protection regime. Section 12(4) of the Computer Security and Critical Information Infrastructure Protection Bill, 2005 does provide for a very limited form of data protection as follows:

---

288 See Nwauche, E.S., "The Right to Privacy in Nigeria" (2007) 1 Review of Nigerian Law and Practice 63.

289 For more information about these two bills see Udo Udoma & Belo-Osagie, Law: I*ntercepting Private Communications in Nigeria,* 7 March 2012. Available at: http://www.proshareng.com/articles/2406.

290 Available at: http://www.nigeria-law.org/Nigerian%20Communications%20Commission%20Act%202003.htm.

291 For more information on these bills see Akinsuyi, Nigerian Cyber Crime and Privacy Legislations, Time for Review, 9 August 2010. Available at: file:///Users/toby/Documents/Consultancies/Privacy%20-%20UNESCO/Country/Nigeria.Cyber%20Crime%20law.webarchive.

> Any data retained, processed or retrieved by the service provider at the request of any law enforcement agency under this Act or pursuant to any regulation under this section, shall not be utilised except for legitimate purposes. Under this Act, utilisation of the data retained, processed or retrieved shall constitute legitimate purpose only with the consent of individuals to whom the data applies or authorised by a court of competent jurisdiction or other lawful authority.

3.2.9 South Africa

With the end of Apartheid in South Africa, the country was faced with an enormous challenge in building a legal, not to mention social, political and economic, framework for democracy. Some commentators have suggested that, due to the particular historical context, South African energies tended to be focused more on equality rights, to the detriment of framework rights like privacy. Legally, at least, there is some truth to that, as the country still has yet to put in place a data protection act. There are, however, number of legal sources of privacy protection.

The Constitution of the Republic of South Africa of 1996 protects privacy in Section 14, as follows:

Everyone has the right to privacy, which includes the right not to have—

(a) their person or home searched;

(b) their property searched;

(c) their possessions seized; or

(d) the privacy of their communications infringed.

There has been an active history of constitutional litigation in South Africa, including a number of privacy cases.[292] In an analogous fashion to the European Court, the South African Constitutional Court has developed a theory of the horizontal application of rights, so that constitutional protections can apply as between individuals, as well as between individuals and the State.

There is no specific statutory protection for privacy in South Africa but the courts there have long recognised a right of action based on the general Roman law concept of *actio iniuriarum*, or right of action to protect one's person. This has been interpreted to include unauthorised publication of personal facts (such as a photograph), unreasonable intrusions into a private sphere and the right to a personal identity.

At the time of writing, South Africa still lacked comprehensive data protection legislation, although the issue has been under formal consideration since at least 2000. A draft Protection of Personal Information Bill, introduced in the National Assembly in 2009,[293] sought to introduce an essentially European-style system for protection of personal data held by both private and public entities, with rules on consent for processing, specification of purposes, limitation on use for other purposes, limitations on retention,

---

292 See Burchell, J., "The Legal Protection of Privacy in South Africa: A Transplantable Hybrid", 13.1 Electronic J*ournal Of Comparative Law*, (March 2009), pp. 11-13.

293 Published in the Official Gazette on 14 August 2009.

requirements of notification to both the subject and oversight body, and rights of access and correction for the subject. The Constitutional Court has also set out a very basic framework for data protection, based on the constitutional protection of privacy.[294] Strong personal data protection rights are also found in the National Credit Act,[295] in part to address historic practices of discrimination in the financial sector. These include a right to have "confidential information" treated in confidence, used only for a lawful purpose and disclosed only to the person to whom it relates.

In terms of communications, the primary legislation is the Regulation of Interception of Communications and Provision of Communication-Related Information Act.[296] This act is similar to others of its genre, providing generally for the confidentiality of private communications and then carving out exceptions for various reasons, in particular security and law enforcement, subject to certain conditions. The Act requires telecommunications service providers to ensure that their services are capable of storing relevant information about communications and can be intercepted, before they offer them to the public. It also requires service providers to store information, as directed by the responsible minister, for between three and five years.

3.3 Corporate initiatives

It is clear that initiatives of some sort by corporations must play a key role in any integrated system for protection of privacy online. In the United States of America, these remain the primary system for data protection in relation to private sector actors. Under European-style systems, they are seen as an important supplement to the mandatory rules internally, and often underpin 'adequacy' decisions for third party data transfers. Article 27 of Directive 95/46 calls on States and the Commission to support the drawing up of codes of conduct for the purposes of self-regulation, and the new proposals extend this by creating the possibility of establishing certification mechanisms for self-regulatory systems, along with data protection seals and marks, to enable users to assess the quality of these systems. In his introductory remarks to an independent study on new data protection directions for Europe, Richard Thomas, the United Kingdom's Information Commissioner opines that, in the long run, abandoning the rules and placing the onus on data exporters for protection of data transferred to third parties (a form of self-regulation) may be inevitable.[297]

At the same time, there is no shortage of criticism of systems of self-regulation which, it is widely agreed, have not resulted in adequate protection for users' privacy in the United States of America. Dan Tynan described the problem by way of analogy: "When it comes to the online ad industry, self-regulation is a bit like the Pirate's Code in all those Johnny Depp movies: They're really more like guidelines that can be broken whenever the script calls for it."[298]

---

294 Burchell, note 292, p. 14.
295 No. 34 of 2005.
296 No. 70 of 2002.
297 See Robinson, Graux, Botterman and Valieri, Review of EU Data Protection Directive: Summary, note 215, Foreword.
298 "Privacy pirates: Self regulation is a sinking ship", 9 August 2011. Available at: http://www.itworld.com/it-managementstrategy/191917/privacy-pirates-self-regulation-sinking-ship.

Self-regulatory initiatives take various different forms. Many ISPs and the larger, more high profile online service providers (OSPs),[299] like Google, Yahoo and Facebook, have developed their own privacy policies. Google has a new privacy policy which came into effect on 1 March 2012.[300] A related option is for entities to come together in a network or association with a central privacy policy or set of standards. Respect for this policy is a condition of membership. This is the approach adopted by the groups such as the Direct Marketing Association (DMA)[301] and TRUSTe.[302] Their members are allowed to display a seal or certification attesting to their membership and commitment to the collective standards.

In terms of substance, there are a number of policy approaches. Most policies make certain commitments to users, and many allow users to select certain privacy options. Thus, the homepage of each Facebook user contains a drop-down menu which takes you to options like account settings, privacy settings and logout. Under 'privacy settings', one can block people from seeing one's content, set other viewing options for one's Facebook content and so on. One cannot, however, control the use Facebook itself makes of your private data, although various aspects of this are covered by its privacy policy.

In some cases, policies allow users to opt out of having their data used for various purposes, mostly marketing. Thus, the Network Advertising Initiative (NAI)[303] provides users with an opt out option on the front page of its site, which prevents you seeing tailored advertisements from the member companies you have opted out of. However, this does not prevent cookies being placed on your computer or remove personal data from databases. A more powerful option, used by some facial recognition networks, such as the Digital Signage Federation (DSF)[304] and Point of Purchase Advertising International (POPAI),[305] is based on an opt in, whereby member companies are supposed to gain users opt-in before collecting certain types of data.

There are a number of structural reasons why the effectiveness of self-regulation has been limited. One is that many systems place most of the burden on the user. Many privacy policies are long, complex and highly legalistic, and users may not understand them or their privacy options. Even if they do make the effort for ISPs and OSPs that they use regularly, they cannot possibly do this for all of the services they use that might be in a position to collect data from them. In an attempt to simplify matters for its users, Google has recently announced that it is combining privacy policies on all of its services, so that users will only need to acquaint themselves with one version.[306] In the vast majority of cases, entities reserve the right to change their privacy policies without notifying users, creating a further barrier for users.

Another problem is that while the incentives to act in privacy-respecting ways may be present for some companies – particularly those that are larger and more well-known –

---

299 OSPs are entities that offer online services such as web hosting, email services, social networking, blogging platforms and so on.
300 Available at: http://www.google.com/policies/privacy/.
301 See www.the-dma.org.
302 See www.truste.org.
303 See www.networkadvertising.org/.
304 See www.digitalsignagefederation.org/.
305 See http://popai.com/.
306 See http://www.google.com/policies/.

for many companies the incentives all line up the other way, since they make money by collecting and selling personal data. It can be costly to implement strong privacy rules. Implementation of many systems is weak, amongst other things because monitoring is costly and rarely done systematically. Finally, implementing privacy policies can actually increase a company's liability, as they may be held responsible for failures to respect those policies.[307]

At the same time, many commentators point to various benefits of self-regulation. It places control and responsibility in the hands of the companies, which are the very entities most likely to understand the privacy risks and to be able to design effective solutions in a very complex and fast-moving environment. Self-regulation is more likely to be sensitive to business needs, and to provide the flexibility businesses need, again in the context of an incredibly dynamic sector. In other words, self-regulation can help protect the economic and social benefits of online innovation.

A number of ideas have been proposed to enhance self-regulatory systems. One is to employ privacy by design, or building privacy systems into the very design of service systems. This no doubt makes good sense, but it cannot resolve many of the problems noted above.

Some co-regulatory ideas would perhaps be more effective. Some commentators, including the Federal Trade Commission (FTC) in the United States of America, have called for the imposition of a 'do not track' system, along the lines of the popular 'do not call' rules that have been put in place in some countries for telephone calls.[308] This system would allow users to opt out of the collection of information relating to their online behaviour for purposes of targeted advertising. This could be achieved, for example, through the placement of a setting on the user's browser indicating their preferences. Another possibility, albeit less stringent in nature, would be to require companies to publicise any breaches of their privacy policies. One commentator has called for legislators to give companies a year to come up with proposals, and then to require all companies to implement the most effective system.[309]

---

307 The Federal Trade Commission (FTC) in the United States, for example, treats violations of a company's privacy policy as a deceptive business practice, which is illegal. See Marsh, "Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet" (2009) 15 *Michigan Telecommunications and Technology Law Review* 543, p. 555.

308 FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers: Preliminary FTC Staff Report*, December 2010. Available at: http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

309 Ibid., pp. 559-562.

4. CONCLUSIONS – INTERSECTIONS BETWEEN PRIVACY AND FREEDOM OF EXPRESSION

The rights to privacy and freedom of expression relate to each other in complex ways. In many instances, respect for the right to privacy supports the right to freedom of expression, as it does other democratic rights. To give an obvious example, respect for privacy of communications is a prerequisite for trust by those engaging in communicative activities, which is in turn a prerequisite for the exercise of the right to freedom of expression.

In other cases, however, respect for privacy can clash with the right to freedom of expression, for example where a newspaper wishes to publish private details about a leading politician, perhaps because the newspaper believes this is in the public interest. An example of this was cited above, whereby some commentators criticised excessive French protection for privacy for the failure of the media and others to investigate allegations of previous questionable acts by former IMF president Dominique Strauss-Kahn.

These relationships are manifested in both traditional and new ways on the Internet, as is evident from both of the examples above (i.e. with online communications systems and online media). Indeed, these issues have come into far greater relief with the massive changes in freedom of expression brought about by the Internet and other digital communications systems (such as mobile phones). For example, the power of the State to track individuals' activities via communications has increased by a quantum degree in line with the massive increase in the data mining potential that digital systems enable.

This part of the report explores these relationships. It looks first at the way freedom of expression is negatively impacted where protection for privacy is poor. It then looks at tensions between the protection of these two rights, in some cases identifying threats to freedom of expression posed by excessive protection of privacy and in other cases simply highlighting the tensions.

4.1 The impact of poor protection for privacy on freedom of expression

The earliest drivers for protecting privacy came from instances of State intrusion into private spaces and this remains a key need for strong protection for privacy online. There has long been a tension between the need for effective law enforcement and respect for privacy, and this is reflected in the huge number of cases, both nationally in many countries and before international human rights courts, claiming a breach of privacy rights by law enforcement officials. This applies most importantly and obviously to digital

communications, but is also relevant in a number of other privacy sensitive areas, such as access to banking and credit information.

This tension has become more complex in recent years due to a number of trends. First, as noted above, the value of available information, from the perspective of law enforcement, has increased massively as new technologies capture far more information about us on an ongoing and automated basis than previously, whether provided voluntarily, for example on a Facebook page, as a necessary part of providing a service, for example logging telephone calls from a mobile phone, or as driven by business interests, for example tracking our online purchasing patterns. The rapidly growing processing power of modern computers delivers a strong multiplier effect here.

For example, the data stored in a modern smartphone of an active user provides a veritable wealth of information about the movements, calls (and so on) of the user. Furthermore, many forms of communication are now automatically recorded and can be computer searched, vastly increasing their effective usefulness for law enforcement purposes. The potential usefulness of facial recognition capabilities, especially when combined with increasingly ubiquitous video surveillance cameras, is another example of this.

Second, from a regulatory perspective, it is much more difficult to control surveillance than in the old offline world. In the past, there were reasonably straightforward rules relating to wiretaps, or monitoring of telephone conversations, albeit often subject to exceptions or overrides and not always applied properly in practice. This activity required the installation or activation of specialised equipment and the putting in place of a specific process of monitoring or recording. Compare this with searching the data stored on a mobile phone seized from a criminal suspect. Furthermore, the ways in which private information is captured and may be accessed is constantly changing, which also poses a regulatory challenge. This is rendered even more challenging by the possibility of voluntary cooperation between ISPs and OSPs and law enforcement authorities, which may be governed primarily by the privacy policies of those service providers.

Third, there has been a clear trend, even among democracies, to put in place legal regimes which facilitate the use of this information for law enforcement purposes. This is driven by the desire to use all available means to counter crime, including the fact that criminal elements often make effective use of technology, particularly for purposes of organised crime and terrorism. However, it is not always clear that privacy concerns are fully taken into account, and many of these regimes have been sharply criticised by privacy advocates. The EU Data Retention Directive, which has fared badly before national constitutional courts, is a good example of this. Furthermore, systems which may be rendered privacy compliant where strong protections for privacy are in place, may still be subject to serious abuse in (the many) countries where privacy protections are weak.

The risk of weak privacy protection is often combined with poor direct protection for freedom of expression, leading to a multiplier effect. There have been some high-profile cases where the Chinese authorities have required OSPs to provide private data which has led to criminal convictions for expressive activities which are protected under international law.

For example, Chinese journalist Shi Tao was given a 10-year sentence in 2005 for email about a government notice on reporting about the anniversary of the 1989 Tiananmen

Square protests. Yahoo! had provided emails from Tao's Yahoo! email account to the Chinese government upon request. These emails provided the basis for Tao's conviction for disclosing State secrets.[310]

In many cases, countries have put in place specific regimes to address expressive activities through the Internet. Thus, the 2007 Thai Computer-Related Offences Commission Act, better known as the Computer Crime Act, has specific provisions on the holding and dissemination of false or pornographic information, or information likely to harm public order or national security, which includes lèse majesté. These provisions have been applied on numerous occasions since the law was adopted.[311] Similarly, the 2088 Indonesian Electronic Information and Transaction Law criminalises the online dissemination of false news, defamatory material and pornography.[312] Both of these regimes have been strongly criticised by freedom of expression activists.[313]

4.2 Tensions between freedom of expression and privacy

The question of tensions between freedom of expression and privacy online is far more complex and varied than that of the impact of poor privacy protections on freedom of expression. While the latter usually involves clear (and often acknowledged) interferences with privacy, sought to be justified on grounds of overriding law enforcement needs, here the very question of what constitutes privacy becomes important. As noted above, both national and international courts have refused to provide a clear definition of privacy, although the approach taken by courts in the United States of America, which involves both subjective (actual expectation of privacy) and objective (reasonably expectation of privacy) elements has much to recommend it.

The scope of the concept of privacy becomes very important in some cases involving freedom of expression. For example, does a minister of defence have a reasonable expectation of privacy when having a private dinner in a restaurant, but with a foreign arms dealer? What if a prime minister is invited to the wedding of a celebrity? This question could be answered differently in different countries, with important implications for media seeking to report on these activities.

This issue also has to be understood in light of the key framework of challenges facing protection of privacy in the online world, and the types of regulatory responses this has engendered. As this report makes clear, there are massive challenges to regulating privacy in the current environment. These include:

- A core business model which effectively involves trading or ceding privacy in exchange for free services.

---

310 See: http://www.businessweek.com/stories/2007-11-06/jerry-yang-on-the-hot-seatbusinessweek-business-news-stock-market-and-financial-advice.

311 See Tunsarawuth, S. and Mendel, T., *Analysis of Computer Crime Act of Thailand* (2010). Available at: http://www.law-democracy.org/wp-content/uploads/2010/07/10.05.Thai_.Computer-Act-Analysis.pdf.

312 Law No 11/2008. See Articles 27 and 28.

313 For Thailand, see *Analysis of Computer Crime Act of Thailand,* note 312 and for Indonesia, see *AJI, Building the Fortress of Freedom* (2009), on file with the author.

- In many cases, service models which also involve exposing private information either as a core part of the model (as, for example, with Facebook) or to create efficiency (for example tools to optimise searches based on a user's typical preferences).
- An environment flowing from the above in which even if incentives can be created, such as public opinion, which exert pressure on some businesses to respect privacy, it is impossible or nearly so to do this for many other businesses.
- An environment which makes informed consent by users for privacy rules almost impossible due, among other things, to the inherent complexity of the rules, the vast number of different applications users use, and an apparent lack of interest or awareness about this among most users, or perhaps acceptance of the trade-off described in the first bullet point above.
- Inherent difficulties in protecting privacy, including due to the incredible fluidity of information and the fact that, once something is "out there", you can never bring it back.

There has been a marked difference in the regulatory response, in particular towards data protection, in the United States of America, (and those countries with similar frameworks), on the one hand, and Europe (and the countries which follow its approach), on the other. The United States of America, where many of the main global OSPs are based, has taken a largely laissez-faire approach, limiting State regulation to certain sectors, which has arguably resulted in inadequate protection for privacy by private actors. Europe, on the other hand, has taken a relatively intrusive approach to regulation, which has been criticised for being too rigid, out of touch with industry realities and ineffective in practice (for example in the area of consent to data collection and use), and, to some extent as a result of these criticisms, for allowing too great an element of discretion in the application of its many exceptions and claw backs.

The main interface between these two approaches is the International Safe Harbor Privacy Principles Certification Program, which allows companies based in the United States of America to be certified as providing adequate protection by the European Union. This system has been criticised for not providing European level protection for privacy, which seems to be patently the case, among other things because of the lack of effective redress. On the other hand, the incentives for the European Union to certify OSPs is clear; it would be nearly impossible for the European Union to refuse companies like Facebook or Google certification.

In terms of specific impacts on freedom of expression, a number of different areas can be identified, as described below.

4.2.1 The public interest

It is well established under international law that where a conflict arises between freedom of expression and privacy, reference should be had to the overall public interest, or some such analogous test, to decide which interest should prevail. This was, for example,

clearly established in the two *Von Hannover v. Germany* cases before the European Court of Human Rights.[314]

The public interest balancing exercise between privacy and freedom of expression is relevant in two main contexts. First, as in the Von Hannover case, the issue arises when information, although private in nature, is accessible to the media, but where the further dissemination of this material is deemed under national law to give unreasonable publicity to private life (or some related wrong). In such cases, a public interest defence, whether cast as an element of the right to freedom of expression or as part of the rules relating to privacy, is essential. Thus, in the second Von Hannover case, the European Court found the publication of otherwise private information to be a justified invasion of privacy (or a protected activity through the right to freedom of expression) essentially because the relationship between the "reigning sovereign of the Principality of Monaco" and members of his family during an illness was a matter of legitimate public concern. Unfortunately, in many countries, this public interest override is either missing from or unclear in the law.

Second, the public interest should be taken into account when applying the privacy exception to the right to access information held by public bodies (right to information). Thus, in a Joint Declaration adopted in 2004,[315] the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression in 2004 stated:

> The right of access should be subject to a narrow, carefully tailored system of exceptions to protect overriding public and private interests, including privacy. Exceptions should apply only where there is a risk of substantial harm to the protected interest and where that harm is greater than the overall public interest in having access to the information.

Similarly, a 2002 Recommendation of the Committee of Ministers of the Council of Europe[316] states, in Principle IV(2):

> Access to a document may be refused if the disclosure of the information contained in the official document would or would be likely to harm any of the interests mentioned in paragraph 1, unless there is an overriding public interest in disclosure.

Although many right to information laws do provide for a public interest override for the privacy exception, many do not.

International courts have provided some indication of how the balancing between freedom of expression and privacy should work. They have made it clear that there is a very strong presumption in favour of freedom of expression, that the notion of public interest in this context should be construed narrowly and that where there is a public interest in publication of the material, the right to freedom of expression will normally

---

314 24 June 2004, Application No. 59320/00 and 7 February 2012, Applications Nos. 40660/08 and 60641/08. The Court referred more to the question of debates on matters of general interest, but this seems to be essentially the same idea, albeit adapted to the facts of the case.

315 Adopted on 6 December 2004. Available at: http://www.unhchr.ch/huricane/huricane.nsf/0/9A56F80984C8BD5EC1256F6B005C47F0?opendocument

316 Recommendation R(2002)2 the Committee of Ministers to Member States on access to official documents, 21 February 2002.

trump the privacy interest. The reason for this is fairly obvious: the right to freedom of expression is a fundamental underpinning of democracy, and discussions about matters of public interest, which are for the benefit of everyone in society, must be protected even if they may cause harm to an individual's privacy.

The case of *Mosley v. the United Kingdom*, involved the publication of private pictures of Max Mosley, then Director of Formula One racing, involved in sexual acts under the heading "F1 boss has sick Nazi orgy with 5 hookers". Mosley eventually won his case before the British courts, in part because the newspaper had been mistaken and there was not Nazi theme to the event, which might have engaged the public interest. He had earlier been refused an interim injunction to prevent further publication of the material; this was applied for only after the initial publication of the material and so much of the damage had already been done. Mosley appealed to the European Court of Human Rights, claiming that the United Kingdom of Great Britain and Northern Ireland had violated his right to privacy by not requiring newspapers proposing to publish privacy invading material to notify the individual(s) concerned, so as to give them an opportunity to apply for an injunction against publication before the initial publication (which Mosley had not had).

The European Court rejected this idea. In a judgment elaborating on the underlying principles, it stated, among other things:

> The Court also reiterates that there is a distinction to be drawn between reporting facts – even if controversial – capable of contributing to a debate of general public interest in a democratic society, and making tawdry allegations about an individual's private life. In respect of the former, the pre-eminent role of the press in a democracy and its duty to act as a "public watchdog" are important considerations in favour of a narrow construction of any limitations on freedom of expression. [references removed][317]

In the two Von Hannover cases, the European Court of Human Rights also elaborated in some detail on the issue of balancing privacy and freedom of expression interests (these are elaborated upon in Box XIII). In those cases, as well, the Court seemed to suggest that where there was a public interest in the publication, the freedom of expression interest would normally prevail. It based this, among other things, on its longstanding position that for the press "its duty is nevertheless to impart – in a manner consistent with its obligations and responsibilities – information and ideas on all matters of public interest".[318]

The same approach has also largely been applied when balancing the right to freedom of expression against reputation, where international courts have again placed great reliance on the importance of allowing significant latitude to speech relating to matters of public interest. Thus, in the case of Herrera-Ulloa v. Costa Rica, which involved a criminal conviction for defamation, the Inter-American Court of Human Rights stated:

> In this context, it is logical and appropriate that statements concerning public officials and other individuals who exercise functions of a public nature should be accorded, in the terms of Article 13(2) of the Convention,

317 10 May 2011, Application No. 48009/08, para. 114.
318 Von Hannover v. Germany, 24 June 2004, Application No. 59320/00, para. 60.

> a certain latitude in the broad debate on matters of public interest that is essential for the functioning of a truly democratic system.[319]

Support for this idea can also be found in the section 12(4) of the United Kingdom of Great Britain and Northern Ireland Human Rights Act, 1998, which states:

> The court must have particular regard to the importance of the Convention right to freedom of expression and, where the proceedings relate to material which the respondent claims, or which appears to the court, to be journalistic, literary or artistic material (or to conduct connected with such material), to-
>
> (a) the extent to which
>
> (i) the material has, or is about to, become available to the public; or
>
> (ii) it is, or would be, in the public interest for the material to be published;
>
> (b) any relevant privacy code.

4.2.2 Privacy vs. data protection

There are important differences between protection of privacy per se and data protection rules. The latter are designed to address the specific problems that can arise when public or private bodies engage in the systematic collection of data about individuals. There is a strong overlap between data protection and privacy, and international courts have held that certain elements of data protection regimes are covered by the right to privacy.

At the same time, data protection rules are different from privacy, both in their scope and substantive rules. Data protection applies to all personally identifying data, while privacy, although it has never been comprehensively defined, applies only to a narrower scope of information, normally information about which a person has a reasonable expectation of privacy. At the same time, data protection rules are more limited inasmuch as, broadly speaking, they only apply to the automated processing of data or the processing of structured data sets, whereas privacy can apply to any information (for example the fact that a person is having dinner with another person in a restaurant).

This is not a problem in itself. However, unlike legal interpretations of the right to privacy, data protection rules do not recognise a general public interest override. In the case of European Union Directive 95/46,[320] there are specific public interest overrides which allow for the processing of data and also for the transfer of data,[321] but not a general public interest override. The same regime also allows States to provide for an exemption from the main rules where data processing is carried out for journalistic, artistic or literary purposes, as necessary to respect the right to freedom of expression. Once again, it may be noted that this is limited in scope, and would not cover many forms of expression (arguably even including this report).

---

319 2 July 2004, Series C No. 107, para. 128.
320 See note 205.
321 See Articles 7(e), 8(4) and 26(1)(d).

In practice, this issue is most problematical when it comes to the right to information. In many countries, there is either a legal link, or confusion at the level of application, between the data protection rules and the exception in favour of privacy in the right to information law.

Better practice right to information laws include a qualifier for protecting privacy which makes it clear that not all identifying information is covered. Thus, section 34 of the South African Promotion of Access to Information Act[322] establishes an exception to prevent the "unreasonable disclosure of personal information about a third party". Such laws also include exceptions to the privacy exception, for example where consent has been given, the information is already public or the information relates to the official functions of a public official.[323] Finally, such laws include a clear public interest override for all exceptions, so that even private information shall be disclosed where this is in the overall public interest. All of these rules are clearly consistent with interpretation by international courts of the right to freedom of expression, upon which the human right to information is based.

At the same time, in many countries, with or without such limitations on the privacy exception to the right of access, the relationship between the right to information and data protection laws is not clear, and the dominant practice in at least some countries is to apply the latter in the case of personal data. In the case of India,by contrast, the proposed Privacy Bill, which would establish a general data protection system, would not affect the regime established by the Right to Information Law, 2005.

4.2.3 Scope of protection and jurisdiction

In some countries, there have been attempts to extend the scope of privacy protection in a way that would negatively impact on freedom of expression. The example of Argentina, noted above, where privacy rules have been applied to search engines on the basis that they led the searcher to privacy infringing data, is a good example of this. Another example is a case from Italy, where three Google executives were each given six month suspended sentences for a video posted on Google Videos showing an autistic boy being bullied, even though the video was taken down promptly after a formal complaint was received. Richard Thomas, former Information Commissioner of the United Kingdom of Great Britain and Northern Ireland, called the case "ridiculous",[324] and Google promptly lodged an appeal against it.

In both of these examples, a reasonable argument could be made that the original authors of the material were guilty of privacy infringements. However, holding OSPs liable in these types of situations, if practised widely, would make it almost impossible for them to continue to provide the important freedom of expression enabling services they currently offer.

Both of these examples involve material which relates closely to the jurisdiction in which the courts were based (Argentine celebrities and an Italian boy). There is, however, also a potential risk of the forum shopping in privacy cases that has been witnessed globally in relation to defamation, in a practice known as 'libel tourism'. Thus, plaintiffs could try to

322 Act No. 2, 2000. Available at: http://www.gov.za/gazette/acts/2000/a2-00.pdf.
323 See section 34 of the South African law, ibid.
324 See: http://news.bbc.co.uk/2/hi/8533695.stm.

bring privacy cases in jurisdictions where they feel they have stronger chance of success, even though they have limited connection to the jurisdiction. This promotes the lowest common denominator in the balancing of privacy and freedom of expression.

An extreme case of this was the defamation action brought against Rachel Ehrenfeld, a New York-based author, by Sheikh Khalid bin Mahfouz, a wealthy Saudi businessman profiled in Ehrenfeld's book, Funding Evil: How Terrorism is Financed and How to Stop It. The courts in the United Kingdom of Great Britain and Northern Ireland heard the case, even though only 23 copies of the book had been sold there, and gave a default judgment in favour of bin Mahfouz (Ehrenfeld had refused to defend the case).[325]

4.2.4 Court information

Privacy concerns, or related concerns, are starting to impact on the way courts present information about their processes. This is an area where there is very little in the way of established standards, even within countries, and where decisions are often left to individual courts or court systems. While the principle of open justice is well established, including in international human rights law, it has normally been applied primarily to the issue of access to court cases, as opposed to court documents.

In some countries, courts are fully included within general right to information laws, and so their openness in relation to documents is determined by that regime. In many countries, however, such coverage is limited in scope, sometimes by being limited to the administrative functions of the court and sometimes by not including the judicial function at all.

Whereas there is an almost universal tendency for public bodies to increase the amount of information they post online,[326] privacy concerns have led to some courts, primarily in the United States of America, where the practice of courts posting information online is most developed, to move in the opposite direction. It is, for example, one thing to publish criminal convictions in a local newspaper and another to post them online, after which they may be accessible at any point in the future, potentially negatively impacting on the ability of the person concerned to get a job or reintegrate into society.

As a result of these privacy concerns, Florida, once a leader in the area, has imposed a moratorium on efforts to expand online access.[327] A case from California involved a businessman who accessed and then sold on information about individuals involved in criminal cases. The issue was whether he could access computer records containing consolidated information about criminal defendants, rather than having to travel to individual courts to get this. The court held that it was the very fact that the information was electronic that gave rise to the privacy concerns:

---

325 See *Mapping Digital Media: Reference Series No. 1: Online Media and Defamation* (2011, Open Society Foundations). Available at: http://www.soros.org/sites/default/files/online-media-and-defamation-20110503.pdf.

326 Along with major international movements to support this, such as the Open Government Partnership (OGP). See: http://www.opengovpartnership.org/.

327 See Open Society Justice Initiative, Report on Access to Judicial Information, March 2009. Available at: http://www.right2info.org/resources/publications/Access%20to%20Judicial%20Information%20Report%20R-G%203.09.DOC/view.

> There is a qualitative difference between obtaining information from a specific docket or on a specified individual, and obtaining docket information on every person against whom criminal charges are pending in the municipal court. … It is the aggregate nature of the information which makes it valuable to respondent; it is that same quality which makes its dissemination constitutionally dangerous.[328]

328 Westbrook v. County of Los Angeles (1994) 27 Cal. App. 4th 157, p. 165.

5. POLICY RECOMMENDATIONS

This report contains an in-depth examination of the issue of privacy on the Internet, from the vantage point of freedom of expression, looking at the various issues involved, international standards and country practice. This section of the report contains our recommendations to States and corporations for better practice, based on international law and the practice of other States, in terms of respecting privacy on the Internet, taking into account potential conflicts with other rights, in particular freedom of expression.

The classical means of resolving tensions between privacy and freedom of expression under international law, as described in the previous chapter, is to give priority to whichever right will best serve the overall public interest in any particular case. Thus, wide latitude is given to reports on matters of public interest, for example involving politicians, even where this may otherwise represent an invasion of their privacy.

The advent of modern data protection regimes, which provide important protection for privacy, has introduced some confusion into the classical balancing test just noted. It is important, in this regard, to stress that data protection is not the same thing as privacy. Data protection rules are designed to address possible abuses associated with the automated processing of data sets. While there is significant overlap with privacy, they are not the same. Data protection rules are broader inasmuch as they apply to all personally identifying information, while privacy applies only to information in which there is a reasonable expectation of privacy. And data protection rules are narrower inasmuch as they only apply to data sets, normally those subject to automated processing. Thus, they would not apply to information held by a media outlet pursuant to its investigation of possible corruption on the part of an official.

The distinction is important because, while most data protection regimes include a number of specific rules to protect various public interests, they do not provide for a general public interest override for their rules. As a result, their application may not always ensure full respect for freedom of expression.[329]

5.1 Legal and regulatory measures

5.1.1 Constitutional measures

- Strong constitutional protection should be provided for both privacy and freedom of expression. This should encompass positive protections for these rights and, ideally, impose a positive obligation on the State to provide protection against private interferences with these rights.

---

329 A good analysis of this in the context of access to information is provided in Mendel, T. (2012) *Facilitating Access to Information for Research Purposes – A Comparative Survey.* Belgrade, UNDP. Available at: http://www.poverenik.org.rs/en/publications-/studies/1384-facilitating-access-to-information-for-research-purposes-a-comparative-survey.html.

- The constitution should allow only limited restrictions on both privacy and freedom of expression. This regime should be designed to accommodate conflicts between these two rights, through a process of assessing the overall public interest. Absent of strong countervailing considerations, this should be interpreted so as to allow public debate about matters of public concern, even where this involves the disclosure of private information.

The constitution sits at the pinnacle of the legal system and most constitutions include bills or charters of rights, guaranteeing the principle human rights. It is perhaps surprising that many of the countries reviewed above do not include direct protection for privacy in their constitutions, although in many cases courts have interpreted this into their decisions.

Despite this, it is clearly better practice to provide for protection for privacy in the constitution. That said, it is often complex to amend constitutions, as it should be, and this should only be done after widespread public consultation, so as to ensure that the constitution reflects the dominant will, and attracts the widespread support, of the people.

Understandings of privacy have long been shaped by available technologies. While at the most obvious level privacy involves restricting invasions of physical space and the protection of home and personal possessions, concerns about controlling what information is known about a person are inevitably part of adjusting to the impact of communication technologies.

Some constitutions describe, often on a non-exclusive basis, the content of the right to privacy. For example, the Constitution of South Africa indicates that it includes the right not to have one's home or property searched, possessions seized or communications intercepted.[330] Similarly, the Constitution of Nigeria refers to privacy of the home, correspondence and other forms of communication.[331] While these lists have the merit of clarity, they also present a risk that items which are not included – for example the reasonable expectation of seclusion is not included in the examples above – may not be included. If specific reference is made to communications, it should be clear that this covers all types of communications, including the range of types of communications made over the Internet (emails, postings to social networking sites or online groups, purchases, searches, websites visited, etc.).

It may be preferable simply to refer in the constitution to respect for privacy writ large, as is the case with the main international instruments. As an alternative, the constitution might refer to the main general characteristics of privacy, for example as including both subjective and objective elements, or referring to the idea of personal autonomy which is at its root. These characteristics could be spelled out directly in the constitution or left to the courts to elaborate.

Under international law, and in the constitutional law of many countries, protection for human rights is against the potential abuse of power by the State, rather than private actors. At the same time, international law and many constitutions recognise that this may include positive obligations on the State to protect individuals against harm to rights caused by private actors, which is sometimes referred to as the horizontal application of

330 Section 14.
331 Section 37.

rights. Given that threats emanate both from State and private actors, this is an important component of the overall protection for privacy.

Privacy is not an absolute right, as this report makes clear. It may be limited, among other things, because it may be overridden by law enforcement needs or the rights of others (among other things to seek, receive and impart information and ideas, i.e. to freedom of expression). This should be reflected in constitutional guarantees. To ensure that the core of the right remains protected, the constitution should place clear limits on the scope of any restrictions on privacy.

The ICCPR is rather unhelpful here, as it simply protects against "arbitrary or unlawful interference with privacy", which provides almost no guidance as to what is and is not permitted, and the ACHR uses similar language. The ECHR is more detailed, imposing three conditions on restrictions, namely that they be provided for by law, that they protect one of the interests listed, and that they be necessary in a democratic society to protect that interest. This is very similar to the test under both the ICCPR and the ECHR for restrictions on freedom of expression, which has proven to be fairly robust as a basis for protecting these rights.

The Mexican Constitution, in contrast, focuses in some detail on procedural protections for privacy, stipulating clear conditions for search orders and searches, and for interception of communications.[332] The South African Constitution is modelled more along the lines of the ECHR, requiring restrictions to be provided for in a law of general application, and to be "reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom", taking into account various factors.[333]

It is also important that the constitution provide protection for freedom of expression. Under international law, the regime of exceptions for this right is very similar to that which applies under the ECHR for privacy. Specifically, this involves a three-part test that permits only restrictions which are provided for by law, which protect one of the listed interests and which are necessary to protect that interest.

Regardless of how the specific regime of exceptions is cast, it is important that constitutional protection for both privacy and freedom of expression be designed so as to accommodate each other. As noted in the previous chapter, this essentially means that in a case of conflict between these two rights, the overall public interest should dominate.

5.1.2 Civil law protection

- The civil law should provide a private remedy against invasions of privacy, defined appropriately (either explicitly or through court interpretation) to cover information regarding which the individual has a reasonable expectation of privacy.
- To accord with the constitutional standards recommended above, this rule should allow for a public interest balancing when issues of freedom of expression are involved.
- This remedy should offer those whose privacy has been breached an appropriate remedy, capable of taking into account freedom of expression interests where relevant.

---

332 Article 16.

333 Section 36(1). See also section 45 of the Nigerian Constitution, which is similar in nature.

The primary practical means of protecting privacy in most countries is through a civil action brought by those who claim their privacy has been breached. The main rationale for this is that invasions of privacy, like attacks on reputation, are essentially a private matter between the parties involved, which should therefore be resolved through the civil law. Furthermore, this is the most practical way of ensuring protection for this right.

In many countries, the law recognises a specific legal cause of action for invasions of privacy. In other countries, such a cause of action has been found to be part of broader remedies. Thus, in common law countries, which follow the legal system of the United Kingdom of Great Britain and Northern Ireland, the action for breach of confidence has been used to provide a remedy for invasions of privacy, while in many civil law countries, which base their legal system on detailed legal codes, the Roman law concept of *actio iniuiarum* has been used to similar effect.

Providing for a civil action for breaches of privacy obviously constitutes better practice, and is a legal obligation under international law (and in many constitutions).[334] For reasons of clarity, it is probably preferable to provide for explicit protection for this right, although international tribunals have recognised that the action for breach of confidence may provide adequate protection for privacy.[335]

Many privacy laws do not actually define privacy, and the problems with a precise definition have been noted. At the same time, it is important to signal that privacy is not the same as personally identifying (which is the standard used in data protection rules). Instead, the notion of a reasonable expectation of privacy is one which is found in a number of jurisdictions – including France,[336] Canada[337] and Australia[338] – and this idea has also been referred to by the European Court of Human Rights.[339] It would seem to provide a solid general limitation on the scope of the concept (for if one does not have such a reasonable expectation, then surely the material cannot be defended as private). Many of the specific limitations on the scope of privacy found in different laws – for example where the person has consented to the disclosure, the information is already public or the information is about the public functions of an official – can be seen as specific elaborations of the general idea of a reasonable expectation of privacy.

In the United States of America, the tort of invasion of privacy has long provided essentially commercial protection for appropriation of one's name or likeness. But privacy as a personal autonomy issue and commercial interests arising from control over private information have been distinguished in other countries. The issue arose in the United Kingdom of Great Britain and Northern Ireland in the case of *Douglas v. Hello! Ltd*, which involved the unauthorised publication of photos of Michael Douglas's wedding to

---

334 See, for example, General Comment 16 of the UN Human Rights Committee, The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), 8 April 1988.

335 See *Earl Spencer and Countess Spencer v. the United Kingdom*, 16 January 1998, Application Nos. 28851/95 and 28852/95 (European Commission of Human Rights). Since that time, courts in the United Kingdom have essentially fashioned a direct cause of action for invasion of privacy from the law of breach of confidence. See *Campbell v MGN Ltd* [2004] 2 AC 457, para. 51.

336 *Schneider v. Sté Union Editions Modernes*, 5 June 1979, Paris Court of Appeal.

337 *Aubry v. Éditions Vice-Versa Inc*. [1998] 1 SCR 591, para. 57 et seq.

338 *Australian Broadcasting Corporation v. Lenah Game Meats Pty Ltd* [2001] HCA 63 (15 November 2001), para. 42.

339 *Von Hannover v. Germany*, 24 June 2004, Application No. 59320/00, para. 51.

Catherine Zeta-Jones by *Hello!* magazine, when they had sold exclusive rights for this to another magazine, namely *OK!*. The UK Court of Appeal held that even though they had consented to the publication of pictures of their wedding, the individual plaintiffs retained a (minor) privacy right, largely because they had a right of veto over the publication of pictures by *OK!*, which they could not assert against *Hello!*.[340] The Court also held separately that they held a protected commercial interest. There are stark differences between these two types of interests – namely privacy and commercial value – among other things because only one, privacy, is protected under international human rights law. These differences would appear to warrant different treatment of these interests in law.

An important issue is the scope of remedies for invasions of privacy, especially where this involves issues of freedom of expression, as is not infrequently the case. Financial awards are the most common remedy for breach of privacy. Under French law, other remedies are available, including seizure of the offending material and such other remedies as may be appropriate to cease the privacy invasion. In the *Douglas v. Hello!* Ltd case, the UK Court of Appeal refused to grant an injunction against publication of the photos, among other things because *OK!* could obtain commercial relief from *Hello!* at trial, and the individual plaintiffs retained only a limited privacy interest (having sold off most of their privacy rights).[341] In Argentina, the courts may award damages, order cessation of the infringing activity and, where appropriate, order publication of the judgment.

Under international law, even where it is appropriate to restrict rights, the imposition of excessive penalties may, of itself, constitute a breach the right.[342] As a result, even where a privacy interest trumps the right to freedom of expression, the scope of the remedy must take this into account (i.e. the remedy must also be proportionate).

5.1.3 Criminal law protection

- States should put in place sector-based criminal rules on privacy, to protect certain highly sensitive information, such as privacy of telecommunications and banking.
- While these protections should not be absolute, for example where surveillance of telecommunications is necessary for law enforcement purposes, there should be both strong procedural (i.e. normally requiring a court order) and substantive (e.g. proof that the measures are necessary to investigate a serious crime) barriers to removing them.
- A general criminal prohibition on invasions of privacy, which is likely to come into conflict with the right to freedom of expression, should be avoided.

Some countries – such as China, Argentina and the United States of America – have limited criminal protection for privacy, essentially prohibiting the dissemination of certain

---

340 *Douglas & Ors v Hello Ltd. & Ors* [2005] EWCA Civ 595 (18 May 2005), para. 109. In an earlier case before the Court of Appeal on whether or not to issue an injunction against publication by *Hello!*, Justice Sedley stated: "If all that had happened were that Hello! had got hold of OK's photographs, OK would have proprietary rights and remedies at law, but Mr Douglas and Ms Zeta-Jones would not, I think, have any claim for breach of the privacy with which they had already parted." *Douglas & Anor v Northern And Shell Plc & Anor* [2000] EWCA Civ 353 (21 December 2000), para. 140.

341 *Douglas & Anor v Northern And Shell Plc & Anor* [2000] EWCA Civ 353 (21 December 2000), para. 144.

342 See, for example, *Tolstoy Miloslavsky v. United Kingdom*, 13 July 1995, Application No. 18139/91 (European Court of Human Rights).

types of sector-based information (for example in relation to telecommunications or banking). In addition to these obvious candidates, some countries have put in place criminal schemes to address particular problems.[343] In some cases, these criminal rules only apply to information held by officials, while in other cases they apply to the private sector as well.

In a few countries – notably in France – there are more general criminal proscriptions on privacy invasions. In the case of France, several of these criminal rules were specifically designed to address paparazzi-type behaviour and even media use of paparazzi content. Thus, pursuant to Article 226-1 of the Penal Code it is a crime wilfully to violate the private life of another person without their consent by, among other things "taking, recording or transmitting the picture of a person in a private place".

The sector-based approach has much to recommend it, inasmuch as strong protection is needed for certain categories of private material due to the risk of (other) crimes or civil wrongs being committed if it is not protected. Banking information is perhaps the most obvious example of this. However, as the experience of many countries demonstrates, there is no need to establish a general criminal offence of invasion of privacy, and this is particularly problematical where such rules are applied to limit freedom of expression.

Under international law, and the law of many countries, these protections can only be removed where there is a very compelling public interest for doing so. A classic example of this is for law enforcement purposes (i.e. where police are authorised to monitor telecommunications as part of an investigation into a crime). There should be both procedural and substantive barriers to removing these protections. Procedurally, this should normally require a court order, and substantively it should require a demonstration of a clear and overriding public interest, such as the investigation of a serious crime.

5.1.4 Data protection systems

- States should put in place strong data protection regimes which include the key features noted below, namely broad applicability, the right of consent, the right to access and correct, obligations on data controllers and the right of redress.
- There should be exceptions to these rules for certain types of data collection, in particular where this is for purposes of freedom of expression.
- Otherwise, however, conflicts between freedom of expression, including the right to information, and data protection rules should be resolved in accordance with the constitutional regime for resolving conflicts between freedom of expression and privacy, namely through decisions which favour the overall public interest. Remedies should also be proportionate.

It is now widely agreed that data protection regimes are an essential component of the wider protection of privacy, and some elements of these regimes are mandated by international human rights law. As a result, democracies are increasingly putting in place

343 A good example of this is the United States Driver's Privacy Protection Act 1994, 18 USC Chapter 123, which was adopted in response to the growth in sale of sensitive personal information contained in motor vehicle records.

such regimes. The main characteristics of such regimes are described in Box XVI.[344] Key features of a strong regime include:

(1) **Broad applicability –** these rules should apply to personal data sets and data controllers in both the public and private sectors.

(2) **The right of choice/consent –** Individuals should normally be given the choice of whether their information is collected. There should only be limited exceptions to this where there is an overriding interest, defined in law, in the collection of such information. This implies that individuals understand and are given clear notice of a public or private body's information practices before any personal information is collected. This notification should describe what information is proposed to be collected and held, who will collect it, how the information will be used, and who will have access to it. It should also be clear to the subject whether the provision of the requested information is voluntary or required by law and the consequences of a refusal to provide the requested information. Information should not be used for purposes which are incompatible with the use for which the information was originally collected.

(3) **The right to access and correct –** Individuals should have the right of access to any information held about them at reasonable intervals and without undue delay. They should also have the right to require the data controller to correct any inaccuracies or to delete the data, where appropriate.

(4) **The responsibilities of information holders –** Data controllers must take reasonable steps to ensure the information they hold is accurate and secure. Access to the data should be limited in accordance with the established uses of the data. Transfers should only be made to third parties which can ensure similar respect for data protection principles. Data should be destroyed once it is no longer needed for the established uses, or converted to anonymous form. While held, appropriate steps should be taken to ensure the confidentiality, integrity and quality of the data.

(5) **The right of redress –** Individuals should have the right of redress against both public and private bodies which fail to respect data protection rules in relation to data about them. Remedies can be provided through self-regulation, private law actions and government enforcement. Oversight of the system should be undertaken by an independent body.

Better practice data protection regimes include exceptions for data processing relating to the exercise of freedom of expression (albeit sometimes described unduly narrowly as for journalistic or artistic purposes to the exclusion of other means of expression, such as publishing a book). This is important amongst other things because of the very broad definitions of personal data used in these regimes (personally identifying data) and the lack of accommodating principles governing use (i.e. systems to give effect to the public interest override).

Even where data protection rules do apply, conflicts between privacy and freedom of expression should be resolved in accordance with the general constitutional rules for

344 Although formally that Box describes the European Union data protection regime, it broadly represents better practice in this area.

addressing such conflicts. In other words, an assessment of the overall public interest should be undertaken.

A potentially more complicated issue is the relationship between data protection and access to information regimes. Here again, however, better practice is to rely on general protections for and definitions of privacy, rather than the specialised rules in the data protection regime, which were not designed to provide an appropriate general balancing between access and secrecy in the area of privacy. Given that the right to information is part of the right to freedom of expression under international law, this approach is consistent with the previous point (i.e. about balancing freedom of expression and privacy). It is also consistent with fundamental principles of the right to information, including that information should be made public where this is in the overall public interest, even if this would cause harm to a protected interest, such as privacy.

5.2 Corporate policy and practice

- Corporations should develop strong privacy policies to protect users. These should, as a general principle, allocate as much control over privacy as possible to users and include rules about changing the policy that provide protection to users against increased exposure to privacy intrusions. More detail on the possible approach for these policies is provided below.
- More attention needs to be given to developing self- and possibly co-regulatory initiatives, as well as cooperative options, for protecting the privacy of users. Corporations should allocate more time and resources to this important issue, in consultation with other stakeholders.
- Corporations should make a general commitment to take the issues of privacy and freedom of expression seriously. What this means in practice will depend on the specific activities of each corporation, but it should at least mean that the corporation devotes some time and energy to thinking about ways it can adapt its operations so as to enhance respect for these fundamental rights. In most cases, this should involve a transparent policy development process.

As noted elsewhere in this report, self-regulatory initiatives by corporations present a challenge in relation to privacy because for most ISPs and OSPs the business incentives all line up against privacy, apart from public opinion which only really applies with significant force to a small number of companies. As a result of this, many commentators have been critical of self-regulatory efforts.[345]

At the same time, good business practices are essential to successful protection of privacy online. Perhaps the most important aspect of this relates to consent, which, once given, effectively waives the most important data protection rules. It is often through mechanisms of consent that users accept the privacy policies and (often less formal) approaches toward privacy of ISPs and OSPs. As noted, there are various challenges to getting these systems to work, including the (probably necessary) complexity of the policies/approaches, the large number of different services which people use and the low level of engagement by users around this issue. There is also the issue of companies

345 Some of these are noted above. See footnote 298 and related text.

changing their privacy policies. All of this effectively transfers a lot of control, and so also responsibility, to companies.

A number of better practices can be identified for privacy policies. First, corporations should commit to developing clear privacy polices, based generally on the standards of respect for privacy that are outlined in this report. Many ISPs and OSPs still do not have such policies in place. These policies should be user-friendly, for example by being easily accessible on the website and by being written, as far as possible, in clear, plain language(s).

Second, wherever possible – including where this is consistent with the service provided and the core business model of the company – control over privacy should be put in the hands of users. For example, Facebook allows users to set some privacy choices, at least in relation to what other users can see, while the Google Privacy Policy provides for various opt-ins and opt-outs.[346] Inasmuch as opt-ins require a greater degree of attention on the part of the user, they are preferable from a privacy perspective.

Third, companies should make certain commitments to users regarding changes to their privacy policies. Google promises not to reduce users' privacy without their explicit consent. Facebook promises to allow users a 7-day comment period for most changes and, if more than 7,000 people provide comments, not necessarily an impossibly high barrier given the very large total number of users, they will put the matter to a vote. The vote will be binding, one way or the other, if 30% of all registered users participate.[347] This is a pretty high barrier (NB the low rates of participation even in national elections in most countries), but perhaps not impossibly high for a very controversial change.

In some ways, the debate about corporate policies in this area is just beginning. Much more work needs to be done to develop ideas, test them and try to agree on some best practice approaches. To address some of the shortcomings of self-regulatory or company motivated programmes, some commentators have called for co-regulatory initiatives, involving companies, civil society organisations and governments. More work needs to be done to ascertain whether and what ideas might be feasible and whether they pose greater risks than benefits to the very interests that they seek to promote, namely respect for privacy and freedom of expression.

The idea of cooperative arrangements could also be fertile ground. Cooperation differs from co-regulation inasmuch as it is voluntary in nature, although it is similar inasmuch as it involves both the public and private sectors. A potentially promising idea here is that of formal certification of service providers. This would involve agreement on a set of core standards and then certification of companies that meet those standards. Various options could be explored regarding oversight of the system, which could either be done by an independent public body, such as the telecommunications regulators in many countries, or a sector body, and various cooperative arrangements might be devised for enforcement of the rules.

Although more work needs to be done on these issues, at the same time some companies are seeking to develop better policy options for protecting privacy online. One example

346 The policy is available at: http://www.google.com/policies/privacy/.
347 Their policy is available at: http://www.facebook.com/about/privacy/.

is Mozilla, who provide the Firefox browser.[348] Based on the Mozilla approach, a possible set of principles to underpin a corporate policy on privacy could be as follows:

(1) **No Surprises.** Companies and services should only use, collect and share information about users as disclosed in clear, concise, easy to understand, notices.

(2) **Real Choices.** Companies and services should give users actionable and informed choices by providing clear information at the point of collection and providing a choice to opt-out whenever possible.

(3) **Sensible Settings.** Companies and services should establish default settings in products and services that balance privacy, security and user experience.

(4) Limited Data. Companies and services should collect and retain the least amount of information necessary for the feature or task and meet users' reasonable expectations of privacy. Anonymous, aggregate data should be used whenever possible, and personal information collected should only be kept for as long as necessary to serve the purpose it was collected for.

(5) **User Control.** Companies and services should not track or disclose personal user information without the user's consent. They should employ privacy enhancements that put people in control over their information and enable them to understand how their information is being used and stop collection and tracking of their personal information if they choose.

(6) **User Access.** Users should have the right to know when their data is being collected or processed and to access that data in an understandable form. This information should be provided to users without charge and they should have the power to delete or correct errors in information.

(7) **Trusted Third Parties.** Companies and services should make privacy a key factor in selecting and interacting with partners. In addition, all third party companies, services, and applications should uphold these privacy principles.

(8) **Security.** Companies and services should take appropriate measures to protect data against both natural and human risks, including unauthorized access, misuse or error. If a website or service's security is breached, users have a right to know immediately.

(9) **Transparency of Government Sharing.** Companies and services should notify users about government requests for information associated with users' accounts when permitted to do so by law, giving users the opportunity to contest that demand for their data if they choose to.

(10) **Providing Remedies:** Where a company identifies that they have caused or contributed to adverse impacts on users' privacy, they should make provision for, or cooperate in, handling complaints and providing a remedy to those users through a transparent process.

(11) **Privacy Across the Board.** Privacy protections should apply equally across all online and mobile platforms and to all companies, services and third-party applications. Companies should also make sure partners uphold strong privacy principles.

---

348 http://www.mozilla.org/about/policies/privacy-policy.html.

Potential conflicts with freedom of expression raise difficult issues for ISPs and OSPs. Companies that operate in the many countries where the legal framework does not give strong protection to freedom of expression are often faced with hard choices, as the example of Yahoo! in China, cited above, demonstrates. Rather than face these choices, Google effectively pulled out of mainland China in March 2010.[349]

In many other countries, a number of options exist for companies, ranging from 'harder' approaches such as using the legal framework to insist on their rights vis-à-vis governments which are seeking to limit privacy and/or freedom of expression, to using their leverage (especially for the larger international companies) to employ softer, but often quite effective, approaches such as putting in place systems to promote awareness about rights among staff and members of governance structures, sharing information about problems and solutions, studying risks and designing solutions and responses and reviewing progress. Many of these are detailed in the Global Network Initiative's (GNI) Implementation Guidelines.[350] A lot of this is dependent on political will, which unfortunately appears to be rather low among ISPs and OSPs, as reflected in the fact that the GNI still only has five corporate members.

5.3 Awareness raising

- States should undertake awareness-raising efforts about privacy and new technologies, both aimed at younger people through the school system and using other systems to reach adults.
- Other actors in a position to raise awareness – such as corporations, parents and civil society groups – should also play a role in fostering a better understanding amongst the general public about privacy and new technologies.
- There is an important role for the media in raising awareness about the importance of privacy and how different challenges present themselves as the Internet develops. Recent events in the United Kingdom of Great Britain and Northern Ireland, where mobile phone of crime victims were hacked leading to the closure of the UK's best-selling newspaper, shows the reputational damage that can be caused by a lack of awareness of how privacy online needs to be respected. Journalists need to be aware, and to raise awareness, about the implications for the media of new technologies and how they can violate privacy. At the same time, the media should also be alert about how controls in the name of privacy may lack sufficient safeguards to protect freedom of expression.

No set of policy recommendations about privacy and freedom of expression on the Internet could be complete without a reference to the general public, i.e. the main users of the Internet. Much can be done directly by users to protect their own privacy and freedom of expression online. Even somewhat sophisticated devices, such as encryption tools, are now quite user friendly while at a much more basic level, awareness of simple aspects of the nature of new technologies can help users avoid some privacy pitfalls. For example, being aware that some employers use the Internet to find out about the background of

349 See the announcement of this by Google at: http://googleblog.blogspot.ca/2010/03/new-approach-to-china-update.html.

350 Available at: http://globalnetworkinitiative.org/implementationguidelines/index.php.

potential employees may lead to greater prudence in the setting of Facebook privacy controls.

Media and Internet literacy should be included as a basic life-skill in the education system, starting from quite an early age, as part of broader civic education or human development courses. States should also direct outreach efforts about privacy and new technologies at adults, for example through developing awareness raising resources and making them accessible online and in other places where adults can access them.

Many other social actors can also play a role here. ISPs and OSPs should make an effort to highlight the potential risks of privacy 'carelessness' to users, recognising that it may be difficult to get companies to warn potential customers of the risks of using their own services. The media should address this issue as part of its general mandate to inform people about matters of public concern. Many civil society organisations work on issues for which privacy on the Internet is important or relevant, and they should also incorporate awareness raising initiatives into their work. Parents should also be encouraged to play a role here, protecting their children through making them aware of online privacy risks. This is a huge task, but with the concerted involvement of all of these actors, much can be achieved.

6. USEFUL RESOURCES

This document compiles information collected on Internet privacy and freedom of expression. The information was organized to cover the following five regions: Africa; Asia and the Pacific; Latin America and the Caribbean; Arab States; and Europe and North America. In addition, a section with a specific focus on gender was included at the end. The documents, reports, books and papers gathered were found through academic libraries as well as top non-governmental organizations and academic centres working on these issues. In the general and regional sections, a number of documents were prioritized and placed at the top of the respective list. The research was finished on July 6th. Until then, all links were active.

6.1 General

Banisar, D. and Davies, D. (1999), "Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments", available at http://www.jcil.org/journal/articles/117.html

Faris, R., Wang, S. and Palfrey, J. (2008), «Censorship 2.0" Innovations: Technology|Go vernance|Globalization, available at http://www.mitpressjournals.org/doi/abs/10.1162/itgg.2008.3.2.165

Lanois, P. (2011), "Privacy in the age of the cloud", *Journal of Internet Law*, ISSN 1094-2904, 12/2011, Volume 15, Issue 6, p. 3.

Bambauer, D., Palfrey, J., and Zittrain, J. (2004), «A Starting Point: Legal Implications of Internet Filtering», Open Net Initiative, available at http://opennet.net/docs/Legal_Implications.pdf

Boyd, D. (2010). «Living Life in Public: Why American Teens Choose Publicity Over Privacy.» Association of Internet Researchers. Gothenburg, Sweden, available at http://www.danah.org/papers/talks/2010/AOIR2010.html

Boyd, D. (2010). «Making Sense of Privacy and Publicity.» SXSW. Austin, TX., available at http://www.danah.org/papers/talks/2010/SXSW2010.html

Boyd, D. (2010). «Privacy and Publicity in the Context of Big Data.» Raleigh, NC, available at http://www.google.com.ar/url?sa=t&rct=j&q=%22privacy%20and%20publicity%20in%20the%20context%20of%20big%20data&source=web&cd=1&ved=0CGAQFjAA&url=http%3A%2F%2Fwww.danah.org%2Fpapers%2Ftalks%2F2010%2FWWW2010.html&ei=cTD3T_fSE4OE8ASPw8TuBg&usg=AFQjCNHvgZNDYr_f3a28tOWhUlHFyHdq4A

Boyd, D. (2010). "Privacy, Publicity, and Visibility." Microsoft Research TechFest. Redmond, WA.

Boyd, D. (2010). «The Future of Privacy: How Privacy Norms Can Inform Regulation.» International Conference of Data Protection and Privacy Commissioners. Jerusalem, Israel, available at http://www.danah.org/papers/talks/2010/PrivacyGenerations.html

Boyd, D. (2011). «Networked Privacy.» Personal Democracy Forum. New York, NY, June 6, available at http://www.danah.org/papers/talks/2011/PDF2011.html

Boyd, D. and Marwick, A. (2011). «Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies.» Paper presented at the Oxford Internet Institute Decade in Internet Time Symposium, September 22, available at http://www.danah.org/papers/2011/SocialPrivacyPLSC-Draft.pdf

Boyd, D. and Marwick, A. (2011). «Social Steganography: Privacy in Networked Publics.» International Communication Association. Boston, MA, available at http://www.danah.org/papers/2011/Steganography-ICAVersion.pdf

Brunton, F., and Nissenbaum, H. (2011), "Vernacular resistance to data collection and analysis: A political theory of obfuscation", First Monday, Volume 16, Number 5, available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3493/2955

Deibert, R. (2000), «International Plug n' Play? Citizen Activism, the Internet, and Global Public Policy,» International Studies Perspectives, Vol. 1, No. 3, pp. 255-272.

Deibert, R. (2003), «Black Code: Censorship, Surveillance, and Militarization of Cyberspace,» Millennium: Journal of International Studies, Vol. 32, No. 3.

Deibert, R. (2004), «Firewalls and Power: An Overview of Global State Censorship of the Internet,» with Nart Villeneuve in Klang, M. & Murray, A., (eds) Human Rights in the Digital Age, Cavendish Publishing London.

EFF (2011), "Freedom of Expression, Privacy and Anonymity on the Internet. Comments submitted to the United Nations Special Rapporteur on the promotion and protection of the right to Freedom of Opinion and Expression", available at https://www.eff.org/sites/default/files/filenode/UNSpecialRapporteurFOE2011-final_3_0.pdf

Faris, R. and Zittrain, J. (2009), "Web tactics" Index on Censorship, 38; 90, available at http://ioc.sagepub.com/content/38/4/90.full.pdf+html

Franda, M. (2002), Internet and the Cyberspace, Internet Development and Politics in Five World Regions, Lynne Rienner Publishers, inc. United States of America and United Kingdom, available at http://books.google.com.ar/books?hl=es&lr=&id=k89jJKN1wXcC&oi=fnd&pg=PR11&dq=privacy+and+internet+arab+region&ots=aYTBncvUIw&sig=4vOeAgHxO5UWDquGdba1EE18Kks#v=onepage&q=privacy%20and%20internet%20arab%20region&f=false

Global Network Initiative (2010), Inaugural Report 2010. Our work. Our vision. Our progress., available at: http://www.globalnetworkinitiative.org/files/GNI_Annual_Report_2010.pdf

Hartzog, W. (2009), "The privacy box: A software proposal", First Monday, Volume 14, Number 11 – 2, available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2682/2361

Internet Governance Forum (2010), Developing the Future Together, Edited by Brian Gutterman, The Fifth Meeting of the Internet Governance Forum, Vilnius, Lithuania, available at http://www.intgovforum.org/cms/2011/book/IGF_2010_Book.pdf

Leon, P., Ur, B., Balebako, R., Cranor, L., Shay, R. and Wa, Y (2011), "Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising", available at http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html

Madrid Privacy Declaration (2011), available at http://thepublicvoice.org/madrid-declaration/

Marwick, A., Murgia Diaz, D., and Palfrey, J. (2010), "Youth, Privacy and Reputation", available at http://cyber.law.harvard.edu/publications/2010/Youth_Privacy_Reputation_Lit_Review

Palfrey, J. (2008), "The Public and the Private at the United States Border with Cyberspace", available at http://cyber.law.harvard.edu/publications/2008/Public_and_Private_at_US_Border_with_Cyberspace

Palfrey, J. and Rogoyski, R. (2006), «The Move to the Middle: The Enduring Threat of 'Harmful' Speech to Network Neutrality,» *Washington University Journal of Law and Policy.*

Privacy International (2012), An assessment of the EU-US travel surveillance agreement, available at https://www.privacyinternational.org/reports/an-assessment-of-the-eu-us-travel-surveillance-agreement

Raynes-Goldie, K. (2010), "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook", First Monday, Volume 15, Number 1 – 4, available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432

Rodriguez, K (2012), "Biometric National IDs and Passports: A False Sense of Security", available at https://www.eff.org/deeplinks/2012/06/biometrics-national-id-passports-false-sense-security

UN General Assembly (2012), "The promotion, protection and enjoyment of human rights on the Internet", available at http://www.regeringen.se/content/1/c6/19/64/51/6999c512.pdf

Van den Berg, B. and Van der Hof, S. (2012), "What happens to my data? A novel approach to informing users of data processing practices", First Monday, Volume 17, Number 7, available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/4010/3274 .

Van Schewick, B. (2012), "Network Neutrality and Quality of Service: What a Non-Discrimination Rule Should Look Like", available at http://cyberlaw.stanford.edu/publications

Villeneuve, N. (2006), «The filtering matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace» First Monday, Volume 11, available at http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1307/1227

Volokh, E. (1999), “Freedom of Speech, Information Privacy, and the Troubling Implications of a Right to Stop People from Speaking About You”, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=200469

Zittrain, J. (2003) «Internet Points of Control», Boston College Law Review, available at http://cyber.law.harvard.edu/publications/2003/Internet_Points_of_Control

Zittrain, J. (2003), «Be Careful What You Ask For: Reconciling a Global Internet and Local Law» (PDF), Who Rules the Net? The Cato Institute, available at http://cyber.law.harvard.edu/node/367

Zittrain, J. (2006), «The Generative Internet», Harvard Law Review, Vol. 119, p. 1974, May 2006, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=847124

6.2 Africa

Thabang Masete, N, (2012), “The Challenges in Safeguarding Financial Privacy in South Africa”, J*ournal of International Commercial Law and Technology*, ISSN 1901-8401, 07/2012, Volume 7, Issue 3, pp. 248 – 259

Olinger, H., Britz, J. and Olivier, M. (2007), “Western privacy and/or Ubuntu? Some critical comments on the influences in the forthcoming data privacy bill in South Africa”, *International Information and Library Review*, ISSN 1057-2317, 2007, Volume 39, Issue 1, pp. 31 – 43

Mivule, K. and Turner, C. (2011), “Applying Data Privacy Techniques on Tabular Data in Uganda”, available at http://arxiv.org/abs/1107.3784

Open Net Initiative (2009), “Internet Filtering in Sub-Saharan Africa”, available at http://opennet.net/sites/opennet.net/files/ONI_SSAfrica_2009.pdf

Ncube, C. (2004), “A Comparative Analysis of Zimbabwean and South African Data Protection Systems”, Journal of Information, Law and Technology, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_2/ncube/caroline.doc

Banisar, D. (2009), “ICT policies relating to privacy, freedom of expression and access to information : a briefing paper”, Makerere University, Human Rights and Peace Centre”, available at http://idl-bnc.idrc.ca/dspace/handle/10625/34234

Boniface Makulilo, A. (2012), Privacy and data protection in Africa: a state of the art, Oxford University Press. Available at http://idpl.oxfordjournals.org/content/early/2012/06/11/idpl.ips014.full

Cohen, T. (2000), “But for the nicety of knocking and requesting a right of entry’: surveillance law and privacy rights in South Africa”, available at http://idl-bnc.idrc.ca/dspace/handle/10625/42079

Faris, R., Roberts, H., Heacock, R., Zuckerman, E. and Gasser, E. (200x), “Online Security in the Middle East and North Africa. A Survey of Perceptions, Knowledge, and Practice”, Harvard Cyber Law, available at http://cyber.law.harvard.edu/node/6973

IDRC, “Protecting youth’s privacy in Latin America”, available at http://www.idrc.ca/EN/Programs/Science_and_Innovation/Information_and_Networks/Pages/ResultDetails.Aspx?ResultID=60

Kofi-Armah, D., (2012), Internet Security and Data Protection in Ghana, Africa: A Hacker’s Perspective, available at: http://www.connectedafrica.com/internet-security-and-data-protection-in-ghana-africa-a-hackers-perspective-interview-with-sepo/

MacKinon, R., Risen, T., Hussain, H., Li, W., Losey, J. and Myers, S. (2012), Netizen Report: Intervention Edition, Global Voices Online, Posted 14 June 2012, available at: http://advocacy.globalvoicesonline.org/2012/06/14/netizenreport-intervention/

Makulilo, A. (2012), “Privacy and data protection in Africa: a state of the art”, International Data Privacy Law, available at http://idpl.oxfordjournals.org/content/early/2012/06/11/idpl.ips014.abstract

Privacy International (2006), South Africa, available at: https://www.privacyinternational.org/reports/south-africa

6.3 Arab states

Aladwani, A.M. (2003), Key Internet characteristics and e-commerce issues in Arab countries, information Technology & People, Vol. 16 Iss: 1, pp.9 – 20, available at: http://www.emeraldinsight.com/journals.htm?articleid=883574&show=abstract

Warf, B. and Vincent, P.(2007), Multiple geographies of the Arab Internet, Area Volume 39, Issue 1, pages 83–96, March 2007, available at: http://onlinelibrary.wiley.com/doi/10.1111/j.1475-4762.2007.00717.x/full

Al-Rasheed, A. (2001), “The Internet in Saudi Arabia”, available at http://www.isu.net.sa/library/CETEM2001-AlRasheed.pdf

Bureau of Democracy (2007), Human Rights, and Labor, Iraq, US Department of State

Burkhart, E. (1998), “National Security and the Internet in the Persian Gulf Region”, available at http://www.georgetown.edu/research/arabtech/pgi98-10.html

Messieh, N. (2011), “Discover Digital Arabia: Middle East Internet usage in numbers”, available at http://thenextweb.com/me/2011/08/25/discover-digital-arabia-middle-east-internet-usage-in-numbers/

Noman, H. (2009), “An Overview of The Demographics and Usage Patterns of Internet Users in Developing Countries: Yemeni Internet Population as a Case Study”, United Nations Development Programme, at http://opennet.net/sites/opennet.net/files/ONI_Yemen_2009.pdf

Open Net Initiative (2004), “Internet Filtering in Saudi Arabia”, available at http://opennet.net/studies/saudi

Open Net Initiative (2005), “Internet Filtering in Bahrain in 2004-2005”, available at http://opennet.net/studies/bahrain

Open Net Initiative (2005), "Internet Filtering in Iran in 2004-2005: A Country Study", available at http://opennet.net/studies/iran

Open Net Initiative (2005), "Internet Filtering in the United Arab Emirates in 2004-2005: A Country Study", available at http://opennet.net/studies/uae

Open Net Initiative (2005), "Internet Filtering in Yemen in 2004-2005: A Country Study", available at http://opennet.net/studies/yemen

OpenNet Initiative (2004), Internet Filtering in Saudi Arabia, available at http://www.opennetinitiative.net/studies/saudi/#toc4c

Privacy International (2006), United Arab Emirates, available at: https://www.privacyinternational.org/reports/united-arab-emirates

Privacy International (2006), Iraq, available at: https://www.privacyinternational.org/reports/united-arab-emirates

Rohozinski, R. (2004) «'Secret Agents' and 'Undercover Brothers': The Hidden Information Revolution in the Arab World», available at http://mediaresearchhub.ssrc.org/201csecret-agents201d-and-201cundercover-brothers201d-the-hidden-information-revolution-in-the-arab-world/attachment

Sait, S., Ali, S., Al-Tawil, K. and Sanaullah, S (2010), "Trends in Internet Usage & its Social Effects in Saudi Arabia", available at http://www.google.com.ar/url?sa=t&rct=j&q=saudi%20arabia%20privacy%20internet&source=web&cd=5&ved=0CGcQFjAE&url=http%3A%2F%2Ffaculty.kfupm.edu.sa%2Fcoe%2Fsadiq%2Frichfiles%2Frich%2Fdoc%2FSocialEffectsTrends.doc&ei=-CL3T_-yM4aQ8wSi0KSJBw&usg=AFQjCNGL6f6FgAK5e1hDNLiEaXff8QcwpA

Zittrain & Edelman, "Documentation of Internet Filtering in Saudi Arabia", available at http://cyber.law.harvard.edu/filtering/saudiarabia/sa-yahoo-3.html

6.4 Asia and the Pacific

Open Net Initiative (2009), «Internet Filtering in Asia», available at http://opennet.net/sites/opennet.net/files/ONI_Asia_2009.pdf

Chung, R. (2003), Hong Kong's "Smart" Identity Card: Data Privacy Issues and Implications for a Post-September 11th America, Asian-Pacific Law & Policy Journal; Vol. 4, Issue 2

Jho, W. (2005), "Challenges for e-governance: protests from civil society on the protection of privacy in e-government in Korea", available at http://ras.sagepub.com/content/71/1/151.abstract

Gomez, J. (2003), "Dumbing down democracy: Trends in internet regulation, surveillance and control in Asia", Pacific Journalism Review, available at http://gomezcentre.academia.edu/JamesGomez/Papers/116683/Dumbing_down_democracy_trends_in_internet_regulation_surveillance_and_control_in_Asia

Kitiyadisai, K., (2005), "Privacy Rights and Protection: Foreign Values in Modern Thai Context", Ethics and Information Technology", available at http://www.stc.arts.chula.ac.th/feeds/Krisana/7156321v361p0324.pdf

Chik, W. (2006), "The Lion, the Dragon and the Wardrobe Guarding the Doorway to Information and Communications Privacy on the Internet: A Comparative Case Study of Hong Kong and Singapore – Two Differing Asian Approaches", *International Journal of Law and Information Technology*, ISSN 0967-0769, 04/2006, Volume 14, Issue 1, p. 47

Greenleaf, G. (2012), "Promises and illusions of data protection in Indian law", available at http://idpl.oxfordjournals.org/content/1/1/47.full.pdf+html

ARTICLE 19 (2011), "South East Asia: the state of free expression", available at *http://www.article19.org/resources.php/resource/2258/en/south-east-asia:-the-state-of-free-expression*

Cheung, A., (2009), "China Internet going wild: Cyber-hunting versus privacy protection", available at http://www.sciencedirect.com/science/article/pii/S026736490900065X

Wu, Y., Lau, T., Atkin, D. and Lin, C., (2011), "A comparative study of online privacy regulations in the US and China", *Telecommunications Policy*, ISSN 0308-5961, 2011, Volume 35, Issue 7, pp. 603 – 616.

Viner, N., (2007), "The Global Online Freedom Act: Can US Internet Companies Scale the Great Chinese Firewall at the Gates of the Chinese Century?", *Iowa Law Review*; 11/1/2007, Vol. 93 Issue 1, p361-391.

Bamman, D., O'Connor, B. and Smith, N. (2011), "Censorship and deletion practices in Chinese social media, First Monday, Volume 17, Number 3, available at http://www.firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3943/3169

Deibert, R. (2001), «Dark Guests and Great Firewalls: Chinese Internet Security Policy,» *Journal of Social Issues*, 58, 1: 143-158.

Deibert, R. (2006), «The geopolitics Asian Cyberspace», Far Eastern Economic Review, available at http://www.feer.com/articles1/2006/0612/free/p022.html

Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (2011), "Access Contested: Security, Identity, and Resistance in Asian Cyberspace", Harvard Cyber Law, available at http://oni-access.net/contested/

Greenleaf , G (2011) 'Outsourcing and India's new privacy law: No cause for panic' Privacy Laws & Business International Report, Issue 111, 16-17, April 2011

Greenleaf, G (2011c) 'Breach notification and diffused enforcement in Taiwan's DP Act' Privacy Laws & Business International Report, Issue 109, 12-13, February, 2011

Greenleaf, G (2011a) 'India attempts data protection by regulations' Privacy Laws & Business International Report, Issue 110, April 2011

Open Net Initiative (2005), "Internet Filtering in Burma in 2005: A Country Study", available at http://opennet.net/studies/burma

Open Net Initiative (2005), “Internet Filtering in China in 2005: A Country Study”, available at http://opennet.net/studies/china

Open Net Initiative (2005), “Internet Filtering in Singapore in 2005: A Country Study”, available at http://opennet.net/studies/singapore

Open Net Initiative (2005), “Internet Filtering in Tunisia in 2005: A Country Study”, available at http://opennet.net/studies/tunisia

Open Net Initiative (2006), “Internet Filtering in Vietnam in 2005-2006: A Country Study”, available at http://opennet.net/studies/vietnam

Rohozinski, R. (1999), «Mapping Russian Cyberspace: Perspectives on Democracy and the Net» (PDF), UNRISD Discussion Paper No. 115.

Rohozinski, R. (2000), «How the Internet Did Not Transform Russia,» Current History, Volume 99, no 334.

6.5 Latin America and the Caribbean

Bertoni, E. (2012), “Towards an Internet Free of Censorship. Proposals for Latin America”, Universidad de Palermo, Facultad de Derecho, Centro de Estudios en Libertad de Expresión y Acceso a la Información, available at: http://www.palermo.edu/cele/english/publication.html

Remolina, N. (2010), “¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?”, International Law, Revista Colombiana de Derecho Internacional, 16(2010), p. 493.

Leonardi, M. (2005), “Responsabilidade Civil dos Provedores de Serviços de Internet”, Doctorate dissertation originally published by Juarez de Oliveira, 2005, São Paulo.

Albornoz, B., Barindelli, F., Caballero, J., Duaso, R., and Esquivel, W. (2011), “Derechos y justicia y el movimiento social en Internet” Instituto de Investigación para la Justicia, AR, available at http://hdl.handle.net/10625/46335.

Barindelli, F, and Gregorio, C. (2010), “Datos personales y libertad de expresión en las redes sociales digitales : memorándum de Montevideo”, Ad-Hoc, Buenos Aires, AR, available at http://hdl.handle.net/10625/46022

Bossio Montes de Oca, J, (2009) “Peru : the battle for control of the internet”, Association for Progressive Communications, Quito, EC, available at http://hdl.handle.net/10625/42792

Carvalho Lima, C.C. & Leite Monteiro, R. (2011) Comentários ao Anteprojeto de Lei sobre Proteção de Dados Pessoais (Comments on the new Brazilian data protection bill), Observatório da Internet.br – observatório brasileiro de políticas digitais (Internet Observatory – Brazilian observatory of digital policies), available at: http://securitybreaches.files.wordpress.com/2011/05/anteprojeto-de-lei-brasileiro-sobre-protecao-de-dados-pessoais.pdf

Gregorio, C. and Ornelas, L. (2011), "Protección de datos personales en las redes sociales digitales : en particular de niños y adolescentes; memorándum de Montevideo", Instituto de Investigación para la Justicia, Buenos Aires, available at http://hdl.handle.net/10625/46963

Gregorio, C.G. (2004), "Protección de Datos Personales: Europa Vs. Estados Unidos, Todo un Dilema para América Latina", available at http://www.bibliojuridica.org/libros/3/1407/12.pdf

Instituto de Investigación para la Justicia (2004), "Internet, privacidad y sistema judicial en América Latina y el Caribe", IIJ, Buenos Aires, AR, available at http://idl-bnc.idrc.ca/dspace/handle/10625/25922

Monteiro, R and Laurant, C. (2011), "New Brazilian data protection bill adopts data breach notification regime", available at http://blog.security-breaches.com/2011/05/09/new_brazilian_data_protection_bill_adopts_data_breach_notification_regime/

OAS (2010), "Preliminary principles and recommendations on data protection", available at http://thepublicvoice.org/documents/Study_on_Data_Protection-CP25337E04-Eng.pdf

Privacy International (2011), "Guía de privacidad para hispanohablantes", available at https://www.privacyinternational.org/reports/una-guia-de-privacidad-para-hispanohablantes

Rodriguez, K., (2011), "The Politics of Surveillance: The Erosion of Privacy in Latin America", available at http://advocacy.globalvoicesonline.org/2011/07/27/the-politics-of-surveillance-the-erosion-of-privacy-in-latin-america/

6.6 Europe and North America

Carter, E. (2005), "Outlaw Speech on the Internet: Examining the Link Between Unique Characteristics of Online Media and Criminal Libel Prosecutions", Santa Clara Computer and High – Technology Law Journal 21. 2 (Jan 2005): 289-318, available at http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1376&context=chtlj

Elwood, S. and Leszczynski, A. (2010), Privacy, reconsidered: New representations, data practices, and the geoweb, University of Washington, available at: http://www.sciencedirect.com/science/article/pii/S001671851000093X

Lin, E. (2002), Prioritizing Privacy: A Constitutional Response to the Internet, Berkeley Technology Law Journal, available at: http://www.law.berkeley.edu/journals/btlj/articles/vol17/LIN.pdf

Burghardt, T., Böhm, K., Buchmann, E., Kühling, J. and Sivridis A. (2009), A Study on the Lack of Enforcement of Data Protection Acts, available at: http://dbis.ipd.uni-karlsruhe.de/download/bu09edemocracy.pdf

Kuan Hon, W., Millard, C. and Walden, I. (2011), "The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing", Oxford University Press, available at: http://idpl.oxfordjournals.org/content/1/4/211.full

Access Now.org, European Digital Rights, Trans Atlantic Consume Dialog (2012), ¿Qué hace que el ACTA sea tan controversial? (Y porque a los euro-parlamentarios debería importarles), available at: http://www.manzanamecanica.org/files/ACCESS_EDRI_TACD-por_que_oponerse_al_acta_ES.pdf

La Quadrature Du Net, Internet & Libertés (2012), Winning BIG on ACTA and Beyond!, available at: http://www.laquadrature.net/en/winning-big-on-acta-and-beyond

American Civil Liberties Union (2011), Government Requests For Twitter Users' Personal Information Raise Serious Constitutional Concerns, Says ACLU, available at: http://www.aclu.org/technology-and-liberty/government-requests-twitter-users-personal-information-raise-serious-constitu

Budish, R. (2007), In the Face of Danger: Facial Recognition and the Limits of Privacy Law, available at: http://hlr.rubystudio.com/media/pdf/facial_recognition_privacy_law.pdf

Consejo de la Unión Europea (2011), Acuerdo Comercial de Lucha Contra la Falsificación (ACTA), available at: http://register.consilium.europa.eu/pdf/es/11/st12/st12196.es11.pdf, available in english at: http://register.consilium.europa.eu/pdf/en/11/st12/st12196.en11.pdf

De Gucht, K (2012), ACTA: "Making the right choice", European Parliament, International Trade Committee, available at: http://trade.ec.europa.eu/doclib/docs/2012/june/tradoc_149559.pdf

European Commission (2010), "Specific Privacy Statement, Public Consultation on the review of the scheme of generalised tariff preferences (GSP)", available at: http://trade.ec.europa.eu/doclib/docs/2010/march/tradoc_145976.pdf

Gindin, S. (1997), Lost and Found in Cyberspace, San Diego Law Review, available at: http://www.info-law.com/lost.html

Instituto Nacional de Tecnologías de la Comunicación y Agencia Española de Protección de Datos Personales (2009), "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online", available at: http://www.inteco.es/Seguridad/Observatorio/Estudios/est_red_sociales_es

LRDP Kantor and Centre for Public Reform (2010), "Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments—final report to European Commission", available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf

Mitrano, T. (2006), A Wider World: Youth, Privacy, and Social Networking Technologies, EDUCAUSE Review, vol. 41, no. 6, available at: http://www.educause.edu/ero/article/wider-world-youth-privacy-and-social-networking-technologies

Perez, J.C. (2009), Facebook Will Shut Down Beacon to Settle Lawsuit, The New York Times, September 19 2009, available at: http://www.nytimes.com/external/idg/2009/09/19/19idg-facebook-will-shut-down-beacon-to-settle-lawsuit-53916.html

Press Release / Memorandum for publication, Overview of the European Commission's referral of ACTA to the European Court of Justice, available at: http://trade.ec.europa.eu/doclib/docs/2012/may/tradoc_149464.doc.pdf

Privacy International (2011), "Surveillance Monitor 2011: Assessment of surveillance across Europe", available at https://www.privacyinternational.org/reports/surveillance-monitor-2011-assessment-of-surveillance-across-europe

Privacy Rights Clearinghouse, "Online Privacy: Using the Internet Safely", available at: http://www.privacyrights.org/fs/fs18-cyb.htm

Slazmann, V. (2000), "Are Public Records Really Public? The Collision Between the Right to Privacy and the Release of Public Court Records Over the Internet", Baylor Law Review, available at: http://works.bepress.com/cgi/viewcontent.cgi?article=1011&context=victoria_salzmann

Sprague, R. (2009), Rethinking Information Privacy in an Age Of Online Transparency, available at: http://lawarchive.hofstra.edu/pdf/academics/journals/laborandemploymentlawjournal/labor_vol25no2_sprague.pdf

York, J.C. (2011), A Case for Pseudonyms, available at: https://www.eff.org/deeplinks/2011/07/case-pseudonyms

6.7 Gender

Allen, A. (2000), Gender and Privacy in Cyberspace, Stanford Law Review Vol. 52, No. 5, Symposium: Cyberspace and Privacy: A New Legal Paradigm? (May, 2000), pp. 1175-1200, available at : http://www.jstor.org/stable/1229512

Association for Progressive Communications (2012), "Critically absent: Women in internet governance. A policy advocacy toolkit", available at http://www.violenceisnotourculture.org/resources/critically-absent-women-internet-governance-policy-advocacy-toolkit

Bartow, A. (2000), "Our Data, Ourselves: Privacy, Propertization, and Gender", available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=374101

Burnett, K., Subramaniam, M., and Gibson, A. (2009), "Latinas cross the IT border: Understanding gender as a boundary object between information World", First Monday, Volume 14, Number 9, available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2581/228

Clifford, B. (2008), "Online privacy sensitivity and gender: A case study of a highly-educated adult population", available at http://gradworks.umi.com/33/36/3336862.html

EPIC, "Gender and Electronic privacy", available at http://epic.org/privacy/gender/

Grubbs Hoy, M. and Milne, G. (2010), "Gender Differences in Privacy-Related Measures for Young Adult Facebook Users", available at http://jiad.org/article130 .

VAW (2010), "Your Privacy, Your Safety", Violence Against Women Online Resources, available at http://www.vaw.umn.edu/documents/internet-safety/internet-safety.html

Youn, S. and Hall, K., (2008), “Gender and online privacy among teens: risk perception, privacy concerns, and protection behaviors”, available at http://www.ncbi.nlm.nih.gov/pubmed/18954276 .

BIBLIOGRAPHY

Alianza Regional por la Libre Expresión e Información, *Saber Más III: Regional Report on Access to Information and the Protection of Personal Data* (2011: Alianza Regional por la Libre Expresión e Información).

Allison, D., *Protecting Human Rights in the Digital Age: Understanding Evolving Freedom of Expression and Privacy Risks in the Information and Communications Technology Industry* (2011: BSR: The Business of a Better World).

Ang, P., "The Role of Self-Regulation of Privacy and the Internet" (2011) 1 *Journal of Interactive Advertising* 1.

Angwin, J., & Valentino-Devries, J. (2011). Apple's iPhones and Google's Androids Send Cellphone Location. Wall Street Journal. Retrieved December 13, 2011, from http://online.wsj.com/article/SB10001424052748703983704576277101723453610.html

ARTICLE 19, *Written Comments in Inter-American Court of Human Rights Case No. 12.524: Jorge Fontevecchia and Hector D'amico v. Argentina* (2011: ARTICLE 19, London).

Baker & MacKenzie, "A Big Year for Privacy in Greater China: 2011 Wrap Up" *Newsletter: January 2012.*

Banwell, L., Ray, K., Coulson, G., Urquhart, C., Lonsdale, R., Armstrong, C., Thomas, R., et al. (2004). The JISC User Behaviour Monitoring and Evaluation Framework. Journal of Documentation, 60(3), 302-320.

Beresford A. and Stajano F. (2003) "Location Privacy in Pervasive Computing", IEEE Communications Society (http://www.cl.cam.ac.uk/~fms27/papers/2003-BeresfordSta-location.pdf).

Biermann, Kai. 2011. "Data Protection: Betrayed by our own data." *ZEIT Online*. Retrieved March 1, 2012 (http://www.zeit.de/digital/datenschutz/2011-03/data-protection-malte-spitz).

Bits of Freedom, *Contribution Bits of Freedom to the Second Universal Periodic Review of the Netherlands by the United Nations Human Rights Council* (2011: Bits of Freedom, Amsterdam).

Bloustein, E. "Privacy as an aspect if human dignity: an answer to Dean Prosser" (1964) 39 NYU L Rev 962.

Boyd, D., Hargittai, E., Schultz, J., & Palfrey, J. (2011). Why parents help their children lie to Facebook about age: Unintended consequences of the "Children's Online Privacy Protection Act'. First Monday, 16(11).

Brenton, M. (1964) *The Privacy Invaders,* Coward-McCann.

BuiltWith. (2011). Google Analytics Usage Statistics - Websites using Google Analytics. Retrieved December 13, 2011, from http://trends.builtwith.com/analytics/Google-Analytics

Burchell, J., "The Legal Protection of Privacy in South Africa: A Transplantable Hybrid" (2009) 13 *Electronic Journal of Comparative Law* 1.

Cabanellas, G., "The Right of Publicity under Argentine Law" (1998) 18 *Loyola of Los Angeles Entertainment Law Review* 449.

Cai, L., & Chen, H. (2011). TouchLogger: inferring keystrokes on touch screen from smartphone motion. HotSec'11 Proceedings of the 6th USENIX conference on Hot topics in security (p. 9). Berkeley, CA, USA: USENIX Association.

Calcutt, D., *et al*., 1990. *Report of the committee on privacy and related matters*, Chairman David Calcutt QC, London: HMSO (Cmnd. 1102).

Carrasquilla, L., "Personal data protection in Latin America: retention and processing of personal data in the Internet sphere", in Bertoni, E., Ed., *Towards an Internet Free of Censorship. Proposals for Latin America* (2012, Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE), Buenos Aires).

Carter, D. L., & Carter, J. G. (2009). The Intelligence Fusion Process for State, Local, and Tribal Law Enforcement. Criminal Justice and Behavior, 36(12), 1323-1339.

Cavoukian, A. "Whole Body Imaging in Airport Scanners: Building in Privacy by Design" Information & Privacy Commissioner, Ontario, Canada. June 2009 (http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf).

Center for Democracy and Technology, *Data Retention Mandates: A Threat to Privacy, Free Expression and Business Development* (2011: Center for Democracy and Technology, Washington).

Center for Democracy and Technology, *Seeing Is ID'ing: Facial Recognition & Privacy* (2011: Center for Democracy and Technology, Washington).

Chaos Computer Club. (2011). Chaos Computer Club analyzes government malware. Retrieved December 13, 2011, from http://ccc.de/en/updates/2011/staatstrojaner

Cho, D., *Real Name Verification Law on the Internet: A Poison or Cure for Privacy?* Available at: http://weis2011.econinfosec.org/papers/Real%20Name%20Verification%20Law%20on%20the%20Internet%20-%20A%20Poison%20or%20Cu.pdf

Cirio, P., & Ludovico, A. (2011). Face-to-Facebook. Face-to-Facebook. Retrieved from www.face-to-facebook.net/theory.php

Clarke, G. (2011). Do-Not-Track laws gain US momentum. The Register. Retrieved December 13, 2011, from http://www.theregister.co.uk/2011/05/06/senate_do_not_track/

Compa, E. and Bertoni, E., *Emerging Patterns in Internet Freedom of Expression: Comparative Research Findings in Argentina and Abroad* (2010: Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE), Buenos Aires).

Cooper, A. (2007). Competing on Privacy. Center for Democracy and Technology. Retrieved December 13, 2011, from https://www.cdt.org/blogs/alissa-cooper/competing-privacy

Economist, (2010) "Clicking for Gold: How internet companies profit from data on the web", in "A special report on managing information" The Economist, Volume 394, Number 8671

Edelman, B. (2006), "Adverse Selection in Online "Trust" Certifications" Harvard Business School, published online http://www.benedelman.org/publications/advsel-trust.pdf

Electronic Frontier Foundation (EFF). (2011). Mobile Devices. Surveillance Self-Defense Project. Retrieved December 13, 2011, from https://ssd.eff.org/tech/mobile

Electronic Privacy Information Center and Privacy International, *Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments* (2007: Electronic Privacy Information Center and Privacy International, United States of America)

Electronic Privacy Information Center. (2011). Face Recognition. (EPIC). Retrieved December 13, 2011, from https://epic.org/privacy/facerecognition/

Electronic Privacy Information Center. (2011). Personal Surveillance Technologies. Retrieved December 13, 2011, from https://epic.org/privacy/dv/personal_surveillance.html

Electronic Privacy Information Center. (2011). Social Networking Privacy. Retrieved December 13, 2011, from https://epic.org/privacy/socialnet/

Enders, A., Hungenberg, H., Denker, H.-P., & Mauch, S. (2008). The long tail of social networking. Revenue models of social networking sites. European Management Journal, 26(3).

EPIC, *Cloud Computing*, published online http://epic.org/privacy/cloudcomputing/

EPIC, *WHOIS*, published online http://epic.org/privacy/whois/

EPIC, *Privacy and Consumer Profiling* http://epic.org/privacy/profiling/

European Commission, *Report From the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, Brussels, 18 April 2011, COM(2011) 225 final.

European Commission. (2010). Digital Agenda: Commission refers UK to Court over privacy and personal data protection [IP/10/1215]. Retrieved December 13, 2011, from http://europa.eu/rapid/pressReleasesAction.do?reference=IP/10/1215

European Digital Rights (EDRI), *Shadow evaluation report on the Data Retention Directive (2006/24/EC)* (17 April 2011: European Digital Rights, Brussels).

European Parliament. (2000). Charter of fundamental rights of the European Union. Luxembourg: Office for Official Publications of the European Communities.

Facebook, (2012) " Statistics" published online http://www.facebook.com/press/info.php?statistics

Fayyad, U., Grinstein, G. and Wierse, A. (2001) “Information Visualization in Data Mining and Knowledge Discovery”. Morgan Kaufman Publishers.

Federal Trade Commission, (1999) “Self-regulation and Privacy Online: A Report to Congress” March 1999, Published online at http://www.ftc.gov/os/1999/07/privacy99.pdf

Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers: Preliminary FTC Staff Report*, December 2010.

Fernández, G., *China Publishes Draft Privacy Guidelines*, 14 April 2011 (Hogan Lovells).

Filastò, A. (2011). Blue Coat device logs indicate the levels of censorship in Syria. Retrieved December 13, 2011, from http://hellais.github.com/syria-censorship/

Filippi, P. de. (2011). Notes on Privacy in the Cloud.

Fitzpatrick, M. “Mobile that allows bosses to snoop on staff developed” BBC News 10/03/2010 http://news.bbc.co.uk/1/hi/technology/8559683.stm

Flaherty, D. H. (1999). Visions of Privacy: Past, present and future. Visions of privacy: policy choices for the digital age (pp. 19-38). University of Toronto Press.

Fuchs, C. (2009). Social networking sites and the surveillance society a critical case study of the usage of studiVZ, Facebook, and MySpace by students in Salzburg in the context of electronic surveillance. Salzburg : Forschungsgruppe Unified Theory of Information.

Gates, J., & Privacy Working Group. (1995). Privacy and the National Information Infrastructure: Principles for Providing and using Personal Information. Information Policy Committee, Information Infrastructure Task Force. Retrieved from http://aspe.hhs.gov/datacncl/niiprivp.htm

Gellman, R., & World Privacy Forum. (2009). Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing. Retrieved from http://www.worldprivacyforum.org/pdf/WPF_Cloud_Privacy_Report.pdf

Google. (2008). Google Zeitgeist 2008. Retrieved December 13, 2011, from https://www.google.com/intl/en/press/zeitgeist2008/world.html#top

Google. (2011). Google Transparency Report. Google. Retrieved December 13, 2011, from https://www.google.com/transparencyreport/

Gorge, M. (2008). Data protection: why are organisations still missing the point? Computer Fraud & Security, 2008(6), 5-8. doi:10.1016/S1361-3723(08)70095-2.

Greenleaf, G., “Asia-Pacific data privacy: 2011, year of revolution?” [2011] UNSWLRS 30.

Greenleaf, G., *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108*, University of New South Wales Faculty of Law Research Series, Paper 42, 2011.

Griffiths, J. (n.d.). Student searching behaviour and the web: use of academic resources and google. Library trends, 2005, vol. 53, no. 4, pp. 539-554.

Hargittai, E. (2010). Trust online: young adults' evaluation of web content. International Journal of Communication, 4.

Higginbotham, S. (2010). iPhone 4 Sensors Highlight a Bright Spot for VCs. GigaOM. Retrieved from http://gigaom.com/2010/06/08/iphone-4-sensors-highlight-a-bright-spot-for-vcs/

Hilles, L., & Jugendschutz.Net. (2011). Verlockt - Verlinkt - verlernt? Werbung, Vernetzung und Datenabfragen auf Kinderseiten. Mainz, Germany.

Human Rights Council (2009), "Promotion and protection of all human rights, civil, political economic, social and cultural rights, including the right to development: Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin". Human Rights Council, Thirteenth session, Agenda item 3. 28 December 2009, A/HRC/13/37 http://www2.ohchr.org/english/issues/terrorism/rapporteur/docs/A_HRC_13_37_AEV.pdf

Hunton & Williams, *Client Alert*, January 2010. Available at http://www.hunton.com/files/News/4bfa5361-4d8f-4c7e-af03-75055a82202c/Presentation/NewsAttachment/7d2612ba-40d6-4884-83de-c01965341d41/new_chinese_tort_liability_law.pdf

Initiative Vorratsdatenspeicherung. (2011). Stoppt die Vorratsdatenspeicherung. Retrieved December 13, 2011, from https://www.vorratsdatenspeicherung.de/static/verfassungsbeschwerde_de.html

Inter-American Commission on Human Rights, *Report on the Situation of Human Rights Defenders in the Americas.* Available at: http://www.cidh.org/countryrep/defenders/defenderschap1-4.htm

Introna, L. D., & Nissenbaum, H. F. (2009). Facial Recognition Technology: A Survey of Policy and Implementation Issues. SSRN eLibrary. SSRN. doi:10.2139/ssrn.1437730.

ITU World Telecommunication, 2010. Measuring the Internet Society. [online] http://www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without_annex_4-e.pdf

Kilkelly, U., *The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human Rights: Human rights handbooks, No. 1* (2001: Directorate General of Human Rights, Council of Europe, Strasbourg).

King, E. (2011). Our response to EU consultation on legality of exporting surveillance and censorship technology. Privacy International. Retrieved December 13, 2011, from https://www.privacyinternational.org/article/our-response-eu-consultation-legality-exporting-surveillance-and-censorship-technology

Koops, B., and Sluijs, J., *Network Neutrality and Privacy According to Art. 8 ECHR*, Tilburg Law School Legal Studies Research Paper Series No. 017/2011.

La Rue, F. (2011). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue to the U.N. Human Rights Council [A/HRC/14/23]. Geneva: United Nations.

Leon, P., Ur, B., Balebako, R., Cranor, L., Shay, R., and Wang, Y., *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising* (2011: Carnegie Mellon University, Pittsburgh).

Leong, F. and Bakar, H., "Personal Data Protection Act 2010" (July-September 2010) *Legal Herald* 1.

Lessig, L. (1999) "Code and the Laws of Cyberspace" Basic Books, New York.

Marinos, L., & European Network and Information Security Agency. (2011). Cyber-bullying and online grooming: helping to protect against the risks. Heraklion, Greece.

Marsh, R., "Legislation for Effective Self-Regulation: A New Approach to Protecting Personal Privacy on the Internet" (2009) 15 *Michigan Telecommunications and Technology Law Review* 543.

Mayer, J. (2011). Tracking the Trackers: Microsoft Advertising. Center for Internet and Society (CIS), Stanford Law School. Retrieved December 13, 2011, from http://cyberlaw.stanford.edu/node/6715.

McKenzie, P. Dicker, A., and Fang, J., *China Issues New Guidelines on Data Privacy Protection*, 11 April 2011 (Morrison Foerster).

McKenzie, P., and Milner, G., *China Update, March 2009: Recent Developments in Data Protection*, 9 March 2009 (Morrison Foerster).

McKenzie, P., and Milner, G., *Data Privacy in China: Criminal Law Developments*, 25 January 2010 (Morrison Foerster).

Mueller, M. (2011). DPI Technology from the standpoint of Internet governance studies: An introduction. Syracuse University. Retrieved from http://dpi.ischool.syr.edu/Technology_files/WhatisDPI-2.pdf

Mueller, M. L. (2010). Networks and States: The Global Politics of Internet Governance (p. 280). MIT Press.

Mueller, P. (2011). Offene Staatskunst - Strategie für eine vernetzte Welt. Arbeitskreis Internet Governance. Munich, Germany: Münchner Centrum für Governance-Forschung (MCG).

Netter, W. "The Death of Privacy" Privacy Module I: Data Profiling Introduction, University of Harvard, 2002 http://cyber.law.harvard.edu/privacy/Module2_Intro.html

Niemietz v Germany (1992), 16 EHRR 97.

Ong, R., "Recognition of the right to privacy on the Internet in China" (2011) 1 *International Data Privacy Law* 172.

Padania, S., Gregory, S., Alberdingk-Thijm, Y., & Nunez, B. (2011). Cameras Everywhere Report 2011. Retrieved from http://www.witness.org/cameras-everywhere/report-2011

Pang, D., Chen, B., & Lee, D. (2008). Eight now held in internet sex probe. The Standard. Retrieved December 13, 2011, from http://www.thestandard.com.hk/news_detail.asp?pp_cat=12&art_id=61125&sid=17431562&con_type=3#

Pomfret, J. (2009). Technician guilty in Edison Chen sex pictures trial. Victoria News. Retrieved December 13, 2011, from http://www.vicnews.com/entertainment/television/43998412.html

Privacy Foundation, July 9, 2001 http://www.sonic.net/~undoc/extent.htm

Privacy International, (2006) "Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments" http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-65435&als[theme]=Privacy%20and%20Human%20Rights

Privacy International, 1996, ID Card Frequently Asked Questions https://www.privacyinternational.org/article/id-card-frequently-asked-questions

Privacy International. (2006). Privacy International 2006 - Executive Summary. Retrieved December 13, 2011, from https://www.privacyinternational.org/article/phr2006-executive-summary

Privacy International. (2011). United Kingdom – Privacy Profile. Privacy International. Retrieved December 13, 2011, from https://www.privacyinternational.org/article/united-kingdom-privacy-profile.

Privacy Rights Clearinghouse (2010), "Fact Sheet 18: Privacy and the Internet: Traveling in Cyberspace Safely" Published online http://www.privacyrights.org/fs/fs18-cyb.htm

Reding, V. 2010, *Next steps for Justice, Fundamental Rights and Citizenship in the EU European Policy Centre Briefing Brusse*ls, 18 March 2010, Brussels. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/10/108

Robertson, D. S. (1998). The New Renaissance: Computers and the Next Level of Civilization (p. 208). Oxford University Press, USA.

Robinson, N., Graux, H., Botterman, M., and Valieri, L., *Review of EU Data Protection Directive: Summary*, prepared for the UK Information Commissioner's Office, May 2009.

Rooney, B. (2011). U.K. Publishes EU "Cookie" Directive Guidelines. Wall Street Journal. Retrieved December 13, 2011, from http://blogs.wsj.com/tech-europe/2011/05/09/u-k-publishes-e-u-cookie-directive-guidelines/

Ross, L., Gao, K., and Zhou, A., *China Issues Draft Guidelines on Online Privacy, Announces new Agency to Supervise the Internet*, 19 May 2011 (Wilmer Hale).

Rotenburg M. And Hoofnaglem C. "Submission to the House Government Reform Committee on Data Mining" March 25, 2003. http://epic.org/privacy/profiling/datamining3.25.03.html

Schulman, A. "The Extent of Systematic Monitoring of Employee E-mail and Internet Use".

Scott, J. C. (1998). Seeing like a state : how certain schemes to improve the human condition have failed. New Haven: Yale University Press.

Senior, A., & Pankanti, S. (2011). Privacy protection and face recognition. In S. Z. Li & A. K. Jain (Eds.), Handbook of Face Recognition. Springer.

Shaker, L. (2006, April 3). In Google we trust: Information integrity in the digital age. First Monday. Ghosh, Rishab Aiyer. Retrieved from http://frodo.lib.uic.edu/ojsjournals/index.php/fm/article/view/1320/1240

Silva, A., "Personal Data Protection and Online Services in Latin America" in Bertoni, E., Ed., *Towards an Internet Free of Censorship. Proposals for Latin America* (2012, Centro de Estudios en Libertad de Expresion y Acceso a la Informacion (CELE), Buenos Aires).

Silver, V., & Elgin, B. (2011). Torture in Bahrain Becomes Routine With Help From Nokia Siemens. Bloomberg. Retrieved August 28, 2011, from http://www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

Soghoian, C. (2007) "The Problem of Anonymous Vanity Searches" Indiana University Bloomington - School of Informatics. Published online http://papers.ssrn.com/sol3/papers.cfm?abstract_id=953673

Solove, D.J. (2008). *Understanding Privacy* Harvard University Press.

Sonne, P., & Coker, M. (2011). Foreign Firms Helped Gadhafi Spy on Libyans. Wall Street Journal. Retrieved September 23, 2011, from http://online.wsj.com/article/SB10001424053111904199404576538721260166388.html

South African Law Reform Commission, *Project 124: Privacy And Data Protection Report* (2009: South African Law Reform Commission).

Stewart, B. (2004). A comparative survey of data protection authorities. Privacy Law and Policy Reporter, 11(2).

Stuart, K. (2011). PlayStation Network hack: what every user needs to know. The Guardian. Retrieved December 13, 2011, from http://www.guardian.co.uk/technology/gamesblog/2011/apr/27/psn-security-advice

Sung-jin, Y. (2011). 35m Cyworld, Nate users' information hacked. The Korea Herald. Retrieved December 13, 2011, from http://www.koreaherald.com/national/Detail.jsp?newsMLId=20110728000881

Sweeney, L. "Strategies for De-Identifying Patient Data for Research" Carnegie Mellon University, Data Privacy Lab, 1998 http://www.ocri.ca/ehip/2005/presentations/Sweeney_bw.pdf

Telecommunications Research Centre. (2011). World telecommunication. Geneva: ITU.

The Economist, (2010) "New Rules for Big Data", in "A special report on managing information" The Economist, Volume 394, Number 8671.

TRUSTe, (2009), "TRUSTe Press Releases and Facts" published online http://www.truste.com/about_TRUSTe/press-room.html

Tufekci, Z. (2010). Facebook: The Privatization of our Privates and Life in the Company Town. Technosociology: Our Tools, Ourselves. Retrieved December 13, 2011, from http://technosociology.org/?p=131

United Nations Human Rights Committee, General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17), adopted 4 August 1988.

Valentino-Devries, J., Sonne, P., & Malas, N. (2011). Blue Coat Acknowledges Syria Used Its Gear for Internet Censorship Amid Arab Spring. Wall Street Journal. Retrieved December 13, 2011, from http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

Vasile, J. (2011). Presentation of the FreedomBox. Elevate 2011 - Music, Arts and Political Discourse. Graz, Austria: Verein zur Förderung des gesellschaftspolitischen und kulturellen Austausches.

Volio, F. "Legal Personality, Privacy and the Family" in Henkin (ed), The International Bill of Rights (Columbia University Press 1981).

W3Techs. (2011). Usage Statistics and Market Share of Traffic Analysis Tools for Websites. Q-Success Web-based Services. Retrieved December 13, 2011, from http://w3techs.com/technologies/overview/traffic_analysis/all

Warren, S. and Brandeis, L., "The Right to Privacy" (1890) 4 *Harvard Law Review* 193.

Weber, T. Cybercrime threat rising sharply, BBC News, 31/01/09 http://news.bbc.co.uk/1/hi/business/davos/7862549.stm

Westin, A. (1967) "Privacy and Freedom" Atheneum, New York.

Workman, R., "Balancing the Right to Privacy and the First Amendment" (1992) 29 *Houston Law Review* 1059.

York, J. C. (2010). Policing Content in the Quasi-Public Sphere. Boston, MA: Open Net Initiative Bulletin. Berkman Center. Harvard University.

INTERVIEWS

Prof Guo Liang, Director of China Internet Project and Member of UN Secretary General's Multi-stakeholder Advisory Group for the Internet Governance Forum, China Academy of Social Sciences, China

Mr Yang Wang, Ph.D., Research Scientist, CyLab Carnegie Mellon University, U.S

Ms Ceren Unal, LL.M., Department of Civil Law, Bilkent University Faculty of Law

Prof ANG Peng Hwa, Singapore Internet law expert. Director, Singapore Internet Research Centre

Mr Erick Iriarte Ahon, Latin America privacy expert. Monitor in Latin America

Katitza Rodriguez, International Rights Director, EFF

Karen Reilly, Public Policy Director, The TOR Project

Ali G. Ravi, TacticalTech

Moez Chackchouk, Association Tunisienne d'Internet, ATI

Primavera de Filippi, Université Panthéon Assas Paris II

Peter Parycek, Head of Center for E-Governance, Donau-Universität Krems

Robert Bodle, Uni Mount Joseph

Sameer Padania, Macroscope and Witness

Peter Bradwell, Open Rights Group

Ulrike Höppner, Johann Wolfgang Goethe-Universität Frankfurt

Anonymous, Former employee of large technology company

Anonymous, Former employee of large technology company

Anonymous, Former employee of large technology company

Eduardo Bertoni, Director of Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Argentina

Dr. Hong Xue, Professor of Law, Director of Institute for the Internet Policy & Law (IIPL), Beijing Normal University

Monique Fanjoy, New Media Officer, Office of the Privacy Commissioner of Canada

Abu Bakar Munir, Professor of Law, Faculty of Law, University of Malaya, Malaysia

Joe McNamee, EU Advocacy Co-ordinator, European Digital Rights

Amr Gharbeia, Egyptian Initiative for Personal Rights

Jamie Horsley, Senior Research Scholar & Lecturer in Law, Yale Law School, Deputy Director, The China Law Center

Nepomuceno Malaluan, Co-Director, Institute for Freedom of Information, the Philippines

Cynthia M. Wong, Director, Global Internet Freedom Project, Center for Democracy & Technology

Sinfah Tunsarawuth, Independent media lawyer and writer, Bangkok, Thailand

Prim Ot van Daalen, Director, Bits of Freedom, the Netherlands

Sunil Abraham, Director, Centre for the Internet and Society, India

APPENDIX 1: ABBREVIATIONS AND ACRONYMS

ACHPR	African Charter on Human and Peoples' Rights
ACHR	American Convention on Human Rights
APEC	Asia-Pacific Economic Cooperation
CNIL	Commission nationale de l'informatique et des libertés
COPPA	Children's Online Privacy Protection Act
DPAI	Data Protection Authority of India
DPI	Deep packet inspection
DSF	Digital Signage Federation
ECHR	European Convention on Human Rights
ECPA	Electronic Communication Privacy Act
EDRI	European Digital Rights
EFF	Electronic Frontier Foundation
ENISA	European Network and Information Security Agency
EPIC	Electronic Privacy Information Center
FRT	facial recognition technology
FTC	Federal Trade Commission
GNI	Global Network Initiative
GPS	Global Positioning Systems
GPS	Global Positioning Systems
ICCPR	International Covenant on Civil and Political Rights
IMEI	unique mobile device (IMEI)
IMF	International Monetary Fund
IMSI	SIM card identifiers,
IP	Internet Protocol
ISP	Internet Service Provider
LLU	local loop unbundling

MENA	Middle East and North Africa
MIIT	Ministry of Industry and Information Technology
NAI	Network Advertising Initiative
NTRA	National Telecommunication Regulatory Authority
OAS	Organization of American States
OECD	Organisation for Economic Co-operation and Development
OMB	Office of Management and Budget
OSCE	Organization for Security and Co-operation in Europe
OSP	Online Service Provider
POPAI	Point of Purchase Advertising International
RFID	Radio-Frequency Identification
SAC	Standardisation Administration of China
T&Cs	terms and conditions
TRAI	Telecommunications Regulatory Authority of India
UDHR	Universal Declaration of Human Rights (UDHR)

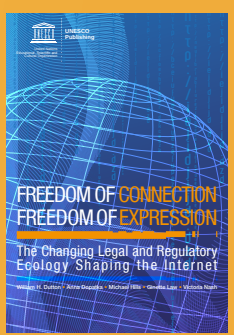
APPENDIX 2:
LIST OF FIGURES AND BOXES

UNESCO, as enshrined in its Constitution, promotes the "free flow of ideas by word and image", and has committed itself to enabling a free, open and accessible Internet space as part of promoting comprehensive freedom of expression online and offline. We hope that this publication will provide UNESCO Member States and other stakeholders, national and international, with a useful reference tool. It is our wish that this publication will contribute to bringing stakeholders together for informed debate on approaches that are conducive to privacy protection without compromising freedom of expression. In the coming years, UNESCO will specifically seek to disseminate information about good practices and international collaboration concerning the points of intersection between freedom of expression and privacy. Research on safeguarding the principle of freedom of expression in Internet policy across a range of issues will continue to be part of UNESCO's normative mandate and technical advice to stakeholders.

Jānis Kārkliņš
Assistant Director-General for Communication and Information, UNESCO

Toby Mendel • Andrew Puddephatt • Ben Wagner • Dixie Hawtin • Natalia Torres

UNESCO SERIES ON INTERNET FREEDOM
Communication and Information Sector
United Nations Educational,
Scientific and Cultural Organization



United Nations
Educational, Scientific and
Cultural Organization

Communication and Information Sector

9 789231 042416