ARTICLE 19

Draft Background Paper:

Friend or Foe? Protecting freedom of expression and privacy in the digital age

May 2016

Report

Table of Contents

Introduction

It is possible to see the rights to free expression and privacy as being two sides of the same coin, with the right to privacy enabling ordinary individuals the autonomy and dignity to independently develop and impart their ideas, opinions and information. The right to privacy provides the space and security necessary for individuals to seek out and receive information. Both rights play an essential role in placing fundamental restraints on the exercise of power by those who possess it – governments and their agents, as well as corporate actors and public figures.

The right to freely express and receive information is a fundamental pillar of any democratic society, ensuring individuals are able to participate wholeheartedly in cultural, educational or political endeavours, and keep public and private power in check. In ensuring that individuals have a secure physical and intellectual space to seek information, expand their knowledge, develop opinions, and express ideas free from intrusion or critique, the right to privacy acts as a pre-condition to the exercise of the right to freedom of expression and information. The confidence to communicate our ideas and opinions, however controversial, is underpinned by the knowledge that we are protected from any unlawful interference with our communications by those we might wish to conceal them from.

Yet the potential for conflict between these two pillars of a democratic society has also long existed, and indeed is provided for by international human rights law. To the extent that privacy can shield individuals from public scrutiny, it constitutes a restriction on the right to freely and unselfconsciously espouse opinions and report information. Oftentimes, the competing imperatives established by each of the rights can be difficult to reconcile, including when media reporting involves the exposure of private information of public individuals, situations which necessitate complex determinations of the definition of the public interest.

The contest between free expression and privacy is particularly acute in the context of internet publishing platforms, social media networks and search engines that facilitate the vast and contemporaneous dissemination of information and expression, and which challenge traditional conceptions of journalism, private space, public figures, celebrity and publication. Digital technologies have multiplied the means for expression and information dissemination, creating new platforms for public and private speech, new opportunities for dissent and critique, and new ways of scrutinising State and corporate behaviour. At the same time, these digital technologies have enabled an exponential increase in the creation of private data pertaining to individuals' movements, communications, shopping habits, political preferences, and financial flows. This data is often generated and interrogated by the corporate entities which provide internet services and technologies, but also is increasingly tracked and surveilled by State actors as well, impacting on individuals' privacy and chilling their free speech.

Internet users are also consciously publishing greater amounts of private information about themselves and, as they interact with and make full use of publication platforms such as social media networks. The auxiliary effects of social media use include the proliferation of activities such as trolling, bullying, revenge porn, harassment, and doxing, creating new challenges to which existing understandings of privacy and free expression need to be applied.

The internet has also transformed conventional privacy violations by dramatically increasing the scale, scope and reach of such violations; and created barriers to the enforcement of rights protections and remedies. The problem of scale equally exacerbates the threat posed to freedom of expression by sanctions for privacy violations; assessing the proportionality of sanctioning the retraction, deletion or take down of information from the internet requires a fundamentally different calculation when taking into account the reach of such sanctions, the sheer numbers of individuals affected by them, and their chilling effect on free expression and access to information. While international human rights law contains the tools for reconciling these competing concerns, new understandings of existing norms are required in order to ensure they appropriately take into account the challenges of the digital era.

ARTICLE 19 believes that, for the most part, free expression and privacy can mutually exist, and the promotion and enjoyment of one can reinforce the other; this is particularly in the context of State surveillance, corporate data collection and the protection and promotion of journalistic sources and whistleblowers. However, there will be situations in which the rights compete, and such situations have increased in number and complexity with the advent of the internet and digital technologies. Mediating them requires understanding the implications of the enjoyment of each for the protection of the other, and – given that the ripple effects of decisions which effect the digital universe do not stop at national borders – taking a global view of such implications. It also requires an updated understanding of how existing human rights standards should be applied to these conflicts, particularly in the context of new technologies. ARTICLE 19 strives to develop a set of principles that practitioners, courts, governments and corporate actors can use to guide decisions that preference the rights to free expression or privacy over the other.

This paper explores the background against which such principles will sit. After analysing the international legal framework for freedom of expression and privacy, this paper views the rights through two separate lenses: first, it approaches privacy as a condition for free expression, looking in particular at the role of privacy in preventing State and corporate surveillance that stifles free expression. Second, it approaches privacy as in contest with free expression, analysing the circumstances in which privacy, and remedies to its violation, act as a barrier to the free and confident expression of and access to ideas and information.

The rights framework

The right to freedom of expression

The free flow of opinions, ideas, information and expression is one of the essential foundations of any democratic society.[1] Enshrined in international law since 1948[2] but with roots which reach back to the French Declaration of the Rights of Man and the Citizen in 1789 and the First Amendment to the United States Constitution in 1791, the right to freedom of expression and opinion is now enshrined in a number of international and regional conventions, including the International Covenant on Civil and Political Rights (Article 19), the European Convention on Human Rights (Article 10), the European Union Charter of Fundamental Rights (Article 11), the American Convention on Human Rights (Article 13), the African Charter on Human and People's Rights (Article 9) and the ASEAN Human Rights Declaration (Article 23). It has come to encapsulate a right not only to impart, but also to seek and receive, information and ideas of all kinds, regardless of frontiers; the right to access information is increasingly accepted under international law as an integral part of the right to freedom of expression.[3]

The medium of expression

International human rights law protects the expression of ideas and opinions for all purposes, from political[4] and religious[5] discourse, to cultural and artistic expression,[6] and in all forms, including spoken and sign language, written materials and non-verbal images and objects. The medium one chooses to express oneself does not determine or attenuate the protection of the right; nevertheless, the role of the internet in redefining the concepts of expression and information cannot be overstated. In addition to dramatically recasting the form, reach, scope and effect of news media and journalistic activity, the internet has transformed the role of the individual in creating, reproducing, storing and accessing knowledge, truth and memory: in the words of the UN Special Rapporteur on freedom of expression in his landmark 2011 report, "individuals are no longer passive recipients, but also active publishers of information" contributing "to the discovery of the truth and progress of society as a whole."[7] The UN Human Rights Committee further expounded upon this transformation in its General Comment No. 34, noting that "[j]ournalism is a function shared by a wide range of actors, including professional full-time reporters and analysts, as well as bloggers and others who engage in forms of self-publication in print, on the internet or elsewhere."[8]

Permissible limitations of freedom of expression

[1] European Court of Human Rights (ECtHR), *Handyside v the UK,* App. no. 5493/72, para. 49, 7 December 1976.
[2] In Article 19 of the Universal Declaration on Human Rights 1948; and Article 19 of the ICCPR 1966.
[3] See UN Human Rights Committee, General Comment No. 34, adopted on July 2011. See also ARTICLE 19's call for the UN to adopt an international convention on the right of access to environmental information.
[4] See Human Rights Committee, *Mika Miha v. Equatorial Guinea,* Comm. No. 414/1990.
[5] See Human Rights Committee, *Ross v. Canada,* Comm. No. 736/97, adopted on 18 October 2000.
[6] See Human Rights Committee, *Shin v. Republic of Korea*, Comm. No. 926/2000, adopted on 16 March 2004.
[7] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (the 2011 Report of the SR on FOE), 16 May 2011, A/HRC/17/27, para 19.
[8] General Comment No 34, *op.cit*, para 44.

Limitations of the right to freedom of expression and information must satisfy a three-part test in order to be permissible under international human rights law: they must be provided by law; necessary to meet a legitimate objective, and they must be proportionate to that objective.[9] Paragraph (3) of Article 19 of the ICCPR stipulates that the only legitimate objectives towards which restrictions can be aimed are (a) for respect of the rights or reputations of others; or (b) for the protection of national security or of public order (ordre public), or of public health or morals.

The transformation of expression and information effected by the internet and digital technologies has necessarily transformed the nature of the scope and meaning of obligations owed by States, even as such obligations remain rooted in long-standing protections for the right to freedom of expression.[10] Restrictions on media publication and information distribution, and penalties which limit internet access or use take on new meaning when such restrictions affect potentially billions of individuals, and the proportionality of such measures must be determined on the basis of an accurate understanding of the nature of digital technologies, the interests and responsibilities of internet intermediaries, the potential for misuse and manipulation of technical restrictions of internet content, and the critical role played by free, secure and unimpeded internet access in facilitating the enjoyment of a range of other human rights.[11]

The rights to privacy and the protection of personal data

Whereas the concept of privacy might be difficult to concisely and objectively define, having many aspects, applications and cultural meanings, the right to privacy is comprehensively defined and enshrined in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights as the right to be free from unlawful or arbitrary interference with one's privacy, family, home or correspondence, and from unlawful attacks on one's reputation, and the right to enjoy the protection of the law against such interference or attacks.

At the regional level, the right to privacy is protected by the European Convention on Human Rights (Article 8), the European Union Charter of Fundamental Rights (Article 7) and the American Convention on Human Rights (Article 11).[12]

Permissible limitations on the right to privacy

While the European Court of Human Rights and some national jurisdictions have developed complex jurisprudence exploring the contours and confines of the right to privacy, until recently there existed few authoritative interpretations from international human rights mechanisms about the right.[13] The most authoritative of UN bodies charged with monitoring

---

[9] This test has been restated in numerous international human rights instruments, most notably in the Human Right Committee's General Comment No. 34, *op.cit.*

[10] For a thorough explanation of standards applicable to freedom of expression and ICTs, see ARTILCE 19, Freedom of expression and ICTs: Overview of international standards.

[11] The 2011 Report of the SR on FOE, *op.cit.*

[12] The African Charter of Human and Peoples' Rights does not contain a right to privacy. Interestingly, however, in 2014 the African Union adopted a Convention on Cybersecurity and the Protection of Personal Data.

[13] In 2013, the Special Rapporteur on the right to freedom of expression published a report on State surveillance of communications and privacy, ending an almost 25 year long silence on the part of UN human rights mechanisms as to the application of the right to privacy (since the publication of General Comment 16 on the right

State compliance with the right, the Human Rights Committee, issued its only General Comment on the right to privacy in 1989. In recent years, however, interpretation and application of the right to privacy and of its role in the "digital age," have developed, and understandings of the right have become more nuanced – and more contested. At issue, in particular, is the correct construction of what amounts to a permissible interference with the right to privacy. Nevertheless, a number of recent consecutive statements from international human rights mechanisms establish that, although Article 17 of the ICCPR does not specifically prescribe a test for permissible limitations on the right, the same tripartite test applies to privacy as it does to freedom of expression.[14] This tripartite test for limitations on Article 17 of the Covenant echoes the test under Article 19 ICCPR, and thus remains the basis upon which much of the jurisprudence on the right to privacy is developing.

The protection of personal data

The protection of personal information is another application of the right to privacy, and has recently emerged as a separate and complementary legal right and entitlement, as specifically recognised in Article 8 of the EU Charter of Fundamental Rights. From the 1970s onwards, the invention and public adoption of computers forced an expansion in understanding of what privacy rights are and how they can be infringed. Rather than simply the right to be let alone, privacy came to be considered as connected with, and essential to the protection of, information. In 1971 the German State of Hessen adopted the world's first "data protection" law, which sought to regulate the conditions under which public and private actors should handle individuals' personal information; the first national law was adopted in Sweden in 1972. In 1983 the German Constitutional Court issued a landmark decision on the collection of census data in which it argued for greater protection of personal information, nothing that the right to privacy

> [I]s endangered primarily by the fact that, contrary to former practice, there is no necessity for reaching back to manually compiled cardboard-files and documents, since data concerning the personal or material relations of a specific individual can be stored without any technical restraint with the help of automatic data processing, and can be retrieved any time within seconds, regardless of the distance. Furthermore, in case of

---

to privacy in 1989, which made no reference to the internet or digital technologies). The Special Rapporteur's report, along with the Snowden revelations, the first of which was published only days after the Special Rapporteur's report, triggered a series of other UN reports and resolutions on the issue of State surveillance of communications "in the digital age". These included a report by the High Commissioner for Human Rights on *The right to privacy in the digital age*, two General Assembly resolutions, a Human Rights Council resolution establishing a new special procedures mandate dedicated to the right to privacy, and Concluding Observations by the Human Rights Committee in its reviews of the Untied States and United Kingdom which addressed the use of particular digital surveillance techniques. Most recently, the Special Rapporteur on the right to freedom of expression published an entire report dedicated to encryption and anonymity, and their relationship with the rights to privacy and freedom of expression.

[14] In its Concluding Observations of its 2014 review of the USA's compliance with its obligations under Article 17 of the ICCPR, the Committee noted that interferences with the right to privacy must comply "with the principles of legality, necessity and proportionality"(CCPR/C/USA/CO/4, para 22) This sentiment echoed that of the UN Special Rapporteur on freedom of expression in his 2013 report on privacy and communications surveillance, who stated that "[t]he framework of article 17 of the ICCPR enables necessary, legitimate and proportionate restrictions to the right to privacy by means of permissible limitations", the test of which should be understood to be in the same terms as that applicable under Article 19, paragraph 3, despite Article 17 not containing such explicit language. The UN High Commissioner on Human Rights, in her 2014 report, The right to privacy in the digital age, confirmed the Special Rapporteur's interpretation, stating: "[...] authoritative sources point to the overarching principles of legality, necessity and proportionality..." (A/HRC/27/37, para 23).

> creating integrated information systems with other databases, data can be integrated into a partly or entirely complete picture of an individual, without the informed consent of the subject concerned, regarding the correctness and use of data.[15]

In 1980 the Organisation for Economic Cooperation and Development (OECD) issued Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the first international statement on the specific conditions under which personal information should be handled in order to ensure an individual's right to privacy is respected. These principles were reflected, for the large part, in the first internationally binding instrument on the protection of personal information, the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (known as Convention 108).[16] The Convention has been signed by all 48 Council of Europe members and ratified by all but Turkey; in addition, Uruguay ratified the Convention in 2013.

Subsequently, the creation of the European Union resulted in the EU Data Protection Directive 95/46/EC, passed in 1995. Today, there are more than 100 national data privacy laws around the world, nearly half of which are from outside Europe,[17] and many of which closely replicate European standards. The European Union recently modernized and adopted the General Data Protection Regulation ('GDPR'), which is set to provide yet another blueprint for the protection of personal data.[18]

The right to the protection of personal data is affected by all State and private sector generation, collection, publication, storage, retention and analysis of data. In today's digital era, personal data is handled for an expansive range of purposes, including the delivering of public services, the provision of corporate products, marketing and advertising, indexing and archiving, news reportage and journalistic endeavours, open government initiatives, and security and policing activities. In particular, internet and digital technologies have thrown up new challenges to the minimisation and control of personal information, and blurred the line between private personal information and that which is properly in the public domain, creating potential conflicts between the competing imperatives of protecting privacy and facilitating the free flow of information and expression.

Two recent decisions of the Court of Justice of the European Union have seen the right to the protection of personal data given unprecedented – and not uncontroversial – recognition. The decision of the CJEU in *Digital Rights Ireland,* pertaining to the mandatory retention of personal data by telecommunications operators, reaffirmed "the important role played by the protection of personal data in the light of the fundamental right to respect for private life" in invalidating the European Data Retention Directive.[19] Only weeks later, the CJEU issued its decision in the *Google Spain* case, finding Google Inc. to be a data controller for the purposes of the Data Protection Directive and extending the protections thereunder to individuals with respect to whom a search for their name will return search results. The Court found that the fundamental rights to privacy and to the protection of personal data are significantly affected

---

[15] BVerfGe 65, 1.
[16] The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981.
[17] Graham Greenleaf, Asian Data Privacy Laws (Oxford, Oxford University Press: 2014), 55. For details about each of the domestic frameworks, see BakerHostetler, 2015 International Compendium of Data Privacy Laws.
[18] The GDPR was adopted in April 2016 and will take effect after a two-year transition period, at which point it will replace the EU Data Protection Directive 95/46/ EC.
[19] Court of Justice of the European Union (CJEU), *Digital Rights Ireland v Ireland & Ors,* 8 April 2014, para 48.

> When the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him.[20]

The fact that the information at issue was public in nature (namely, proceedings against the applicant for the recovery of social security debts) was irrelevant to the scope of protection. Unlike traditional conceptions of privacy, data protection law is therefore not concerned with the question whether the data at issue is of a private nature but whether it is about a person. In other words, 'personal' data protects data, which may be both private or public. The protection of data protection law accrues when personal data is collected, [republished], catalogued, stored or in another way processed by a third party.

The application of data protection law to public information about a person can therefore raises significant challenges to the right to freedom of expression. This is especially the case when considering that data subjects have enforceable rights to rectify, erase or block information about them against both public and private actors. It is therefore vital to re-visit traditional balancing tests between freedom of expression and privacy, such as the "reasonable expectation of privacy" test, and determine how, if at all, it should be applied in the digital age.

The right to a reputation?

A third, more contested element, of the right to privacy which is relevant to the protection and promotion of the right to freedom of expression is the protection of a reputation. Reputation can be defined as the esteem in which one is held in society. Generally speaking, when someone's reputation is negatively impacted through false statements of fact, an issue of defamation will arise.

Both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights make explicit reference to the protection of reputation as a protected interest under Articles 12 and 17 respectively. It is therefore at least arguable that the right to privacy contains a right to honour and reputation. Article 17 of the ICCPR is not phrased in terms of an obligation to ensure individuals enjoy a positive reputation, however, but rather obliges States to ensure individuals are free from "attacks" on their reputation. Article 19 of the ICCPR, although not its UDHR equivalent, equally provides "respect of the rights or reputations of others" as a ground for which the restriction of the right to freedom of expression may be permissible, where in accordance with the law and necessary. The American Convention on Human Rights adopted similar language, with Article 11 enshrining the right to protection of unlawful attacks upon honour or reputation, and Article 13 echoing the permissible restrictions elaborated in Article 19 of the ICCPR.[21]

---

[20] CJEU, *Google Spain & Ors v Agencia Española de Protección de Datos & Ors*, Case C-131/12, judgment of 13 May 2014, para 80.

[21] Organization of American States (OAS), American Convention on Human Rights, "Pact of San Jose", Costa Rica, 22 November 1969.

The European Convention of Human Rights, however, departs from the construction adopted by the UDHR, ICCPR and ACHR, eschewing reference to attacks on honour and reputation in the right to privacy, enshrined in Article 8. The Travaux Preparatoires on Article 8 of the European Convention reveal that it was the view of the States parties that the phrase "unlawful attacks on his honour and reputation" sought to protect individuals not only from the actions of public authorities, but also from those of private persons. The concern was expressed that, to the extent that the inclusion of the phrase would expand the scope of the article from governmental action to the acts of private individuals, the article may require changes to legislation at the national level, particularly for countries with Anglo-Saxon traditions. An alternative viewpoint was offered, namely that the article merely enunciated general principles for which States would be responsible for putting into effect, but was disregarded.[22] Instead, the "protection of the reputation or rights of others" is listed as a legitimate objective for which the right to freedom of expression can be limited in Article 10(2) of the European Convention.

While the jurisprudence of the European Court on privacy and free expression could be said to have slightly different boundaries to that which we would have expected to develop in the Human Rights Committee – the protection of reputation only existing as a legitimate reason for restricting a Convention right, rather than a right in and of itself – the European Court has in fact inferred a right to protection of reputation into Article 8.

The Court first recognised a right to reputation in *Chauvy and Others v. France*.[23] However, the Court subsequently qualified its approach in *Karako v Hungary*,[24] asserting that the right to a reputation came into play only when a harm rises to the level at which it prejudices enjoyment of Article 8 rights. This was later confirmed in *Axel Springer v Germany*.[25] In that case, the Court further found that Article 8 could not be relied on in order to complain of a loss of reputation which is the foreseeable consequence of one's own actions such as, for example, the commission of a criminal offence. In subsequent cases the Court has not relied on the existence of a self-standing right to a reputation, but merely considered the claims within the context of the competing interests of Articles 8 and 10.[26]

While the application of the Court's approach is discussed further below, it should be noted that this is a developing area of jurisprudence around which absolute clarity still remains elusive.[27] There is currently no cross-jurisdictional consensus of the content of or threshold to engaging the right to a reputation, and the Human Rights Committee and other international human mechanisms have stayed silent on the question.

The development of a balancing test under international law

International human rights law does not prescribe an explicit test for balancing the protection of the right to freedom of expression, on the one hand, and the right to privacy on the other. Rather, both rights are considered equal in value and can be both limited to enable the

[22] European Commission for Human Rights, Travaux Preparatoires, 9 August 1956.
[23] ECtHR, *Chauvy and Others v. France*, App No. 64915/01, para 70, ECHR 2004-VI. See also, inter alia, ECtHR, *Pfeifer v. Austria*, App. no. 12556/03, para 35, ECHR 2007-XII.
[24] ECtHR, *Karako v Hungary,* App no. 39311/05, 28 April 2009, para. 23.
[25] ECtHR, *Axel Springer v Germany*, App no. 39954/08, [GC], 7 February 2012, para. 83.
[26] For example in *Couderc and Hachette Filipacchi Associes v France*
[27] Further resource materials are available here and here.

enjoyment and protection of the other, provided such limitations are in accordance with the articulated limits, namely that they are lawful, necessary and proportionate.

In recent years, the European Court of Human Rights has articulated a number of factors to take into consideration when balancing the rights to freedom of expression and privacy.[28] At the outset, however, it should be noted that this jurisprudence has primarily developed with respect to cases that (1) concern publication in the print or broadcast media; (2) have arisen in the context of adjudication of measures imposed by State courts in the context of violations of Article 8 (for example when State courts have imposed an injunction to prevent the publication of paparazzi photographs). As such, the Court's jurisprudence analyses the positive obligations of States to protect Article 8 by taking measures (including by remedying harms occasioned), rather than the State's negative obligations to ensure that public authorities don't act in a way that interferes with the right.[29]

The Court's approach to the balancing test can be further divided into two categories of cases: (1) the reporting on, and the publication of images of, public figures, and (2) that of non-public figures.

Public figures

A significant proportion of the case-law in the European Court relating to balancing privacy and free expression relates to actors, members of royal families or other celebrities and the publication of information about their personal indiscretions, such as affairs and criminal convictions, or the publication of paparazzi photographs of their personal lives. According to the Strasbourg Court, the relevant factors for striking the right balance between the rights to privacy and freedom of expression in these types of cases include:[30]

- **Contribution to a debate of public interest***:* in assessing the extent to which publication interfering with the Article 8 rights of a particular individual contributes to a debate of public interest, the Court will consider the importance of the question for the public and the nature of the information disclosed,[31] as well as assessing the publication as a whole and having regard to the context in which the article appears.[32] It will generally accord a narrow margin of appreciation to States taking measures to restrict freedom of expression when the public interest is at stake,[33] given the importance of free expression to public debate and participation. For free expression advocates, it is vital for the public interest to be interpreted broadly. For privacy advocates, however, this raises the concern that any information concerning public figures will inevitably fall within the public interest, rendering the protections of Article 8 meaningless for those in the public eye. The Court has previously found, for example, that publications concerning the personality traits of public figures are in the public interest.[34] At the same time, articles about the alleged

[28] The Inter-American Court of Human Rights has adopted a similar test, see *Fontevecchia y d'Amico v Argentina*, 29 November 2011.
[29] At [99].
[30] ECtHR. *Couderc and Hachette Filipacchi Associes v France,* [2015] ECHR 992 (10 November 2015) at [93]
[31] ECtHR, *Von Hannover (No. 2),* [109]
[32] ECtHR,*Tønsbergs Blad A.S. and Haukom v. Norway*, no. 510/04, § 87, 1 March 2007; Björk Eiðsdóttir v. Iceland, no. 46443/09, § 67, 10 July 2012; and *Erla Hlynsdóttir v. Iceland*, no. 43380/10, § 64, 10 July 2012
[33] *Éditions Plon v. France*, no. 58148/00, § 44, ECHR 2004-IV
[34] ECtHR, *Ojala and Etukeno Oy v. Finland*, no. 69939/10, §§54-55, 14 January 2014, and *Ruusunen v. Finland*, no.73579/10, §§ 49-50

extra-marital relationships of senior State officials which contributed only to the propagation of rumours did not justify the Article 8 intrusion,[35] nor did the publication of photographs showing the daily life of a princess who exercised no official functions.[36]

In *Couderc,* the Court held that "the public interest relates to matters which affect the public to such an extent that it may legitimately take an interest in them, which attract its attention or which concern it to a significant degree, especially in that they affect the well-being of citizens or the life of the community."[37] The ECtHR has clarified that it puts a higher value on information which would contribute to public debate rather than a lesser interest in merely providing to the public curiosity. In *Mosley v United Kingdom*,[38] the Court stressed that when assessing whether there is a public interest which justifies an interference with the respect for private life, the focus must be on whether the publication is in the interest of the public and not whether the public might be interested in reading it.[39]

- **The degree of notoriety of the person affected***:* because "[t]he extent to which an individual has a public profile or is well-known influences the protection that may be afforded to his or her private life",[40] the question of how notorious the person affected is will have a bearing on the balancing calculation between privacy and freedom of expression rights. The Court appears to have in mind a spectrum of notoriety, between wholly private persons at the one end, private persons acting in a public context in the middle, and "political figures or public figures" at the far end, with the latter phrase suggesting a connection with the performance of official functions of some description. Privacy interferences will be most justifiable with respect to politicians, who "inevitably and knowingly lay themselves open to close scrutiny of their every word and deed by both journalists and the public at large,"[41] as well as others who place themselves in the public sphere by their actions[42] or their position.[43]

  The exception to this rule arises where individuals have a "legitimate expectation of privacy";[44] although the Court's jurisprudence is unclear on in which situations such a legitimate expectation might arise, it has considered as relevant the following factors: whether photographs were obtained through fraudulent or clandestine operations (using telephoto lenses, for example)[45] or where the details published represented a particularly severe intrusion into intimacy.[46] For a further exploration of the concept of "legitimate expectation of privacy".

- **The subject of the report and nature of the information***:* these considerations are particularly relevant in cases in which reporting contains value judgments as opposed to

[35] ECtHR, *Standard Verlags GmbH v. Austria (no.2)*, no. 21277/05, § 52, 4 June 2009
[36] ECtHR, *Von Hannover (No. 1)* [65]
[37] ECtHR, *Couderc,* at [103], citations omitted.
[38] See ECtHR, Von Hannover no. 2 v Germany, nos. 40660/08 and 60641/08, [GC], 7 February 2012, para. 110
[39] ECtHR, *Mosley v The United Kingdom*, No.48009/08, 10 May 2011, at para. 114
[40] *Couderc,* at [117],
[41] *Couderc,* at [121], citing *Lingens v Austria* (1986) 8 EHRR 407
[42] *Krone Verlag GmbH & Co. KG*, *op.cit.*, para 37
[43] *Verlagsgruppe News GmbH v. Austria (no. 2)*, no. 10520/02, § 36, 14 December 2006
[44] *Von Hannover (No. 2)*, at [97].
[45] *Von Hannover (No. 1)*, at [68]
[46] ECtHR, *Campmany and Lopez Galiacho Perona v. Spain* (dec.), no. 54224/00, ECHR 2000-XII

factual statements, or where the media have not verified the accuracy of the third party allegations it is reporting. It is in respect of this question that the Court's approach to defamation cases has become conflated with the privacy-balancing test. Deriving absolute guidelines from the European Court in this context is therefore difficult. Generally, true statements may still engage the right to privacy, particularly when they call an individual's reputation into question.

In the context of news interviews, journalists should not be penalised for publishing or disseminating statements made by a third party in an interview unless there are strong reasons for doing so:[47] "A newspaper cannot be required to systematically verify the truth of every comment made by one politician about another in the context of a public political debate before publishing such comments".[48]

Even when the veracity of the information is not in question, the extent of the information may render the publication impermissible. In the recent ECtHR case of *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland,*[49] the Court endorsed the finding of the domestic court, which had been reliant on a finding of the Court of Justice of the European Union, that the publication of taxation data on 1.2 million Finish residents could not be considered as journalism but as processing of personal data, which the applicant companies had no right to do. This was despite the applicant companies having previously published the same amount, type and extent of data in 2002.

- **Prior conduct of the person concerned***:* with respect to the prior conduct of the person concerned, the Court held in *Axel Springer v Germany* that "Article 8 cannot be relied on in order to complain of a loss of reputation which is the foreseeable consequence of one's own actions such as, for example, the commission of a criminal offence".*[50]* By contrast, the mere fact of having cooperated with the press on previous occasions could not serve as an argument for depriving a person discussed in an article of all protection although it was nevertheless relevant. [51] For privacy advocates, this criterion is problematic particularly in circumstances where individuals do not always fully realize the extent of the consequences of sharing information about themselves online..

- **Method of obtaining the information***:* the question of how far journalists may go in order to perform their role as a "public watchdog" has received much attention in the past decade, fuelled in particular by the *News of the World* phone hacking scandal in the United Kingdom. Yet it was almost twenty years ago that the Parliamentary Assembly of the Council of Europe adopted Resolution 1165 (1998), in response to the tragic death of Diana, Princess of Wales, in which it noted that "the right to privacy afforded by Article 8 of the European Convention on Human Rights should not only protect an individual against interference by public authorities, but also against interference by private persons or institutions, including the mass media."[52] In *Von Hannover (No.1)*, the European Court criticised the media for the harassment levied upon public figures [68].

---

[47] ECtHR,*Roberts v. the United Kingdom*, no. 38681/08, 5 July 2011
[48] ECtHR, *Axel Springer (No. 2),* op.cit., para 70.
[49] ECtHR, *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland,* App. No. 931/13, 21 July 2015.
[50] *Axel Springer* v Germany, [GC], no. 39954/08, 07 February 2012, at [83].
[51] ECtHR, *Egeland and Hanseid v. Norway*, no. 34438/04, § 62, 16 April 2009
[52] More than 15 years ago ARTICLE 19 wrote a piece on of the difficulty in balancing privacy and free expression.

At the same time, the Court has also repeatedly reinforced the notion that the media should be free to choose the methods which they want to use to conduct their journalistic activities. The method of obtaining the information will normally fall within the realm of journalistic ethics and thus be immune from ex post scrutiny (to the extent that such immunity is necessary to preserve journalists' integrity and independence and support media self-regulation). However, the European Court is increasingly including an analysis of the "fairness of the means used to obtain information" and "the respect shown for the person" subject to the publication in its assessment.[53]

Thus, in the recent case of *Haldimann and Others v Switzerland,*[54] and with consideration to the absence of prohibitions in domestic law or national professional ethics standards, the Court held that the use of covert cameras to record an undercover journalist's interactions with an insurance broker, designed to expose the broker's unethical business practices, was a permissible interference with Article 8. However, the Court noted that the decisive point was that the applicants pixelated the broker's face and altered his voice. Accordingly, the interference with the broker's private life had not been serious enough to override the public interest in the information on alleged malpractice in the insurance industry.

The use of undercover techniques and recordings is rarely regulated, but may generally be said to fall within the ambit of data protection law, which generally provides an exception for journalistic activity. For example, Article 9 of the European Data Protection Directive requires Member States to provide for exemptions or derogations from the processing of personal data carried out solely for journalistic purposes. Nevertheless, as documented by the Media Legal Defence Initiative, a number of European states take an strict absolute approach towards the use of undercover recording techniques,[55] whereas others, such as Germany, France and Greece, provide for their responsible use.

- **Content, form and consequences of the impugned article***:* The content, form and consequences of the impugned article fall within the realm of responsibility accorded to journalists by virtue of their partaking in journalistic activity, and the Court purports to defer to the decisions of the media in this regard, and requires State courts to do the same. However, increasingly it is emphasising that journalistic freedom is not devoid of responsibilities. In *Couderc*, the Court declared:

> Wherever information bringing into play the private life of another person is in issue, journalists are required to take into account, in so far as possible, the impact of the information and pictures to be published prior to their dissemination. In particular, certain events relating to private and family life enjoy particularly attentive protection under Article 8 of the Convention and must therefore lead journalists to show prudence and caution when covering them.[56]

Canadian courts have also developed jurisprudence which takes into account the responsible actions of the journalists in reporting the material. In the case of *Grant v*

[53] *Couderc,* at [132]
[54] ECtHR, *Haldimann and Others v Switzerland* App. no. 21830/09, Judgement of 24 February 2015.
[55] Media Legal Defence Initiative, A Submission to the Euroepan Court of Human Rights in *Haldimann and others v Switzerland*, March 2011.
[56] *Couderc, op.cit.*, para 140.

Torstar Corp,[57] the Supreme Court of Canada, in finding that the current law with respect to statements that are reliable and important to public debate does not give adequate weight to the constitutional value of free expression, argued for the modification of the law of defamation to provide greater protection for communications on matters of public interest. The Court stated that:

> [T]he proposed change to the law should be viewed as a new defence, leaving the traditional defence of qualified privilege intact. To be protected by the defence of responsible communication, first, the publication must be on a matter of public interest. Second, the defendant must show that publication was responsible, in that he or she was diligent in trying to verify the allegation(s), having regard to all the relevant circumstances.[58]

In demonstrating responsible conduct, the Court said,

> [T]he following factors may aid in determining whether a defamatory communication on a matter of public interest was responsibly made: (a) the seriousness of the allegation; (b) the public importance of the matter; (c) the urgency of the matter; (d) the status and reliability of the source; (e) whether the plaintiff's side of the story was sought and accurately reported; (f) whether the inclusion of the defamatory statement was justifiable; (g) whether the defamatory statement's public interest lay in the fact that it was made rather than its truth ("reportage"); and (h) any other relevant circumstances.[59]

- **The circumstances in which a photograph was taken***:* The publication of images triggers particular scrutiny by the Court, which takes into consideration whether photographs were taken without the consent or knowledge of the individual pictured, whether they place the individual in a negative light, whether they present a distorted image of them, and whether they lend support to the content of the publication.[60] The Court has noted that for a private individual, the intrusion effected by the publication of an image may be even more serious than that occasioned through a written article.[61]

  The covert taking of photographs will not always support a conclusion that the photos were taken in circumstances unfavourable to the individuals in question. In *Von Hannover v Germany (No. 2)*, for example, the Court gave consideration to the fact that "photos appearing in the "sensationalist" press or in "romance" magazines (…) are often taken in a climate of continual harassment which may induce in the person concerned a very strong sense of intrusion into their private life or even of persecution."[62] In more recent decisions, the Court has supported the decisions of journalists to publish the material, and to use covert means to obtain it;[63] nevertheless, this could indicate a concerning change in approach.

- **Sanctions***:* The proportionality of the sanctions levied in response to Article 8 interference will be relevant to an assessment of whether Article 10 interest outweigh the privacy

---

[57] Supreme Court of Canada, *Grant v Torstar Corp*, [2009] 3 SCR 640, 2009 SCC 61 (CanLII)
[58] *Ibid.,* para 95, 98]-[99.
[59] *Ibid.,* para 110, 126-128.
[60] *Couderc,* at [135]
[61] *Von Hannover v Germany (No. 2),* GC], nos 40660/08 and 60641/08, 07 February 2012 at [113]
[62] *Von Hannover v Germany (No. 2),* [at [103]
[63] *Haldiman & Ors v Switzerland, op.cit.*.

concerns. In this regard, the Court in *Couderc* noted that the costs to freedom of expression as a result of sanctions, even minor ones, can be high, stating "any undue restriction on freedom of expression effectively entails a risk of obstructing or paralyzing future media coverage of similar questions."[64]

Non-public figures

Reporting by formal media on the personal lives of non-public figures overwhelmingly happens in the context of court proceedings, either with respect to the levying and determination of criminal charges, or civil litigation suits. In these circumstances, the balance between the privacy rights of the individual subject to reporting, on the one hand, and the right of the media to publish information about the proceedings (and of the public to receive that information), on the other, is struck in a context of recognition of the vital role that the media plays in reporting on court proceedings, including contemporaneous reporting of the subject matter of criminal trials, having regard to fair trial rights and the defendant's right to the presumption of innocence.

- **Suspects and defendants***:* in the context of reporting on court proceedings, freedom of expression and information claims will generally take precedence over applications for measures aimed at the protection of privacy, such as prior restraint, anonymity orders, and the exclusion of press from hearings. The right of the public to know of the identity of a defendant pleading guilty to the possession of indecent images of children, for example, will take precedence over the protection of the privacy of the defendant's children, as the UK High Court held in *R. v. Croydon Crown Court, ex parte Trinity Mirro*r.[65] In that case, the Court was of the opinion that "it is impossible to over-emphasise the importance to be attached to the ability of the media to report criminal trials. In simple terms this represents the embodiment of the principle of open justice in a free country."[66] The UK courts have also favoured the importance of public hearings in supporting open justice and the public's right to access information over the Article 8 rights of parties to and witnesses in a civil case.[67]"[i]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[68]

  At the same time, special regard is often given to the more privacy-intrusive nature of publication of *images*, as distinct from written articles, of non-public figures involved in court proceedings. In *Sciacca v. Italy,* the Strasbourg Court found that the publication of a photograph of a suspect, whose photo had been taken by the authorities in the course of their investigation and given to the press, was a violation of Article 8, particularly given that the case involved an "ordinary person," not a public figure or politician. The fact that the applicant was the subject of criminal proceedings did not curtail the scope of the protection..[69]

---

[64] *Couderc*, at [151].
[65] UK High Court held in *R. v. Croydon Crown Court, ex parte Trinity Mirro*r, [2008] 3 WLR 51
[66] *Ibid.*
[67] *Global Torch Ltd v Apex Global Management Ltd* [2013] EWCA Civ 819, [2013] 1 WLR 2993.
[68] Smith v. Daily Mail (443 U.S. 97 (1979))
[69] App. no. 50774/99, 11 January 2015.

In France, the courts take the approach that if the Article 8 interference is mitigated through the imposition of anonymisation measures, the publication is justifiable. In a decision of 31 August 2015, the Paris Court of Appeal, considering the publication of film of a suspect's arrest and handcuffing in a documentary about terrorism and applying the criteria, concluded that the publication contributed to a debate of general interest. However, measures were taken to preserve the privacy rights of the individual – the comments made were general and a hood covered his face.

Similarly, although there is no law prohibiting the disclosure by police of video footage and photographs of crime suspects in China, there is an emerging recognition of the privacy rights of crime suspects.

- **Victims***:* with respect to the publication of images of victims, the ECtHR considers the Article 8 rights of the victim's family,[70] noting that

> Certain events in the life of a family must be given particularly careful protection. The death of a close relative and the ensuing mourning are a source of intense grief and must sometimes lead the authorities to take the necessary measures to ensure that the private and family lives of the persons concerned are respected.[71]

Thus, in *Hachette Filipacchi Asocies v France,* a sanction in the form of an order to publish a statement regarding the prior publication of a photograph of a victim of a terrorist attack was not a disproportionate interference with the media's Article 10 rights. The European Court has also held that the publication of images of a child involved in a custody dispute, along with personal and intimate information about him, warranted the imposition of sanctions on the respective media outlets.[72]

In China**,** it is generally acknowledged that the privacy rights of victims should be protected, particularly when the crime involves children or crime which would do "reputational damage" to the victim such as rape.[73]

- **Witnesses***:* a photograph of a witness placed on the premises of several police stations but not published or disseminated through mass media was also found to be a violation of the individual's Article 8 rights, and, having special regard to the context in which the photograph was disseminated (in connection with a crime), was defamatory. The witness's "status as an "ordinary person" excluded the possibility of curtailing the scope of his private life in favour of any legitimate aim protected by the Convention."[74] However, these cases precede the development of the criteria in *Von Hannover (No. 2)/Axel Springer.*

- **Deceased:** the US courts also have regard to the privacy rights and interests of a deceased person's family when deciding cases at which the publication or dissemination of an image of that person is in issue. For example, the case of *National Archives and*

---

[70] The Article 8 rights of the deceased person are outside the scope of this paper, but for further reading begin with this Amicus brief filed recently in the Constitutional Court of Georgia by the Venice Commission.
[71] ECtHR, *Hachette Filipacchi Asocies v France,* App. No 71111/01) 14 June 2007, para 46.
[72] ECtHR, *Kurier Zeitungsverlag und Druckerei GmbH (no. 2) v. Austria*[72] and *Krone Verlag GmbH v. Austria*, App no. 27306/07, 19 June 2012.
[73] Research memo, China.
[74] ECtHR, *Giorgi Nikolaishvili v Georgia,* App. 37048/04, 13 January 2009, at [123]

> *Records Administration v. Favish*[75] involved the scope of an exemption from the Freedom of Information Act and the dispute over death-scene photographs of Vincent Foster, an aide to former President Bill Clinton. The Supreme Court reasoned that "[b]urial rites or their counterparts have been respected in almost all civilizations from time immemorial" and "[f]amily members have a personal stake in honoring and mourning their dead and objecting to unwarranted public exploitation that, by intruding upon their own grief, tends to degrade the rites and respect they seek to accord to the deceased person who was once their own."[76]

The role of reasonable expectation of privacy

The concept of reasonable expectation does not arise in international human rights texts, nor has it played a role in respect of human rights-based jurisprudence regarding State interferences with the right to privacy (the existence or not of a reasonable expectation of privacy is immaterial to determinations of whether State communications surveillance was lawful, for example). However, it has been used by the European Court of Human Rights in relation to media reporting on public figures, and forms a critical part of the test applied by the British courts in respect of private intrusions into privacy.[77]

In contrast, in the United States, the concept of reasonable expectation is applied to all searches and seizures which engage the Fourth Amendment to the US Constitution, including those conducted by the Sate. Thus, under US law, individuals have no right to privacy *vis a vis* information they voluntarily hand over to third parties, because they have no reasonable expectation of privacy with respect to such information.[78] However, it should be noted that there is a line of authority for the proposition that the "third party doctrine" should be rethought in the digital era. The remarks of Justice Sotomayor in her separate but concurring opinion in *United States v Jones*[79] are apposite:

> [..] it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. E.g., Smith, 442 U. S., at 742; United States v. Miller, 425 U. S. 435, 443 (1976). This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," post, at 10, and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.

---

[75] *United States v Jones,* 124 S.Ct. 1570 (2004)
[76] *Ibid.*
[77] *Campbell v MGN* [2004] UKHL 22
[78] *Katz v. United States*, 389 U.S. 347 (1967), *Smith v. Maryland*, 442 U.S. 735 (1979).
[79] United States v. Jones, 132 S. Ct. 945, 565 U.S. ___ (2012)

Under English law, and to an extent European human rights law, the existence of a reasonable expectation is a relevant consideration in circumstances in which a publication is in breach of a person's privacy rights. The UK House of Lords decision in *Campbell v MGN Ltd*[80] establishes that a two stage test should be applied in these cases, as part of which first stage is to ask "whether in respect of the disclosed facts the person in question had a reasonable expectation of privacy". The European Court takes less of a binary approach, considering the existence of a "legitimate expectation" as one factor among many to determine whether the interference engaged the rights under Article 8.[81]

It remains unclear to what extent the "reasonable expectation" test forms part of international human rights law with respect to privacy infringements by public and private actors. From a privacy perspective, the changing nature of information and communication may give rise to an impetus to redefine "reasonable expectation" or diminish its centrality (where relevant) to considerations of the existence or not of claims to privacy. Arguably, the perspective of data protection law is that individuals have an expectation of privacy in every piece of personal information about them, which information must be treated in a particular manner. By contrast, from a freedom of expression perspective, the "reasonable expectation of privacy" test continues to be an important yardstick by which courts can judge the appropriateness of *publication* of information about an individual in the print or broadcast media or on the Internet.

[80] *Campbell v MGN Ltd* [2004] UKHL 22, [2004] 2 AC 457
[81] *Von Hannover (no. 2)*at [97].

Privacy as a condition to free expression

On Saturday, 20 July 2013, technicians from the Government Communications Headquarters, Britain's electronic surveillance agency, visited the offices of *The Guardian*, a prominent British newspaper which had recently published the first of many articles detailing the British government's extensive surveillance activities, including the mass interception of millions upon millions of private communications, on the basis of documents leaked by NSA whistleblower Edward Snowden. The GCHQ agents, on orders from the British Prime Minister David Cameron, ordered *The Guardian* journalists to physically destroy hard drives, laptops and memory cards containing the Snowden documents, in order to prevent their publication, the exposure of British surveillance efforts to the public scrutiny of people the world around, and the potential resulting technical impediments to such surveillance that would stem from individuals deploying greater security to circumvent interception capabilities.

This incident was illustrative of the interdependence of the rights to privacy and freedom of expression in the context of surveillance, particularly digital surveillance: the actions of the GCHQ agents certainly amounted to an interference with the right of *The Guardian* journalists to publish the documents and use them as a basis to critique the actions of the British security services, and the right of the British public to access information about the government's unlawful activities. The right to privacy was equally implicated by these outrageous actions; not only the privacy of *The Guardian*'s journalists and their sources, but the privacy of the millions upon millions whose communications had been unlawfully intercepted by GCHQ, and who had a right to be informed of – and seek redress for – such unlawful acts. In the balance also hung the rights of whistleblower Edward Snowden to disclose information about unlawful State interferences, and the rights of every person whose fear of State monitoring and surveillance deters them from freely and confidently using the internet.

The Snowden revelations related to, for the most part, mass surveillance – the bulk interception, storage and analysis of internet communications – which presents an equal threat to the rights to both privacy and free expression. Yet many other forms of State monitoring, interception, data collection and retention, and search and seizure of information present dual dangers to these two interlinked rights. In this section we canvass those threats, particularly as they emanate from the State, that establish privacy as a necessary pre-condition to the free and full exercise and enjoyment of the right to freedom of expression and information. We also analyse measures which explicitly undermine the work of journalists and media to report on privacy violations, particularly in the realm of national security.

Mass surveillance of digital communications

States have long possessed the power to intercept and monitor them, whether under the guise of censorship offices established in Britain and the United States during the First and Second World Wars to monitor postal mail, or by using crocodile clips to tap the wires carrying the earliest phone calls. Human rights law evolved to understand the act of communicating as primarily protected by the right to privacy, in particular the right to privacy of correspondence, and extended protections against unlawful or arbitrary surveillance of such correspondence. Where accompanied by appropriate legal and procedural safeguards, targeted interception of an individual's communications is a legitimate act of a democratic government, which can be necessary to prevent crime and disorder and protect national security.

In general, the interception of correspondence tends to be regarded as an interference with the right to privacy rather than the right to freedom of expression. The one exception to this is where interception or other forms of surveillance (including search and seizure) are levied at members of the media as a means of ascertaining information about journalistic sources. The protection of journalistic sources is a fundamental tenet of the right to freedom of expression, and enjoys additional protection under a range of regional and international instruments.[82] In 2000, the Council of Europe's Committee of Ministers recommended that interception or surveillance of communications should not be applied if their purpose is to circumvent the right of journalists, under the terms of these principles, not to disclose information identifying a source".[83] In its decision in *Sanoma Uitgevers B.V v The Netherlands*,[84] the European Court of Human Rights held that any interference with Article 10 rights in the context of identification of journalists' sources must be subject to prior independent authorisation:

> Given the vital importance to press freedom of the protection of journalistic sources and of information that could lead to their identification any interference with the right to protection of such sources must be attended with legal procedural safeguards commensurate with the importance of the principle at stake[...] First and foremost among these safeguards is the guarantee of review by a judge or other independent and impartial decision-making body.[85]

In the digital age, however, our traditional understandings of what constitutes a communication and 'communications surveillance' are changing. With the advent of the Internet, communications have been completely transformed in form – letters, phone calls and radio transmissions have been replaced by emails, text messages, Voice-over-Internet Protocol (VoIP) calls, tweets, Facebook posts, blogs, snapchats, in-app communications on platforms such as Tinder, Grindr and Happen; forums, online gaming, e-commerce purchases, and search engines. The scope, speed and reach of communications are greater by exponential factors, and they continue to radically increase in number every day as millions upon millions more people get connected to the internet. The definition of the act of communicating has been altered – we now communicate not only with other individuals or with our local community, but with the world at large, with our devices, with cell towers, with foreign-based internet platforms and servers, with the Cloud. We can communicate in languages we do not speak, as well as in photos and pictures, emojis and gifs, and using the most advanced cryptography the world has ever known. Simply by using a device we are transmitting – communicating – private data about ourselves, our location and our correspondence to untold entities.

Mass communications surveillance is effected by the placement of mirrors or prisms on undersea fibre optic cables, which carry the bulk of the world's daily digital communications. These mirrors create a copy or "buffer" of all data flowing through the cables; at the point at which the buffer exists, an intercepting State can interrogate the data and decide which parts of the copy it should keep and which parts it should discard. This initial filtering is generally used to dispose of the huge percentage of global internet traffic that is comprised of peer-to-

82 Resolution on Journalistic Freedoms and Human Rights, adopted at the 4th European Ministerial Conference on Mass Media Policy (Prague, 7-8 December 1994); Resolution on the Confidentiality of Journalists' Sources by the European Parliament (18 January 1994, Official Journal of the European Communities No. C 44/34).
83 Council of Europe, Committee of Ministers recommendation No. R (2000) 7, principle 6 (a).
84 ECtHR, *Sanoma Uitgevers B.V v The Netherlands*, App. No. 38224/03.
85 *Ibid.,* para 88.

peer sharing of videos and music. The remaining data is sent to a second stage filter, in which it is compared against selectors. It is expected that, depending on the State and the programme, such selectors number in the tens, if not hundreds of thousands (the NSA provided the German intelligence agency with 800,000 selectors for use in its mass surveillance programme, for example)[86], and may range from the broad (particular words or countries of origin) to the narrow (particular IP addresses). The processing for interrogating results returned against the selector stage differs from State to State, but generally some protections are made available to nationals or residents of the interrogating State.

Mass surveillance capabilities form a key part of American and British surveillance apparatuses, as well as those of Australia, New Zealand, Canada, Germany, France, Switzerland, Sweden, the Netherlands and Denmark. Mass interception systems can also be purchased on the private market; French companies Qosmos and Amesys famously sold such technology to Gaddafi's Libya.[87] That mass surveillance measures are in place is not avowed by most countries (Britain recently introduced legislation containing powers to commit "bulk interception" with the caveat that "this is not mass surveillance"), nor is it necessarily provided for in domestic statutes, although a recent spate of legislative reform across Europe threatens to provide ostensible legal cover for such activities.

A number of recent cases have recently demonstrated the clear impact of mass surveillance in chilling the freedom of expression of journalists, political figures and non-governmental organisations. In the case of *Liberty & Ors v GCHQ,*[88] *Britain's* Investigatory Powers Tribunal, a specially constituted court charged with arbitrating complaints against the intelligence and police services, considered a challenge brought by British NGOs Liberty, Privacy International and Amnesty International, as well as a number of international NGOs, to Britain's mass surveillance practices. The Tribunal found that Amnesty International and South Africa's Legal Resource Centre had both been the subject of unlawful interception under Britain's mass surveillance programme. The Tribunal has also heard claims from lawyers[89] and Members of Parliament[90] in cases concerning the inability of mass surveillance programmes to respect the confidentiality of those entitled to communicate with professional privilege.

The ECtHR is currently considering parallel applications in *Big Brother Watch, English PEN and Open Rights Group v UK,* and *The Bureau of Investigative Journalism v UK*, in which the chilling effect of mass surveillance measures on journalists, and particularly the protection of journalistic sources, will be considered.

There is a strong rationale for considering mass surveillance to be a violation not only of rights to freedom of expression enjoyed by journalists and their sources, but also more generally the rights of all internet users, whose free and confident use of the internet to communicate is chilled by the mass State monitoring of such communications. The ECtHR in *Weber and Saravia v Germany*[91] and the Investigatory Powers Tribunal in *Liberty* looked only at the former question. In *Weber*, in which one of the applicants was a journalist, the Court noted that strategic monitoring powers were

[86] Zeit, BND helped NSA in monitoring European politicians, 23 April 2015.
[87] FIDH, Amesys and Qosmos targeted by the judiciary: is there a new law on the horizon?, 18 June 2013.
[88] *Liberty & Ors v GCHQ,* [2014] UKIPTrib 13_77-H (5 December 2014)
[89] ECtHR, *Belhadj & Ors v Security Service & Ors,* 2014] UKIPTrib 13_132-H
[90] ECtHR, *Lucas & Ors v Security Service & Ors* [2015] UKIPTrib 14_79-CH
[91] ECtHR, *Weber and Saravia v Germany*, App. No. 54934/00, 29 June 2006.

> Not aimed at monitoring journalists; generally the authorities would know only when examining the intercepted telecommunications, if at all, that a journalist's conversation had been monitored. Surveillance measures were, in particular, not directed at uncovering journalistic sources.[92]

They concluded, that "[t]he interference with freedom of expression by means of strategic monitoring cannot, therefore, be characterised as particularly serious," and could be cured by the strong safeguards in place. Such a finding clearly does not take into account the severe chilling effects of such powers, and the prospects for abuse of mass surveillance systems.

The Tribunal in *Liberty* was similarly unpersuaded about the need for exceptional measures to be taken to protect Article 10 rights in the context of mass surveillance. In that case, the claimants argued that Article 10 was equally engaged by the mass surveillance system carried by the UK, to the extent that the NGOs party to the case performed a journalistic function deserving of particular protections under Article 10, namely the protection of prior independent authorisation of any State seizure or interception of communications. The Tribunal found that such prior judicial notification is infeasible in a mass surveillance system.[93]

The case will be heard by Strasbourg alongside that brought by the Bureau of Investigative Journalism, which also made Article 10 claims. In addition, a further case has been filed, in October 2015, by the French Association de la Press Judiciaire. This application arises out of the French Intelligence law (Law No. 2015-912) adopted by the French Parliament on 24 July 2015 which, inter alia, extended the bulk collection and other surveillance powers of the French intelligence and security agencies. The APJ contends that the law infringes the rights and freedoms of journalists, and imperils the protection of sources, contravening Article 10 of the Convention. There are also a number of pending US cases in which claimants have invoked First, as well as Fourth, Amendment arguments in the context of mass surveillance programmes operated by the NSA.[94] It is unclear whether any of these cases will grapple with the wider free expression implications of mass surveillance, or whether they will simply confront the impact of mass surveillance programmes on journalistic activity.

Mandatory data retention and bulk data disclosure

The imposition of mandatory requirements on communications service providers (CSPs) to retain and provide access to communications data – the information about our communications, rather than their content – is a relatively new State surveillance tool, having really only emerged in the aftermath of September 2001. In the United States, section 215 of the Patriot Act 2001, authorised the NSA to obtain, on a bulk scale, the telephone metadata records held by all CSPs. In Europe, the European Data Retention Directive of 2006 placed the obligation on the CSPs to retain the records, which were then available for access and

---

[92] At [151].

[93] "In the context of the untargeted monitoring by s.8(4) warrant, it is clearly impossible to anticipate a judicial pre-authorisation prior to the warrant limited to what might turn out to impact upon Article 10. The only situation in which it might arise would be in the event that in the course of examination of the contents, some question of journalistic confidence might arise. There is, however, express provision in the Code (at paragraph 3.11), to which we have already referred, in relation to treatment of such material." [151]

[94] See, for example, *Wikimedia v NSA* filed in May 2015: the plaintiffs' complaint is available at https://www.aclu.org/legal-document/wikimedia-v-nsa-complaint.

analysis by State authorities. Numerous other countries have attempted to enact data retention regimes but have been thwarted by public or judicial opposition, including Philippines and Paraguay. Australia, however, implemented mandatory two-year data retention laws in 2015.

Although bulk data retention and access powers are relatively new, they grow out of historical preconceptions of metadata as a less revealing, privacy-intrusive, form of personal information, therefore deserving of lower levels of privacy protection. However, digital technologies and the internet have fundamentally altered these historical realities. Given the constant and considerable amount of metadata every single person with a smartphone or internet connection generates – data which includes an individual's location, with whom and when they're communicating, and with which device and IP address – metadata can now be used to paint an entire picture of an individual's life. It reveals relationships, movements, connections, patterns of behaviour, even political or religious affiliations, and its retention and analysis jeopardises individuals' efforts to remain anonymous online. It is of great interest to intelligence and law enforcement authorities, a fact no more vividly illustrated than by NSA General Counsel Stewart Baker's statement that "we kill people based on metadata". Britain's Intelligence and Security Committee, in an inquiry into the use of surveillance capabilities revealed by NSA whistleblower Edward Snowden, noted that the primary value of Britain's bulk interception programmes is the bulk metadata that is derived from the intercepted content.[95]

Historically, scant judicial or legislative recognition had been given to the fact that the acquisition, retention and storage of metadata is indeed a serious interference with the right to privacy. Yet a number of recent cases in the United States, Canada, United Kingdom and the Court of Justice of the European Union have challenged the casting of metadata as deserving of lower levels of protection under the right to privacy, and have also connected data retention with anonymity and free expression.

In the seminal CJEU case of *Digital Rights Ireland v Irelands & Ors*, concerning the validity of the Data Retention Directive 2006/24/EC, which empowered EU Member States to mandate the generation and retention of communications data for the purpose of preventing, detecting, investigating and prosecuting serious crimes, the Grand Chamber noted the dangers of collecting and using personal data in bulk, and concluded that the Directive "entails an interference with the fundamental rights of practically the entire European population".[96]

The invalidation of the Data Retention Directive put in doubt the legal basis in EU Member States for requiring the retention of communications data. Various EU Member States abandoned data retention powers, while others re-legislated for them. The United Kingdom enacted the Data Retention and Investigatory Powers Act 2014 (DRIPA), emergency legislation granting the Home Secretary authority to issue orders to communications service providers concerning the mandatory retention of communications data. The UK High Court, in considering an application for judicial review of DRIPA, concluded it did not comply with the decision in *Digital Rights Ireland.* It paid particular attention to the access regime applicable to retained data, finding that DRIPA failed to provide necessary safeguards in the form of prior independent authorisation for access to retained data.[97]

---

[95] ISC, *Privacy and security: a modern and transparent framework*, para 80.
[96] *Digital Rights Ireland v Ireland & Ors, op.cit.*, para 56.
[97] At [98].

The *Digital Rights Ireland* decision was closely followed by a decision of the Canadian Supreme Court in *R v Spencer,*[98] which concerned police access to information on the identify of the user of an IP address used to access or download child pornography. The Court found that police required a warrant before seeking access to "subscriber information", metadata pertaining to the user of a particular account or IP address. In issuing its decision, the Court considered that informational privacy had three aspects: privacy as secrecy, privacy as control, and privacy as anonymity. The latter aspect was particularly relevant in the context of access to metadata:

> The user cannot fully control or even necessarily be aware of who may observe a pattern of online activity, but by remaining anonymous – by guarding the link between the information and the identity of the person to whom it relates – the user can in large measure be assured that the activity remains private.[99]

In *ACLU v Clapper* (May 2015),[100] the US Court of Appeals ruled that the NSA's "bulk telephone records programme", by which the intelligence agency accessed all metadata records held by telecommunications providers on a rolling basis under the purported authority of section 215 of the Patriot Act, exceeded the statutory power and was thus unlawful. In making the decision, the Court of Appeals noted the exceptional value of metadata to law enforcement and intelligence authorities, distinguishing metadata from the content of communications but concluding that just because "telephone metadata do not directly reveal the content of telephone calls, however, does not vitiate the privacy concerns arising out of the government's bulk collection of such data."[101]

A more recent court decision pertaining to the §215 programme went so far as to find that the programme violated a reasonable expectation of privacy and was thus a search under the Fourth Amendment. In *Klayman v Obama*,[102] the District Court concluded:

> The fact remains that the indiscriminate, daily bulk collection, long-term retention and analysis of telephony metadata almost certainly violates a person's reasonable expectation of privacy" (*citations omitted).*[103]

---

[98] Supreme Court of Canada, *R v Spencer,* [2014] 2 SCR 212.
[99] *Ibid.,* para 46.
[100] US Court of Appeals for the 2nd Circuit, *ACLU v Clapper*, May 2015.
[101] *Ibid.*, p. 8.
[102] In the initial decision in *Klayman,* in December 2013, the court of first instance, the District Court, found that the bulk collection of telephony metadata violated a reasonable expectation of privacy and was thus a search under the Fourth Amendment. The court went on to find that the warrantless bulk collection of call detail records was unreasonable and likely violated the Fourth Amendment, and thus acceded to Klayman's motion for a preliminary injunction barring the government from continuing the §215 programme, staying its order pending appeal. This decision was vacated in August 2015 by the US Court of Appeals for the District of Colombia, finding that the claimant did not possess standing to challenge the bulk records collection programme because the government had consistently maintained that its collection was did not encompass all, or virtually all, call records, and in any event the claimant's evidence related to the disclosure of Verizon's *Business Network Services'* records, while the claimant himself was a customer of Verizon *Wireless* services. The case was remanded to the District Court, which on 9 November 2015 issued another decision again finding the §215 programme unconstitutional and again issuing an injunction preventing the government from proceeding with the programme. The Court of Appeals for the District of Colombia has stayed the injunction pending appeal; with the §215 programme expiring on 29 November, it is likely that this matter will be resolved expeditiously.
[103] District Court, *Klayman v Obama*, 9 November 2015, p. 26.

The §215 programme is also subject to challenge from the perspective of free expression and association rights; in *First Unitarian v NSA*, filed in September 2013, the claimants, associations working on a range of social and religious issues, challenged §215 on First Amendment, rather than Fourth Amendment, grounds. The challenge is based on the seminal case of *NAACP v Alabama*, where the Supreme Court prohibited Alabama from obtaining NAACP membership records, recognizing that to do so would infringe on the First Amendment rights of the NAACP and it members to associate anonymously. The case has been languishing in the District Court since 2013, as the parties have awaited a trial date. Although the passage of USA FREEDOM may ultimately frustrate their claim going forward, they will proceed with claims for damages for past harm.

Mandatory data retention and bulk data acquisition programmes raise similar concerns as mass surveillance of content for the right to freedom of expression and information, both in a general sense, negating individuals' ability to confidently communicate anonymously, and with respect to the protection of journalists' sources. A report by the UK's Interception of Communications Commissioner released in February 2015 showed that in the UK, for example, police forces made more than 600 applications to access communications data for the purpose of uncovering journalists sources in a three year period.[104] In an attempt to address this issue, the UK government adopted in March 2015 Codes of practice for the retention, acquisition and disclosure of communications data, introducing, inter alia, a requirement that police apply to a court for a production order to obtain communications data which is sought to identify a journalist's source.[105]

Trans-border data flows

Both law enforcement and national security agencies on the one hand, and the private sector on the other, significantly interfere with the rights to privacy and data protection by collecting and using data accessible through trans-border data flows. These data flows are considered vital to the digital economy and the (unlawful) 'mass surveillance' practices of some States.

Important gaps in the protection of privacy and personal data arise, however, as data protection and privacy laws may vary from jurisdiction to jurisdiction regardless of the basic principles set out by the international instruments described above.

A number of different mechanisms have been put in place in an attempt at reconciling the discrepancies between legal systems but lawmakers are yet to find a sustainable solution.

Companies rely on different data transfer schemes including Model Contract Clauses and Binding Corporate Rules to transfer data for commercial use. The most well-known example for allowing commercial data flows between the European Union and the United States was the Safe Harbor adequacy decision of the European Commission. Safe Harbor was an industry-developed self-regulatory approach to privacy. Coordinated by the Department of Commerce, the Safe Harbor program allowed U.S. companies to self-certify privacy policies in lieu of complying with legal requirements for the processing of data of Europeans.

---

[104] IOCCO inquiry into the use of Chapter 2 of Part 1 of the Regulation of Investigatory Powers Act (RIPA) to identify journalistic sources, 4 February 2015.
[105] Code of Practice on the acquisition and disclosure of communications data, March 2015, para 3.78.

The Court of Justice of the European Union invalidated the Safe Harbor in the *Schrems* decision on the basis that it did not comply with the requirements set out in EU data protection law, read in light of the EU Charter of Fundamental Rights. At the center of the EU legal framework for the transfer of personal data from the EU to a third country, such as the US, is the notion of 'adequacy' in terms of the level of data protection provided in the third country in question. For the Court, 'adequacy' means that the third country must ensure, through its domestic legal order or international commitments, a level of protection which is essentially equivalent to that guaranteed within the EU.

The Department of Commerce and the European Commission released the proposed Privacy Shield to replace Safe Harbor to allow transatlantic data flows to continue on February 29, 2016. The proposed framework, however, does not meet the criteria set out by EU law and it is expected to fail under future legal scrutiny if the European Commission adopts it as an adequacy decision. Therefore, the current compromise cannot serve as a sustainable solution that guarantees privacy protection and legal certainty for the benefit of individuals and businesses alike.

Data transfers are also sometimes governed by international trade agreements. While the analysis of this phenomenon is beyond the scope of this paper, there is an alarming tendency to restrict fundamental rights in trade agreements.

At any rate, it is clear that for the exercise of the right to freedom of expression to be meaningful, it is essential that privacy and personal data protection be strongly protected, including in legal agreements for data flows. Individuals whose data is travelling between countries, government agencies, and companies should have the same level of protection everywhere in accordance with international human rights standards.

Restrictions on encryption

Encryption tools and services ensure that only the intended recipient is able to read, listen to or watch the communication that was transmitted to them. Encryption thus protects the privacy and security of the communications transmitted through those tools and services, and promotes the confident and free expression and dissemination of information and ideas. The confidence to communicate our ideas and opinions, however controversial, is underpinned by the knowledge that we are protected from any unlawful interference with those communications by those we might wish to conceal them from.

There now exists ample authority to support the contention that access to and use of encryption is an essential pre-condition to the realisation of both the right to privacy and the right to freedom of expression on the internet, providing "individuals and groups with a zone of privacy online to hold opinions and exercise freedom of expression without arbitrary and unlawful interference or attacks".[106] Interference with encryption is an interference with the enjoyment of the rights to privacy and freedom of expression, which must be justified as permissible in accordance with human rights law. The applicable framework for determining whether a restriction on encryption is permissible was articulated at length by the Special Rapporteur on freedom of expression in his 2015 report; essentially, the standard permissible limitations test is to be applied with particular recognition to be given in the proportionality

[106] Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/29/32 (the 2015 Report of the SR on FOE), 22 May 205, para 16.

analysis to the sheer numbers of individuals affected by any restriction on encryption, as well as to "the strong possibility that encroachments on encryption and anonymity will be exploited by the same criminal and terrorist networks that the limitations aim to deter."[107]

Nevertheless, even as individuals begin to demand, and companies begin to provide, simpler and stronger encryption tools, the forces acting against encryption are growing stronger. Governments around the world are seeking to control the development of encryption tools and services, through regulating encryption strengths, controlling the export of encryption products, and banning the deployment of encryption in a variety of circumstances. Governments of countries such as Pakistan, Cuba, China and Ethiopia either prohibit the use of encryption, restrict the level of encryption allowed, or demand individuals seek prior authorisation for its use. In Ethiopia, terrorism charges have been levied at the Zone 9 bloggers for taking part in trainings related to encryption and digital security.[108] In Turkey, the only institutions authorised to carry out encrypted communications include the Turkish Armed Forces and the National Intelligence Organisation.[109] The United States and most European countries require companies seek authorisation for the export of products that deploy encryption above a particular strength.[110] Numerous Western countries are currently considering the introduction of legislation requiring companies to engineer encrypted products to enable State access. Such requirements would arguably fail to satisfy the proportionality requirements of both the privacy and free expression permissible limitations, particularly given their expansive impacts on individuals across the globe completely unconnected with any threat to a legitimate interest.[111]

Ethiopia: Terrorism charges against Zone 9 Bloggers and journalists must be dropped

Mandatory use or registration of identity

Whereas encryption provides security from interference with the content of a communication, it does not guarantee the anonymity of the sender or recipient of that communication, and separate measures must be taken to mask one's identity from detection. These measures may range from the use of a pen name or pseudonym to the wearing of masks, from the use of non-registered SIM cards to the use of anonymisation tools such as Tor. Given the nature of data analysis tools, multiple layers of anonymity may be needed to genuinely protect an individual from being identified, particularly when using digital tools and platforms when communicating. Remaining anonymous is a means of exercising one's privacy, and it may also be a means or precursor to freely expressing oneself, particularly in circumstances in which the expression of controversial opinions, beliefs or affiliations may challenge the status quo and place the person expressing them in danger or at risk of other rights violations. As the UN Special Rapporteur on freedom of expression has noted in his 2015 report on encryption and anonymity, anonymity plays a role in safeguarding and advancing not only privacy, but free expression, political accountability, public participation and debate.

---

[107] The 2015 Report of the SR on FOE, *op.cit*, para 35.
[108] ARTICLE 19, Ethiopia: Terrorism charges against Zone 9 Bloggers and journalists must be dropped, 18 July 2014.
[109] Article 39, Law on Electronic Communications (no. 5809).
[110] See e.g. the Wassenaar Arrangement On Export Controls For Conventional Arms and Dual-Use Goods and Technologies.
[111] The 2015 Report of the SR on FOE, *op.cit*,, para 43.

Anonymity and the rights it protects are threatened by a range of state measures requiring the mandatory use or registration of identity, including laws requiring the use of real names by bloggers and internet commentators, the registration of SIM cards and IP addresses, and the production of identification at cybercafes, as well as by mandatory retention of and State access to metadata. While some such measures have recently been curtailed by courts – the Supreme Court of Canada referenced the importance of enabling anonymity in its decision in *R v Spencer* (above) holding that law enforcement access to subscriber information requires judicial authorisation, and the Constitutional Court of the Republic of Korea struck down anti-anonymity laws as unconstitutional[112] – but they are proliferating in many other jurisdictions. A law currently under consideration in Brazil, Bill PL215/2015, would make it compulsory for all communications service providers (including those providing internet applications as well as telecommunications access) to collect identifying information on their users, including email addresses, telephone numbers and national identity numbers. The original version of the Bill, which included a number of even more harmful provisions that have now been removed, was designed, according to the government, to establish greater rigour in prosecuting crimes against honour taking place on social media.[113]

The Special Rapporteur on freedom of expression has recognized that both privacy and free expression are impacted by restrictions on anonymity. Such restrictions must therefore be lawful, necessary and proportionate in order to be justified. Beyond the UN Special Rapporteur, the Committee of Ministers of the Council of Europe adopted a Declaration on freedom of communication on the Internet which establishes anonymity as a central principle of freedom of communication, declaring that

> In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity.[114]

Big, ambient and anonymised data analysis

Beyond the personal data generated through use of the internet and digital technologies, other forms and sources of data, many of which are the by-product of use of digital technologies, are being identified and exploited by both private and public actors. Such data is often classified as "ambient" or "big" to indicate that it does not immediately related to an identified or identifiable person, and is sought after and used by actors as diverse as national health services, police forces, philanthropic organisations, development agencies, climate change scientists, town planners and transport authorities. Examples of such data sources and their potential uses might include:

- Cell tower location records mapped to public transport usage, which reveal inefficiencies in public transport schedules;[115]
- Purchase records, which reveal indicative factors enabling department stores to predict pregnancies in their customers;[116]

[112] Decision 2010 Hun-Ma 47, 252 (consolidated) announced 28 August 2012.
[113] Danny O'Brien, Brazil's Politicians Aim to Add Mandatory Real Names and a Right to Erase History to the Marco Civil, 14 October 2015.
[114] Council of Europe, Declaration on freedom of communication on the Internet, 28 May 2003, Principle 7.
[115] BBC News, Mobile phone data redraws bus routes in Africa, 1 May 2014.
[116] *Forbes*, How Target figured out a teen girl was pregnant before her father did, 16 February 2012.

- National health records analysis designed to better understand diseases, reveal effectiveness of certain treatments and efficiencies of particular services;[117] and
- Analysis of Google search queries to detect likely flue outbreaks prior to health surveillance efforts such as the Centers for Disease Control and Prevention.[118]

"Big data" has been much heralded as both a public policy solution-generator and a profit-multiplier for the private sector, yet it creates serious challenges to the protection and enjoyment of privacy. As noted by the report of the President's Council of Advisors on Science and Technology to US President Obama in May 2014, entitled *Big Data and Privacy: A Technological Perspective,*

> Anonymization is increasingly easily defeated by the very techniques that are being developed for many legitimate applications of big data. In general, as the size and diversity of available data grows, the likelihood of being able to re-identify individuals (that is, re-associate their records with their names) grows substantially. While anonymization may remain somewhat useful as an added safeguard in some situations, approaches that deem it, by itself, a sufficient safeguard need updating.[119]

Without the shield of anonymisation to prevent ambient data becoming personal data, the potential for interferences with privacy are clear. In addition to the first order interference with privacy – whereby an individual's personal information is being used for a purpose to which they did not consent on an informed basis – a number of subsequent risks arise, not least of which is that the analysis performed on big datasets "can help governments spy on their citizens and criminals prey on their victims", according to Professor Paul Ohm of the Colorado Law School.[120]

In incentivising the creation of databases full of information not previously generated, collected or stored – from location data to Google searches, shopping purchases to train journeys – big data initiatives motivate the tracking and monitoring of individuals (even if anonymous) in previously unimagined ways. This cannot but have a correlative impact on free movement and expression, slowly and imperceptibly changing the way we interface with the internet and potentially inhibiting our attempts to seek and share knowledge there. To the extent that the right to privacy, and particularly that to the protection of personal data, requires that such practices are limited to that which are strictly lawful, necessary and proportionate, it prevents the chilling effect that big data may have on the free enjoyment of the right to expression and information using digital tools and technologies.

Open source intelligence gathering

Information derived from publicly available sources has always been a valuable source of information for police and intelligence services and corporate actors. Analysis of public data, government records, media reporting, classified advertisements and professional and academic literature could always be mined – and paired with other intelligence gathering methods – to paint a picture of an individuals' private life. However, rapid advancements in

---

[117] See, e.g. NHS, Your Health and Care data initiative.
[118] See, e.g. Google Flu Trends.
[119] Executive Office of the President President's Council of Advisors on Science and Technology, Big Data and Privacy: A Technological Perspective May 2014, p. xi.
[120] Paul Ohm, The Underwhelming Benefits of Big Data, 161 *University of Pennsylvania Law Review Online* 339, p. 340.

technological analysis methods, coupled with the exponential expansion in the quantity of publicly available information, has fundamentally changed the nature of open source intelligence gathering. Now, police forces and intelligence agencies are able to used advanced computing capabilities to crunch through gigantic feeds of raw data – from the Twitter and Facebook "firehoses" (the entire stream of all public posts from around the globe transmitted in real time), to digitised books, records and databases; from data on every plane and train journey occurring anywhere in the world, in real time, to every single newspaper and television show transmitted on a daily basis.

Pervasive, systematic or prolonged analysis of public information can interfere with the enjoyment of both privacy and free expression. With respect to the former, it enables intimate profiles to be drawn about an individual, facilitating, for example, the identification of their sexual, political or religious preferences. As the United States Supreme Court observed in *U.S. v. Maynard*,

> Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month.[121]

This sentiment was echoed by the US Supreme Court in the more recent case of *United States v Jones*, where it was found that the use of a GPS tracking device constitutes a search to which the Fourth Amendment applies. Justice Sotomayor's concurring but separate opinion argued for the pressing need to update US jurisprudential approaches to privacy in the digital era; whereas the majority decided *Jones* on the basis that a trespass has occurred on the individual (by virtue of the installation of the GPS device), Sotomayor J argued that a reasonable expectation of privacy existed vis a vis the "sum of one's public movements". In her opinion, Sotomayor J also made the connection between privacy and freedom of expression in the context of pervasive monitoring:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse [...] I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.[122]

European human rights law similarly holds that the collection, storage and retention of public information by the State amounts to an interference with Article 8 that must be justified in accordance with the standards of legality, necessity and proportionality. In *Rotaru v Romania*, the European Court of Human Rights held:

> Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities. That is all the truer where such information concerns a person's distant past...In the Court's opinion, such

[121] 615 F.3d 544 (U.S., D.C. Circ., C.A.)p. 562.
[122] 565 U.S. (2012) at 4.

> information, when systematically collected and stored in a file held by agents of the State, falls within the scope of 'private life' for the purposes of Article 8(1) of the Convention.[123]

This principle was upheld by the British Supreme Court in the recent case of *R (on the application of Catt) v Commissioner of Police of the Metropolis* [2015] UKSC 9, in which the Court affirmed, citing *Rotaru v Romania,* that the "state's systematic collection and storage in retrievable form even of public information about an individual is an interference with private life" for the purposes of Article 8 (at [6]). In the case of *Catt,* the Court was considering, inter alia, the operation of the "Domestic Extremism Database", through which British police collect, retain and store records on the attendance by members of the public at public demonstrations. The Supreme Court overturned a decision of the Court of Appeal which held that the retention and storage of such public information was a violation of Article 8, and in doing so affirmed that the maintenance of such a database, in the circumstances, satisfies the requirements of necessity and proportionality.

It is expected that *Catt* will be subject to a forthcoming application to the European Court of Human Rights, which will hopefully provide further light on how the rights to privacy and freedom of expression are impacted by open source intelligence gathering. For the moment, there remain a number of questions about the extent to which acts of expression in "public" online fora such as Twitter can legitimately be considered private information under certain circumstances, including when they are the subject of State analysis.

Restrictions on investigative journalism and access to information

The interests of privacy and freedom of expression intersect in a critical way in the realm of national security. In an environment of increasingly pervasive secrecy in both democratic and autocratic countries the world over, and in the context of greater state power over communications and information, investigative journalism remains one of the key means by which information about unlawful overreaches of State authorities can be uncovered and exposed to the public. In many countries, investigative journalism is the only mechanism by which the actions of intelligence and security agencies with respect to surveillance and interception of communications can be scrutinised.

Investigative journalists have been key in uncovering unlawful surveillance by intelligence and police authorities since *Washington Post* journalists Carl Bernstein and Bob Woodward exposed the Watergate scandal in 1972. Journalists played a key role in shining light on the Greek wiretapping scandal in 2004, which involved the tapping of more than 100 mobile phones belonging to members of the government and civil service via the Vodafone Greece network. British journalist Duncan Campbell revealed the existence of British plans to acquire an intelligence satellite in 1986, and in 1988 exposed the existence of the ECHELON programme, a "global system for the interception of private and commercial communications."[124] Nicky Hagar, a New Zealand investigative journalist, played a similar role in New Zealand in the 1990s, building on Campbell's work and documenting New Zealand's participation in the secretive Five Eyes Alliance. American journalist and former NSA intelligence analyst James Bamford has spent his career documenting the internal operations and excesses of the NSA and other American intelligence organisations. Most

[123] ECHR 28341/95, paras. 43-44.
[124] European Parliament: Temporary Committee on the ECHELON Interception System, Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system).

recently, journalists Glenn Greenwald, Laura Poitras, Ewan McAskill, James Ball and a number of others have jointly coordinated the publication, interpretation and further investigation of documents released by NSA whistleblower Edward Snowden, to great acclaim.

In addition to working with sources and whistleblowers, and conducting undercover investigations, an essential tool of investigative journalists in the national security space is the use of access to information laws. The Global Principles on National Security and the Right to Information recognise that "it is imperative, if people are to be able to monitor the conduct of their government and to participate fully in a democratic society, that they have access to information held by public authorities, including information that relates to national security."[125] Freedom of Information Act (FOIA) requests have been the mechanism by which many stories about executive use of surveillance and intelligence techniques have overstepped lawful and ethical boundaries; recently, for example, they have facilitated the publication of opinions of the Foreign Intelligence Surveillance Court which corroborate many of the allegations made by NSA whistleblower Edward Snowden. A FOIA request even unearthed a memo published by the Office of the Director of National Intelligence, in the months prior to the Snowden leaks, entitled "Deterring and Detecting Unauthorized Disclosures, Including Leaks to the Media, Through Strengthened Polygraph Programs." Restrictions on access to information, therefore, impair the ability of journalists to properly exercise their important public watchdog functions and equally undermine the enjoyment of other human rights to which the actions of the government in the national security space might apply, including privacy, and must therefore only be implemented in strict compliance with the principles of legality, necessity and proportionality.[126]

A further mechanism for accessing information which supports both privacy and free expression rights is the invocation of the right of access to personal information, held on an individual by a public or private entity, such as is enabled through Subject Access Requests (under European data protection law), or writs of "Habeas Data" (in a number of Latin American countries, as well as the Philippines). Under European Law, individuals can demand to know about what data is being used and request to have reasons given for computer-generated decisions made about them. Habeas Data equally gives the individuals the right to access, correct, and object to the processing of their information. Access to personal information reinforces the right to privacy by ensuring that individuals have control over their personal data and are able to make informed decisions about how to share it; it also supports the right to access information about how companies and governments use data on their citizens. A subject access request was famously used by Austrian privacy campaigner Max Schrems against Facebook to uncover that Facebook was storing and retaining excessive amounts of information, including posts and photos that users had deleted or never even placed online.[127]

Measures undermining the protection of sources and whistleblowers

As the Special Rapporteur on freedom of expression highlighted in his 2015 report on journalists' sources and whistleblowers, even when formal mechanisms exist for the disclosure

[125] https://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf
[126] See also the Johannesburg Principles on National Security, Freedom of Expression and Access to Information.
[127] Kashmir Hill, "Max Schrems: The Austrian thorn in Facebook's side," *Forbes,* 7 February 2012.

of information of public concern, they are not always effective and other approaches may be needed, "for as a general rule, secrets do not out themselves."[128]

The protection of sources and whistleblowers is grounded in the public's right to receive information, which right can only be limited when prescribed by law, necessary and proportionate. International law provides that sources can expect to remain confidential, and journalists cannot be compelled to disclose sources' identity. This principle has been affirmed most recently by the East African Court of Justice in the case of *Burundi Journalists Union v. Attorney General of the Republic of Burundi,* in which the Court held that journalists cannot be compelled to disclose the identity of sources merely because they provide information related to national security.[129]

Technological advancements and the new communication opportunities provided by the internet have challenged existing understandings of who is entitled to claim and guarantee source confidentiality. In addition to the increasingly active role played by NGOs and civil society organisations in using sources to disseminate information of government wrongdoing, bloggers, citizens journalists and other members of the informal media are also engaged in utilising confidential sources for the purpose of expression and reportage. The changing boundaries of who is a journalist or engaged in journalistic endeavours poses challenges to definitive statements about entitlements to source confidentiality, which have to be determined on a case by case basis.[130] According to the Special Rapporteur, however,

> [...] any person or entity involved in collecting or gathering information with the intent to publish or otherwise disseminate it publicly should be permitted to claim the right to protect a source's confidentiality. Regular, professional engagement may indicate protection, but its absence should not be a presumptive bar to those who collect information for public dissemination.[131]

The scope of the protection to which sources are entitled may be subject to some exceptional restrictions, applied by a judicial authority, which should genuinely be confined to situations in which the disclosure of the source's identity is essential for obtaining information that is crucial for the prevention of crimes that pose a serious threat to the physical integrity of a person, and there is no other way of obtaining that information.

---

[128] A/70/361 at [1]
[129] East African Court of Justice, case No. 7 of 2013, judgment of 15 May 2015, paras. 107-111
[130] In the Irish case of *Cornec v Morrice & Ors*, *op.cit.*, the Court considered that "a person who blogs on an internet site can just as readily constitute an "organ of public opinion" as those which were more familiar in 1937." It also found that there was a high constitutional value in ensuring the blogger's right to contribute to public discourse, and that being compelled to reveal their sources would compromise the "right to educate (and influence) public opinion, [which] is at the very heart of the rightful liberty of expression;" at [66].
[131] A/70/361 at [18].

Privacy in conflict with freedom of expression

It is well-established that some acts of expression may interfere with another's privacy rights. Traditionally, such acts have been generally confined to the publication in the print or broadcast media of information and images pertaining to individuals who played some role in public life: from reporting on criminal proceedings, investigations into the past behaviour of political candidates, or the publication of expenses records and official diaries of members of parliament, for example. In general, human rights law provides a mechanism in order determine claims both under the right to freedom of expression and the right to privacy (see three-part test above in sections 1 & 2). The case-law of various national and international courts further provide criteria in order to balance these rights where appropriate.

The advancements of the digital age, however, have increased the complexity of balancing privacy and freedom of expression; in increasing the range of actors, fora and opportunities for expression, technologies have also created new challenges for the protection of privacy and, in particular, personal information. At the same time, hyper-awareness of privacy concerns have created new risks for freedom of expression. Recent measures by courts and governments to ostensibly protect privacy – by requiring the use of real names and identities in online forms, mandating the delinking of particular news articles from search results, or by sanctioning heavy-handed remedies for privacy violations – constitute a serious interference with the rights and ability of individuals around the world to express themselves; they also threaten to entrench State and corporate control over information, memory and truth.

How are we then to balance the rights to privacy and freedom of expression in the digital age? Answering this question requires recognition of the defining features of the modern expression:

- **Information can be generated and shared instantly on a massive scale**: the nature of the "information age" is that information is generated by almost every digital – and some analog – activity. There is exponentially more information to be shared and accessed, and there are exponentially more actors equipped with the capability to analyse and disseminate that information. There are new capabilities to synthesise huge amounts of data, to turn anonymised data into personal information, and to gather and publish data in real-time. Access to and publication of information are becoming democratised, with reportage no longer being the preserve of a select few, but rather anyone with a Twitter, Tumblr – or, increasingly, SnapChat – account. At the same time, the quality of information available through digital technology varies: while enabling the production and dissemination of factual information, news, art and literature, the internet also facilitates the sharing of false information, some of which is potentially defamatory. Meanwhile, private information can be shared instantly and on a scale never before imagined, resulting in serious interferences with the right to privacy. The ubiquity of information has therefore led to a corresponding desire to control it. For individuals, this has translated into a rise of data protection law as a means for individuals to retain control over 'their' data. For governments, this has primarily resulted in website blocking and filtering and mass surveillance laws, often coupled with a push for greater secrecy over transparency. The role of public watchdogs is thus more important than ever.

- **The line between public and private is increasingly hard to draw***:* publicly available information can acquire the protection of data protection law where it is pervasively collected and analysed (e.g. open source intelligence gathering); private citizens can become public figures through the luck of the internet. Any information published on the Internet can potentially have a global audience. All these developments raise the question of the applicable criteria for determining who a public figure might be in the digital age and what amounts to the public interest in circumstances where the audience is the global public.

- **What amounts to content and editorial control is changing**: the birth of social media platforms upon which individuals can express ideas and opinions has cut down the barriers to becoming a public commentator, but it has also created confusion about what is content, and who is responsible for it. Today, content might mean 140 characters or a stream-of-consciousness rant in a comment section. At the same time, some people might consider that content includes a link to an external website and that the algorithmic decision to list search results in a particular way is a form of editorial control,. While the distinction of what is and is not content may appear trivial , the implications of such a distinction for the providers of such platforms are not.

- **The ramifications of restraints on expression are far-reaching**: whereas the impact of an interference with privacy is felt – often painfully - by a sole individual or restricted group of individuals (including family members, friends or colleagues of the person concerned), the harm of a restriction on freedom of expression can be felt by the world at large. Requirements that individuals register their identity when operating a blog or commenting online, the removal of forms of artistic or political expression from online platforms, the compulsory take-down of websites and content: these are remedies which not only impact potentially millions of internet users, but have broader societal impacts, deterring future acts of expression, altering the risk calculation of formal media outlets, and incentivising proactive moderation by internet intermediaries.

Throughout this chapter we seek to identify the circumstances in which the full protection of privacy and freedom of expression respectively create conflicts that need to be resolved through the application of a nuanced balancing test that takes into consideration these, and other, modern realities. We do not attempt to provide an exhaustive categorisation or examination of all such circumstances; only to address them to the extent they give rise to questions that need to be considered.

We first look at five broad areas in which conflicts between the rights to privacy and free expression arise: (1) the protection of reputation; (2) the protection of personality; (3) the protection of personal information; (4) sanctions and remedies for privacy violations; and (5) conflicts which arise in the context of the internet.

Protection of reputation

Protection of reputation under international law

The protection of reputation has traditionally resided not in human rights law, but in the law of defamation, which pertains to the communication of false statements of fact that harm an individual's reputation. There is an extensive body of law detailing the circumstances in which restrictions on freedom of expression may be justified in order to protect the reputation of

others, and ARTICLE 19 has developed (and recently updated) a set of principles in this regard (cite to be added).

In recent years, however, we have seen the emergence of claims to the protection of reputation being made under the right to privacy. As noted in section 2 above, the existence of a right to a reputation is supported by Article 17 of the ICCPR, although its contours and content remains subject to debate. However, there is no right to reputation enshrined in Article 8 of the European Convention, and yet the Strasbourg has in recent jurisprudence referenced it in relation to the right to privacy. This has created considerable confusion in the jurisprudence; whereas defamation relates to false statements of fact which impact upon reputation, the Strasbourg Court has been considering the role of reputation in the context of the publication of true statements, including publications in which there has been no wrongful interference with an individual's privacy.[132] As such, in international law we are seeing the emergence of a self-standing right to reputation which would be contravened by the publication of true information or statements, without any correlative interference with an individual's privacy.

Protection of reputation under domestic law

A number of civil and criminal causes of action exist under various domestic laws to protect reputation:

- **Injury to reputation**: in South Africa, a defamatory statement is under common law by definition one that "has the effect of injuring a plaintiff's reputation," with the veracity of the statement being immaterial to the cause of action. In the 2002 case of *Khumalo & Ors v Holomisa*,[133] the South African Constitutional Court considered whether the lack of a requirement for civil defamation claims to establish the falsity of the statement in question was inconsistent with the right to freedom of expression in section 16 of the South African Constitution. The Court considered that "although freedom of expression is fundamental to our democratic society, it is not a paramount value. It must be construed in the context of the other values enshrined in our Constitution. In particular, the values of human dignity, freedom and equality."[134] Under South African law, defamation is one of a number of causes of action which fall within the ambit of the delict *actio iniuriam*, originally a Roman Law remedy for injury to a person's dignity, reputation and physical integrity. Modern continental European personality rights are also grounded in *actio iniuriam* (see below).

- **Protection of honour and good name**: honour is closely tied to reputation and dignity, and is often an element of defamation offences under both civil and criminal laws. A number of European and Latin American countries provide civil protection for attacks on honour as a distinct cause of action from defamation, including.
  - In Spain, Law 1/1982 of 5 May provides civil protection for the right to honour, alongside personal and family privacy.
  - In Colombia, journalists must refrain from publishing personal information or images that, despite their veracity, lead the audience to conclusions that jeopardise honour, dignity or the good name of the person.[135]

[132] TBC, citation
[133] Case CCT 53/01, judgment of 14 June 2002,
[134] At [25].
[135] Constitutional Court Decision T-439/09

- In Italy, the offences provided for by the Criminal Code to protect people's honour and reputation are insult and defamation. Insult is the act of offending the honour of a person who is present (Article 594) while defamation consists of undermining the reputation of an absent person (Article 595). The Court of Cassation has ruled several times on the question of the limits to the right to report and comment in the light of the need to protect people's honour. With regard to the right to report (that is, free expression pertaining to journalists) the Court of Cassation considers that it applies when the following conditions are met a) the report is in the public interest; b) the facts described are true; c) the ideas are expressed in courteous terms.[136] With regard to the right to comment (the right to free expression enjoyed by ordinary persons commenting, rather than reporting), the Court of Cassation considers that this must be exercised within the following limits: a) appropriate language; b) respect for the rights of others.[137]
- In Armenia, the 1991 Law of the Press, Article 7 prohibits the use of the mass media for encroaching upon the personal lives of citizens, their honour or dignity.[138]
- In Albania, under Article 625 of the Civil Code, a person who has suffered "harm to the honour of his personality" has a right to compensation.[139]

There also exists a number of criminal prohibitions relating to honour:

- The Bulgarian Criminal Code, Article 146 (1) provides that "Anyone who, through word or deed, insults the honour or dignity of a person in his or her presence" shall be punished by a fine, unless the insult is returned immediately;[140]
- In Azerbaijan, there are specific protections against attacks on the "honour and dignity of the President" (Article 106 of the Constitution, Article 323 of the Criminal Code);[141]
- The Swiss criminal code provides, in Article 173, that "All persons who in addressing a third party, accuse or cast suspicion on others of dishonourable conduct or of other conduct that is liable to damage those persons' reputation or persons who disseminate such accusations or suspicions shall on complaint be liable to a prison sentence not exceeding six months or a fine;"[142]
- Numerous jurisdictions legislate to criminalise "crimes of honour" relating to sexual practices and marriage, or provide for honour defences for men accused of harming their wives.[143]

- **Dignity**: The concept of dignity underpins most international, regional and constitutional human rights texts, and can generally said to be at the core of a number of human rights, not just the right to privacy.[144] The concept of dignity has been central to the development of norms around abortion, apartheid, sexual violence and racial

[136] Judgment 3999/2005.
[137] Judgment 10135/2002.
[138] Council of Europe, Draft Study on the alignment of laws and practices concerning defamation with the relevant case-law of the European Court of Human Rights on freedom of expression, particularly with regard to the principle of proportionality, CDMSI(2012)Misc11.
[139] *Ibid.*
[140] *Ibid.*
[141] *Ibid.*
[142] *ibid.*
[143] A bibliography on crimes of honour, the Centre for Islamic and Middle Eastern Law (CIMEL) and INTERIGHTS.
[144] See Christopher McCrudden, Human Dignity and Judicial Interpretation of Human Rights, 19 *European Journal of International Law* 4, 655-724.

discrimination. In the context of conflict with free expression rights, however, dignity is relevant to the extent that injury to dignity is used as cause of action to restrict the expression or publication of material, information or images that impair the dignity of another person.

Such a cause of action exists under South African law. Actions can be brought under South African law with respect to injury to dignity when "a person is subjected to offensive and degrading treatment or is exposed to ill-will, ridicule, disesteem or contempt": *Sokhulu v New Africa Publications Ltd t/a "The Sowetan Sunday World" and Others*,[145] citing *Minister of Police v Mbilini.*[146] Jurisprudence establishes the centrality of dignity in post-apartheid South Africa; in *Dawood and Another v Minister of Home Affairs and Others; Shalabi and Another v Minister of Home Affairs and Others; Thomas and Another v Minister of Home Affairs and Others*[147] the Constitutional Court argued that the Constitution "asserts dignity to contradict our past in which human dignity for black South Africans was routinely and cruelly denied. It asserts it too to inform the future, to invest in our democracy respect for the intrinsic worth of all human beings." Under the action of dignity, injurious words uttered by a defendant to a plaintiff in the presence of another person can constitute a serious violation of dignity, if such words are of a particularly offensive nature and depending on all the circumstances of the case: *Ryan v Petrus.*[148]

New challenges in the context of the Internet

- **Defamation on social media**: a recent case of "defamatory" comments made by South African users on Facebook illustrates the concerns for freedom of expression that arise from broad laws seeking to protect 'dignity'. In the case of *Isparta v Richter*,[149] the plaintiff brought a defamation claim against the first and second defendants for comments made by the first defendant on her Facebook wall which had referenced the plaintiff, and in which the second defendant had been "tagged" by the first. Not only were the defendants found liable for defamation on the basis that the comments were injurious to the plaintiff's reputation (despite them being true), the second defendant was found jointly liable despite not having made the comments, but merely having allowed himself to be associated with them by virtue of the "tag".

- **Revenge pornography, cyber-bullying and harassment***:* in some cases, private images are being maliciously reproduced and disseminated online in an express attempt to cause harm to another's privacy or their reputation, often in a manner that constitutes harassment. In recent years, this phenomenon, often called "revenge porn", has been met with the elaboration of legislation which seeks to criminalise or penalise the deliberate publication of images online for the purpose of harassment.

  Twenty-four States of the United States have adopted revenge pornography laws. For example, California enacted SB 255 Electronic Communication Devices: Prohibited Distribution of Personal Information in October 2013, amending the penal code to create a new misdemeanour of disorderly conduct by way of distribution of intimate photographs

[145] [2002] 1 All SA 255 (W) at 259c – d
[146] [1983] (3) SA 705 *(A) at 715G – 716A*
[147] [2000] ZACC 8; 2000 (3) SA 936
[148] (CA 165/2008) [2009] ZAECGHC 16
[149] **(22452/12) [2013] ZAGPPHC 243**

with the intent to cause serious emotional distress. The original text of the bill was opposed by First Amendment advocates such as the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation, which argued that the bill could result in criminalisation of speech, particularly as it was designed to criminalise what they labelled "victimless instances", where no individual was able to demonstrate that they experienced harm as a result of the action. Accordingly, the bill was amended to include, as a condition of the crime, that the parties must have established an agreement or understanding that the image should remain private, and the image was subsequently distributed in violation of that agreement.[150]

The Arizona equivalent law was far broader, banning the posting of nude images without consent, clearly raising concerns from the perspective of freedom of expression to the extent that it would impede the publication of legitimate artistic or consensual images. The law was again challenged by the ACLU on First Amendment grounds and in July 2015, the Arizonan government agreed to not enforce the law.[151]

In Canada, the province of Nova Scotia adopted in 2013 the controversial Cyber Safety Act, providing for a process whereby individuals subject to cyber bullying (or, in the case of minors, their parents) can apply to a justice for a protection order against an individual. The legislation came about as a direct result of the death of 17-year-old Nova Scotia student Rehtaeh Parsons, who took her own life after having been subject to months of harassment and humiliation stemming from the dissemination online of a photo of her being allegedly sexually assaulted. She died on 7 April 2013; three weeks later, the Cyber Safety Bill was introduced into the Nova Scotia provincial parliament.

The Cyber Safety Act contains provisions requiring electronic communications service providers to assist the court in identifying individuals responsible for cyber bullying. The act also creates the tort of cyber bullying, enabling individuals to sue another for damages arising out of cyber bullying. In particular, the Act defines cyberbullying as

> Any electronic communication through the use of technology including, without limiting the generality of the foregoing, computers, other electronic devices, social networks, text messaging, instant messaging, websites and electronic mail, typically repeated or with continuing effect, that is intended or ought reasonably be expected to cause fear, intimidation, humiliation, distress or other damage or harm to another person's health, emotional wellbeing, self-esteem or reputation, and includes assisting or encouraging such communication in any way.

The Cyber Safety Act also amends the Safe Communities and Neighbourhoods Act 2006 to establish a CyberSCAN unit tasked with investigating complaints related to cyber bullying, issuing warning letters, requesting an internet service provider to discontinue service, or applying to the court for an order requiring the production of information about the identity of an individual accused of cyber bullying. In response to an application by a director of public safety, the court may issue an order requiring information to identify who may have used an IP address, website, account or username, or particular device; and to produce cell phone records, text message records, internet browsing history records and any other records that would assist in investigating the complaint.

---

[150] Bill No: SB 255, Bill Analysis.
[151] Joe Mullin, "Arizona makes deal with ACLU, won't enforce bad law on "revenge porn, *Arstechnica*, 12 July 2015.

The Act has been challenged at least twice on the basis that it contravenes rights set out in Canada's Charter of Fundamental Rights. In March 2015, an order issued under the act was overturned by the Supreme Court of Nova Scotia, which held that the order caused damage to the subject's constitutional right to free speech and to his property right to use his own technical equipment.[152] In December 2015, the Supreme Court of Nova Scotia struck down the Act as being too draconian.[153] In particular, the Court found that in determining whether the Act unnecessarily caught material that had little or nothing to do with the prevention of cyber-bullying, the Act – and the definition of cyberbullying in particular - was a 'colossal failure'.[154]

Balancing protection of reputation with freedom of expression

As the Internet and new technologies challenge what it means to define and assert one's identity, the concept of protection of reputation is taking on new importance. There is an emerging recognition of the ways in which an individual's reputation may be negatively affected by another's exercise of their freedom of expression, particularly through online means. Arguably, reputation and its related concepts is becoming even more important in the digital era than it was previously, particularly as businesses and relationships are becoming increasingly globalized.

However, the concepts of honour, dignity and reputation are inherently broad, subjective and prone to manipulation by those who harbor ulterior motives to silence critics and those who challenge the status quo. The protection of these interests will often result in serious implications for freedom of expression, including the silencing of critical voices, and can have chilling effects on the broadcast and print media, as well as on individuals using social networks and other only platforms that facilitate the exchange of ideas and opinions.

In order to develop principles to assist in balancing reputational claims on the one hand, with freedom of expression concerns, on the other, we propose the following questions will be relevant:

- The form of expression interfering with the individual's reputation: was it written or verbal, was it a formal (print or broadcast media) or informal (online commentary)?
- Who was the audience: readers of a newspaper or a blog, "Friends" on Facebook, family members at an event?
- Was the intention of the person making the relevant statement: to inform, expose, offend, or cause distress?
- Was there a public interest in the relevant statement being published?
- What was the degree and extent of the harm to the individual's reputation?
- What opportunities are there to mitigate the harm to the individual's reputation?
- How long-lasting will the effects on the individual's reputation be?

---

[152] Harry Sullivan, "Order overturned," *Truro Daily*, 27 March 2015, available http://www.trurodaily.com/News/Local/2015-03-27/article-4092650/Order-overturned/1

[153] See CBC News, *Court strikes down anti-cyberullying law created after Rehtaeh Parson's death,* 11 December 2015, available http://www.cbc.ca/news/canada/nova-scotia/cyberbullying-law-struck-down-1.3360612

[154] Supreme Court of Nova Scotia, *Crouch v. Snell*, 2015 NSSC 340, at page 47 ff, available from http://www.courts.ns.ca/Decisions_Of_Courts/documents/2015nssc340.pdf

Protection of personality and images

The term "personality rights" is used in a number of contexts; interchangeably with the right to privacy or to an even broader conceptualization of how privacy enables the development of an individual's personality (primarily in civil law jurisdictions); and in the context of the property right to "publicity", the ability to control the commercial use of one's name and image (primarily in common law jurisdictions). In both legal traditions, personality rights confer particular protections to an individual's image, its use and publication.

Personality rights in civil law jurisdictions

Continental European notions of "personality rights" are grounded in the delict *actio iniuriam*, originally a Roman Law remedy for injury to a person's dignity, reputation and physical integrity. Although "personality rights" as understood under the domestic law of a number of European countries have their roots, just as with the right to privacy, in the protection of human dignity and autonomy, the civil right to a personality arguably has broader contours than the right to privacy as it is currently understood under international human rights law.

German law protects a general right of personality through both its civil and Basic Law (constitutional law). According to the German Federal Constitutional Court states, the right of personality serves to "secure the closer personal sphere of life and the maintenance of its basic condition."[155] Actions of defamation under German law fall within the ambit of personality rights, as the right protects against "statements that are capable of having a negative effect on a person's reputation, in particular his or her public image," especially when these "distorted or falsified representations" will have a significant impact on the development of personality.[156] In addition, the Federal Supreme Court of Germany said in the *Marlene Dietrich* case, that the general right of personality

> Guarantees as against all the world the protection of human dignity and the right to free development of the personality. Special forms of manifestation of the general right of personality are the right to one's own picture and the right to one's name. They guarantee protection of the personality for the sphere regulated by them" (citations omitted).[157]

French courts have referenced the notion of personality rights since the 1960s,[158] and such rights are commonly understood to be enshrined in Article 9 of the French Civil Code, although the *travaux preparatoires* to Article 9 show that the French government explicitly rejected the framing of personality rights in drafting the Article, choosing instead to echo the language in the European Convention, despite France not being a party to the Convention at that time.[159]

There are no identifiable causes of action specifically related to personality rights, but rather the term personality is connected with domestic law protections for privacy, in countries like Germany, France and Estonia. The reasoning of the German courts with respect to

---

[155] Federal Constitutional Court, BVerfGE 119, 1, para. 70 = 39 IIC 606, para. 70 (2008).
[156] *Ibid*.
[157] *Marlene Dietrich* Case, BGH 1 ZR 49/97, judgement of 1 December 1999.
[158] Paris civil court 8 July 1965, consorts de Rothschild c Peyrefitte et Editions Flammarion, JCP. 1965.II.14443, note RL ("an incontestably grave infringement of his personality"; Paris court of appeal, 13 March 1965, Dame Philipe c France Editions Publications, JCP.1965.II. 14223 (" the protection of the rights of personality").
[159] Roger Errera, The Origins and Content of Article 9 of the Civil Code on the Right to Privacy, speech delivered at the Franco - British Lawyers Society Privacy in an open society, 22-23 September 2011.

enforcement of the right to personality demonstrates that the concept is broadly interpreted to include "the individual's claim to social respect and value".[160]

Common law understandings of personality rights

In common law jurisdictions, continental approaches to personality rights are reflected in two separate legal cannons; personal rights pertaining to a person's private information or private space, and property rights pertaining to a person's image, name or notoriety. The latter are often called "publicity rights", but are also called personality rights. In common law jurisdictions such as Australia, New Zealand and the United Kingdom, publicity rights are given protection through the **tort of passing off**, which prevents one trader from misrepresenting goods or services as being the goods and services of another, and also prevents a trader from holding out his or her goods or services as having some association or connection with another when this is not true.

In US law the **tort of appropriation** affords protection against the use of an individual's name, likeness, or identity without consent for purposes such as ads, fictional works, or products. The tort of **publicity given to private life** provides that "*o*ne who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[161] The case of *Cox Broadcasting Co. v. Cohn* holds that under the First Amendment there can be no recovery for disclosure of and publicity to facts that are a matter of public record.[162]

Canadian courts protect an individual's right of publicity through the tort of **"appropriation of personality",** which is intended to protect the goodwill in one's identity or image and prevent misuse.[163] While Canada does not have a constitutional protection applicable to the private law in respect of capturing and distributing images, the freedom of expression considerations articulated in the Charter are generally applied in interpreting and applying this civil action.[164] The primary limitation for determining appropriation of personality is if there was to be a direct or indirect endorsement by the specific individual: Krouse v. Chrysler Canada Ltd.[165] Even when the use of an image does not constitute an endorsement, the plaintiff's personality will have been appropriated where there has been commercial use of his or her image without consent: *Athans v. Canadian Adventure Camps Ltd.*[166]

The publication of images of individuals who aren't celebrities or public figures without their consent are also protected by personality rights in many jurisdictions. In Greece, for example, images are protected under **"publicity rights"** provisions in the Greek Civil Code, provisions 57, 58 and 59. Image, name and alias, voice and all characteristics relating to an individual's identity person are all protected under the right of publicity, regardless of their notoriety and whether their identity is commercialised. A number of cases have shown that even using

---

[160] BVerfGE 30, 173, Federal Constitutional Court (First Division), 1971.
[161] Restatement of the Law, Second, Torts 652D
[162] (1975) 420 U.S. 469
[163] Rob McDonald and Chad Zima, *I am the Greatest' The Use of Celebrity Endorsements and Images*, Miller Thomson.
[164] John S. McKeown, *Fox on Canadian Law of Copyright and Industrial Designs,* FoxCopyright 6:2 (2003).
[165] (1973), 1 O.R. (2d) 225 (Ont. C.A.).
[166] (1977), 17 O.R. (2d) 425 (Ont. H.C.).

photographs of inhabitants of rural Greece on postcards and in tourist guides without their consent constitutes an infringement of their right of publicity.[167]

In contrast, the British courts have traditionally rejected developing actions for the protection of personality features such as likeness, voice, distinctive clothes, etc. or a establishing a more general right of publicity.[168] The protection of publication of images under British law has historically been available only under evolving interpretations of the tort of passing off. However, as European human rights law develops and is imported into British jurisprudence, this situation is changing.

Personality rights in ECtHR jurisprudence

Although Article 8 of the European Convention on Human Rights makes no mention of personality, publicity or image rights, the concepts have been gradually read into the right to privacy through the jurisprudence of the Strasbourg Court. In the seminal case of *Von Hannover v Germany (No. 2),*[169] the ECtHR made explicit reference to the concept of personality as falling within Article 8, stating that

> The concept of private life extends to aspects relating to personal identity, such as a person's name, photo, or physical and moral integrity; the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings.[170]

The Court also made the link between the right to personality and the images or photos which are linked to that personality, noting that "a person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers."[171]

Reference to personality rights was also made by the Grand Chamber in its controversial 2015 decision in *Delfi v Estonia* (addressed further below).[172] In that case, the Court was adjudicating the violation of Article 10 in the context of a domestic jurisdiction (Estonia) in which national legislation made express provision for personality rights. Nevertheless, the reasoning of the Court clearly evidences that the Court considers personality rights to broadly form part of the Article 8 protections. The Court concluded,

> [W]hile the Court acknowledges that important benefits can be derived from the Internet in the exercise of freedom of expression, it is also mindful that liability for defamatory or other types of unlawful speech must, in principle, be retained and constitute an effective remedy for violations of personality rights.[173]

The Delfi case therefore appears to signal the Court's willingness to take a more expansive approach to the protection of Article 8 rights, one which embraces the broader continental

---

[167] Case 168/1979 and Case 3051/2003.
[168] *Tolley v Fry* [1931] A.C. 333, *McCulloch v May* (1948) 65 R.P.C. 58, *Elvis Presley Enterprises Inc. v Sid Shaw Elvisly Yours.* [1999] R.P.C. 567.
[169] App. No. 40660/08 [2012] ECHR 228 (7 February 2012)
[170] *Von Hannover (no. 2),* at [95].
[171] *Ibid.,* at [96].
[172] App. no. 64569/09, 15 June 2015
[173] *Delfi,* at [100].

notion of 'personality rights'. In particular, Judge Zupancic noted in his separate concurring opinion in Delfi:

> The substance of the case concerns the protection of personal integrity, that is, of personality rights in Estonia and also, after this case, elsewhere in Europe. For many years personality rights were, so to speak, discriminated against *vis-à-vis* the freedom of expression, specifically the freedom of the press. In my concurring opinion in the *Von Hannover v. Germany (no. 1)* case (no. 59320/00, ECHR 2004-VI), I wrote that "[t]he *Persönlichkeitsrecht* [personality rights] doctrine imparts a higher level of civilised interpersonal deportment", and I believe the facts of the case at hand confirm this finding.[174]

New challenges in the context of the Internet

Republication of images posted online*:* there are now many internet applications whose primary function is to enable the reproduction and sharing of images, including images of individuals who have not given their consent for the upload and dissemination of their image. On Facebook, for example, individuals can upload photos and choose whether or not to notify the affected individual (through "tagging") and whether or not to make those photos accessible to the general public (through the manipulation of privacy settings).

The reproduction of another person's image clearly engages their right to privacy, and its permissibility depends on all of the circumstances of the case. The Colombian Constitutional Court has found that the use of a women's image by her previous employer on the employer's Facebook page, in the context in which she had previously given authorisation for the image to be used, was a violation of the woman's right to privacy, an element of which is the right to self-image.[175] The Court found that the employer's conduct violated the woman's fundamental rights and ordered the image to be taken offline. According to the Court, an authorisation to use someone's image cannot be so broad as to prevent the individual from understanding the scope of its consent. Even when there is an express authorisation, there can still be a violation of fundamental rights, because an authorisation does not entail a definite waiver of the right, and individuals have the right to change their mind.

A question remains as to whether journalists should publish images that individuals themselves have placed in the public domain, such as via Facebook. The temptation for media outlets to use publicly available images of individuals when ordinary persons fall into the public spotlight is considerable, and the acceptability of such use from the perspective of privacy is complex; it is unlikely that an individual would have contemplated or expected their image to be published in the mass media, but did they accept or consent to such a possibility when posting the image online.

Guidelines developed by the BBC[176] and Press Complaints Commission[177] encourage journalists to take privacy settings into account when deciding whether or not to publish a picture; that is, if someone has eschewed the various privacy settings available on social networks in favour of a closed or private account, they have a lower expectation of privacy as to the images published on that account.

---

[174] At p. 65.
[175] Constitutional Court Decision T-634/13
[176] BBC, Editorial Guidelines./
[177] Press Complaints Commission, Guidelines.

Balancing protection of personality with freedom of expression

To the extent that personality rights are more broadly encompassing than traditional understandings of the right to privacy, particularly with regards to the use and republication of images, their protection may give rise to conflicts with the enjoyment of freedom of expression, particularly in the context of artistic and creative expression. Limiting expression that disproportionately interferes with an individual's claim to "social respect and value", for example, may result in the curtailment of legitimate academic and creative publication and expression.

In order to develop principles to assist in balancing claims to the protection of personality, on the one hand, with freedom of expression concerns, on the other, we propose the following questions will be relevant:

- Is the person committing the relevant act of expression benefitting commercially from its publication?[178]
- Did they have the consent of the individual affected?
- The form of expression interfering with the individual's personality: was it written or verbal, did it include images or videos?
- What was the extent of publication: was it published on print or broadcast media or online commentary)?
- Who was the audience: readers of a newspaper or a blog, "Friends" on Facebook, family members at an event?
- Was the intention of the person making the relevant statement: to inform, expose, offend, or cause distress?
- Were there any particular aggravating factors, i.e. was a child involved?
- Was there a public interest, including the public's interest in artistic and creative fulfillment, in the relevant statement being published?
- What was the degree and extent of the harm to the individual's personality?
- What opportunities are there to mitigate the harm to the individual's personality?

Protection of personal data

Data protection rights are those which pertain to an individual's ability to make decisions about who has access to their personal data and how that data is used. The "important role played by the protection of personal data in the light of the fundamental right to respect for private life" has most recently been confirmed by the Court of Justice of the European Union in its October 2015 decision in *Schrems v Data Protection Commissioner of Ireland.*[179]

Personal data or information[180] has historically been approached, for instance, by the Human Rights Committee in its General Comment 16, as information "concerning a person's private

---

[178] In the seminal Canadian case of *Gould Estate v. Stoddart Publishing,*[178] the court distinguished between using the identity of a celebrity for endorsement purposes from the situation where the identity of the celebrity is the actual subject of the work (i.e. a biography). The courts should focus on if the portrayal of an individuals' image serves a social function (i.e. "public interest") valued by the protection of free speech (i.e. contributes information, which is not false or defamatory, to public debate or provides free expression of creative talent), noting that commercial exploitation of portrayals should never be permitted.

[179] Case C-362/14, Judgement of 8 Ocotber 2015, at [78].

[180] For the purposes of this paper, we treat these two terms as interchangeable, as they are used interchangeably in

life". However, with the advent in recent decades of "data protection law" – the body of regulation which controls the conditions under which private and public bodies can collect, process, store, and retain personal data – the definition of personal data has expanded to include any information relating to an identified or identifiable natural person, whether that information is relating to the person's private life or not. Thus, whereas the right to privacy generally protects information which is private, data protection concerns the protection of 'personal data' - i.e. data about a person - which may be both private or public. This is an important distinction, which presents serious difficulties in reconciling the protected interests where they diverge. This divergence is most obvious in the context of information which is already in the public domain.

Causes of action related to the protection of personal information fall into one of two categories; tortious or equitable actions in common law countries, which generally protect the disclosure or misuse of *private* information, and statutory causes of action grounded in data protection law, whose scope is generally broader.

Common law equitable actions and torts

- **Breach of confidence**: the common law equitable claim of breach of confidence arises when a duty of confidence exists, what is "when confidential information comes into the knowledge of a person, in circumstances where he has notice, or is held to have agreed that the information is confidential."[181] In British, Australian and New Zealand law, the original qualifying factor that the law only recognizes a duty of confidence in pre-existing relationships has now been dispensed with,[182] such that the appropriate test is now whether the person publishing the information knows or ought to know that there is a reasonable expectation that the information in question will be kept confidential.[183] Thus, in the seminal case of *Campbell v MGN*, the publication by the Daily Mirror of information about model Naomi Campbell's drug addition and attendance at Narcotics Anonymous meetings was a breach of confidence for which the applicant was entitled to receive damages.[184] The claim of breach of confidence was also substantiated by public figure Max Moseley when the *News of the World* published photographs, information and video of sexual acts in which Mr Moseley participated.[185] A subsequent application by Mr Moseley to the European Court in which he argued that the court's failure to impose a regime of prior disclosure in potential cases of breach of confidence was unanimously rejected, with the Strasbourg Courting finding sufficient protections were in place and that the damages awarded to Mr Moseley were adequate.[186]

- **Misuse of private information***:* A claim for breach of confidence is an equitable cause of action, not a claim in tort. In the UK, jurisprudential developments have seen the emergence of a tort of misuse of private information. In *OBG Ltd v Allan and Douglas v Hello!* the Court of Appeal described how breach of confidence now covers both confidential and private information, the latter of which "may be in the public domain,

---

European data protection law, and in fact personal data is defined to mean "any information […]"
[181] "The Spycatcher case", Attorney General –v- Guardian Newspapers [1999] 1AC 109.
[182] *Mosley v News Group* [2008] EWHC 1777 at [7].
[183] *Campbell v MGN* [2004] UKHL 22
[184] *Campbell v MGN* [2004] UKHL 22
[185] *Mosley v News Group Limited*, [2008] EWHC 1777 (QB)
[186] *Mosley v United Kingdom* [2011] 53 EHRR 30

and not qualify for protection as confidential, and yet qualify for protection on the grounds of privacy. Privacy can be invaded by further publication of information or photographs already disclosed to the public."[187] The existence of a self-standing tort of misuse of private information was confirmed in the recent case of *Vidal Hall and Ors v Google Inc.*[188]

- **Intrusion upon seclusion***:* this tort exists under both American law and the law of Ontario, Canada, which only recently recognized it. Under American law, the tort provides that "**o**ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person". Physical intrusions into a person's space will be sufficient to engage the tort, as will some other form of investigation or examination into an individual's private concerns, as by opening his private and personal mail, searching his safe or his wallet, etc. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the photograph or information outlined.[189]

  In *Jones v. Tsinge*, the Ontario Court of Appeal largely replicated the American tort for intrusion upon seclusion.[190] Here, the plaintiff and the defendant worked together at a bank and the plaintiff was in a relationship with the defendant's ex-husband. An action was brought after the plaintiff discovered the defendant had regularly accessed the plaintiff's banking information. The court sided with the plaintiff as the defendant's conduct met the criteria of being intentional; unlawful invasion of private affairs and highly offensive. The court also ruled that such an action must be deliberate and significant, and gave examples of categories for what could be considered "highly offensive" to invade: financial or health records; sexual practices and orientation; employment; and diary or private correspondence.

Data protection claims

For the large part, data protection laws do not create interferences or conflicts with the right to free expression, overwhelmingly pertaining to the manner in which private and public entities handle personal information they collect for business or governance purposes. However, in a number of circumstances data protection claims will compete against free expression interests. These include data protection claims with regard to the following:

- **Search results***:* the most visible and controversial application of data protection law in this regard has been in the context of search engine results responding to a search of an individual's name, which the European Court of Justice held in the *Google Spain*[191] decision constitutes the processing of personal data for the purpose of the Data Protection Directive.[192]

---

[187] [2008] 1 AC 1 Lord Nicholls, para 255.
[188] [2014] EWHC 13 (QB)
[189] Restatement of the Law, Second, Torts 652B
[190] Rahool Agarwal and Pamela Sidney, *Jones v. Tsige: Ontario Court of Appeal Recognizes Tort for the Invasion of Privacy*, 1 C.L.A.R. 2 (May 2012).
[191] Case C-131/12, judgment of 13 May 2014.
[192] ARTICLE 19, Right to Be Forgotten, 29 March 2016.

- **Large public or corporate datasets published in the name of transparency***:* A number of recent cases have concerned the publication of large datasets in the name of transparency. In Spain, the Spanish Audiencia Nacional (a special court with national jurisdiction over very specific issues) considered the publication of social security numbers within the scope of a trade union action, finding it an acceptable interference with data protection because it was aimed at denouncing a situation of unjustified privileges that disrupted the correct exercise of the union's rights.[193] In contrast, in an earlier decision the Audencia Nacional found that the publication by a company of information from the Commercial Registry about third parties, including information about their judicial proceedings, was a breach of the latter's data protection rights. The Audiencia Nacional considered (i) the aim of the publication (to provide information to companies willing to assess their risks when entering into commercial relationships); (ii) the fact that the information was easily accessible to a broad potential public at a reasonable price; and (iii) the fact that the information was not aimed at protecting the general interest.[194]

  In the recent ECtHR case of *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland,*[195] the Court applied the balancing test criteria elaborated in *Axel Springer* and others in considering whether the domestic court's decision preventing the publication of taxation data on 1.2 million Finnish residents on data protection grounds was an unjustifiable interference with Article 10 rights. The Court found that the publication of the taxation data by the respondent, Satamedia, was an act of data processing to which data protection law applied, not a journalistic activity which would fall within journalistic exemptions to data protection law. Of particular importance was the extent of the data published, not its private nature nor that it was inaccurate; the publication of personal information to such an extent could not be considered as journalism, but as processing personal data. The case has now been referred to the Grand Chamber of the European Court.

- **Browser-generated information, such as cookies***:* in the recent UK case of *Google v Vidal-Hall,*[196] the English Court of Appeal found that the collection by Google of "browser-generated information" (BGI) was an act of data processing because BGI amounts to personal data, despite it being anonymous information. The Court of Appeal found that because BGI "individuates" the individual, by ensuring that the individual is able to be differentiated from others, it amounts to personal data, despite the data not revealing information such as the actual name of the individual. It also rejected Google's argument that that because Google would never in practice actually identify individuals by aggregating their BGI with other information, the claim should fail.

- **Photographs taken in public spaces***:* in September 2014, the Singapore Personal Data Protection Commission released guidelines on the application of Personal Data Protection Act to photography.[197] Unless exceptions apply, consent is required for the collection, use or disclosure of photos as photos are treated as personal data. Professional photographers (or their organization) taking photos of individuals in the course of business will need to

[193] Decision dated 3 December 2013
[194] Decision dated 16 March 2006
[195] App. No. 931/13, 21 July 2015.
[196] *Google v Vidal-Hall* [2015] EWCA Civ 311
197 Advisory Guidelines On The Personal Data Protection Act For Selected Topics – Chapter 9, Photography

obtain consent. Similarly, where a photographer submits a photo for a competition, it is likely that consent of the person within the photo will also be required. For photos taken in public places, while they would typically constitute collection of personal data that is publicly available (and thus exempted from the requirement to obtain consent), the Guidelines did clarify that there can be "private spaces within public spaces" and the mere fact that members of the public may look into the premises does not make it public.

The law in other countries is not as clear. The UK's Information Commissioner's Office has not issued unambiguous guidance on the question of photography, stating only in its publication *Data protection and journalism: a guide for the media* that images can amount to personal data, and if such personal data is capable of identifying an individual – which most photographs are prone to do – it will fall within the ambit of data protection legislation.[198] The Article 29 Working Party – the committee of European data protection authorities – has similarly refrained from issuing authoritative guidance on the question of photographs.

Under UK common law, the publication of photographs taken without consent in a public place does not automatically amount to a breach of confidence: in *Campbell v Mirror Group Newspapers Limited.*[199]

New challenges in the context of the Internet

- **Deliberate disclosures of personal information and "doxing"***:* As with revenge porn, the deliberate and often malicious disclosure of personal information (including addresses, phone numbers or credit card details) is becoming an increasingly frequent feature of discourses on the regulation of online content. The use of such techniques, known as "doxing", is commonly associated with acts of revenge or vigilante justice, although it arguably encapsulates some elements of citizen journalism and investigation into government corruption. In China, for instance, the term "human search flesh engine" is used to describe the phenomena whereby internet users collectively research and disclose information online in response to a particular event or allegation. The "human search flesh engine" has been responsible for disclosing the identity of women who killed a kitten on a video and a Communist official in China's central Shaanxi province who was spotted smiling at the scene of a deadly traffic accident, but it has also gone after ordinary persons in clear acts of harassment and abuse.[200]

  Doxing is a challenging phenomena to rationalise from the perspectives of freedom of expression and privacy; on the one hand, it is often connected to the collation and publication of information that is already available on the internet, so doesn't always strictly involved the use of purely private information. It can also play a role in exposing corruption in the private or public sectors, by identifying the perpetrators of particular acts or expositing corrupt companies' beneficial ownership, as some argue has been the case with respect to the "human flesh search engine."[201]

---

[198] CO, *Data protection and journalism: a guide for the media*.
[199] [2004] UKHL 22
[200] Celia Hatton, China's internet vigilantes and the 'human flesh search engine, *BBC News*, 28 January 2014.
[201] Wang, Fei-Yue; Zeng, Daniel; Hendler, James A.; Zhang, Qingpeng; Feng, Zhuo; Gao, Yanqing; Wang, Hui; Lai, Guanpi (August 2010). "A Study of the Human Flesh Search Engine: Crowd-Powered Expansion of Online Knowledge". *Computer* (IEEE Computer Society) 43 (8): 45–53.

At the same time, from a privacy perspective, the extent to which individuals realise and genuinely consent to their personal data being collected and retained online remains a serious question. Moreover, doxing, as distinct from the accidental or incidental disclosure of personal information, often appears to be clearly targeted at impeding an individuals' enjoyment of their right to privacy, particularly when that individual is not a public figure and their actions have not warranted them being in the public sphere.[202] In a notorious example of malicious doxing, for example, video-game engineer Zoe Quinn had her personal information posted online by anonymous hackers in response to a scandal related to the ethics of the gaming industry, known as "Gamergate".[203]

- **Open data***:* the right to freedom of expression and access to information requires the State to collect, retain and make available to the public data which may include the personal information of individual citizens, including data on court judgments, taxation records, census data records of elections, beneficial and corporate ownership, and historical archives. This duty relates not only to the State's obligation to facilitate public participation and government transparency and accountability through access to information, but also to the role of such access in facilitating the right to truth – both in the collective right of a society to access information essential to the workings of a democratic society, and the right of individual victims and their families to know of and seek redress for serious violations of human rights.[204] The set of principles for the protection and promotion of human rights through action to combat impunity, updated in 2005, emphasises the role that the preservation and facilitation of access to archives (principles 14 and 15) plays in facilitating the right to truth.[205]

  There is emerging recognition that the State's responsibility to provide access to information includes and obligation to "open" up as much data as possible, and make such data readable, accessible and analysable by the public at large. For example, the Open Government Partnership was launched in 2011 and promotes the growth of open government, particularly through the use of the internet and new technologies. The US, Japan, Kenya, the UK and Ghana, for example, have all launched open data initiatives in the past few years.

  The potential for conflict between free expression and privacy in this context is clear. On the one hand, the State is charged with collecting and maintaining records to facilitate accountability of public institutions and facilitate the right to truth. Doing so, on the other hand, entails interferences with the right to privacy of every individual whose information is collected and retained, and creates risks that such personal data might be used for alternative, and potentially malicious, purposes.

  Although all acts of State collection and storage of personal information will amount to an interference, that inference will often be justified by reference to a legitimate interest, including the promotion of the public interest in maintaining records and the delivery of

[202] In contrast to, for example, the publication of the identity of the inventor of Bitcoin, Satoshi Nakamoto, by *Newsweek* journalist Leah McGrath, an act which users on Reddit considered doxing.
[203] Caitlin Dewey, The only guide to Gamergate you will ever need to read, *The Washington Post*, 14 October 2014.
[204] Inter-American Commission on Human Rights, *Lucio Parada Cea and others v. El Salvador*, Report No. 1/99, Case 10.480, 27 January 1999, para. 151.
[205] E/CN.4/2005/102/Add.1 8 February 2005

public services. Activities such as the maintenance of census records, taxation records and records of court judgments would be necessary to achieve these aims and proportionate in a democratic society. Data protection law provides an exemption for the maintenance of personal information for pursue historical purposes provided appropriate safeguards are in place, including the prohibition of any use of the data in support of measures or decisions regarding any particular individual.[206]

In relation to the collection and retention of the data in pursuit of the objective of the prevention and detection of crime, the ECtHR has held that the demands of the right to privacy do not prevent governments from maintaining databases of sexual offenders, which databases can be accessed by courts, police and administrative authorities, provided that appropriate safeguards are in place, including the possibility for applicants to apply for deletion of data, and access to the data is subject to a duty of confidentiality and is restricted to precisely determined circumstances.[207] However, the maintenance of a database of DNA samples which includes samples on individuals who have never been charged with or convicted of a crime is a disproportionate interference with the right to privacy.[208] Entry onto a database which results in serious implications for the affected individual without prior independent authorisation of the measure will also fail to satisfy the requirements of human rights law; in *Albanese v Italy*,[209] for example, the European Court held that the entrance without judicial review of the applicant's name onto a bankruptcy database which resulted in his automatic disqualification from participation in electoral processes for a period of five years was not necessary in a democratic society.

Information in the possession of State authorities is properly subject to access requests by members of the public; as the Special Rapporteur on freedom of expression noted in a 2000 report, "all public bodies should be required to establish open, accessible internal systems for ensuring the public's right to receive information."[210] ARTICLE 19 has written at length on the contours of the obligation to provide access to information, and in 1999 published *The public's right to know: Principles on Freedom of Information Legislation.*[211] It is a generally agreed tenet that the provision of access to information may be attenuated by concerns about privacy and that access may be curtailed to ensure the protection of information about an individual's private life. However, the application of this principle is increasingly challenging in the current context, particularly as understandings evolve as to what constitutes private information and how isolated pieces of personal data might be used with adverse effects on an individual.[212] At the same time, in the context of government resistance to greater accountability, privacy exemptions are often exploited and over-used to prevent public access to information.

Two US decisions reveal how courts there have struggled to strike the balance in the context of access to information. The US Court of Appeals in Atlanta (11th Cir.) ruled that the public has a right to the addresses of recipients of federal disaster relief funds issued by the Federal Emergency Management Agency following several hurricanes in

---

[206] Data Protection Directive 95/46/EC, Article 6.
[207] *B.B. v. France* (App. no. 5335/06), *Gardel v France* (App. no. 16428/05), *M.B. v. France* (App. no. 22115/05), judgements of 17 December 2009.
[208] *S v Marper* [2008] ECHR 1581
[209] 77924/01, judgement of 23 March 2006.
[210] E/CN.4/2000/63
[211] ARTICLE 19, The Public's Right to Know Principles on Freedom of Information Legislation, June 1999.
[212] Such as subscriber data – see *R v Spencer* [2014] 2 SCR 212.

Florida in 2004. However, the Court ordered that the names of those individuals be protected, as release would violate their personal privacy rights.[213] This is arguably a meaningless distinction, and increasingly so in the era of powerful data analysis technologies and Google Maps. Recognition of this fact seems to have been given by the US Court of Appeals in Denver (10th Cir.) decision in 2005 in which it refused to order the release of electronic maps from FEMA. The Court held the electronic information could be manipulated to reveal flood insurance policy holders' names, addresses, flood risk and insurance information.[214]

Some government employees or public figure have sought to render information exempt from access to information requests through the use of a private email account. The case of Sarah Palin's emails is apposite; in 2008 a group of journalists applied for access to the then Governor of Alaska's emails. After three years, and due to the use by Palin of personal email accounts for government business, 11,000 emails were disclosed, almost 1,000 were held back, and information was redacted from 2,300 emails.[215]

A further conflict in this area is the emergence of beneficial ownership disclosure laws, in which companies are required to record their beneficial owners in a public central registry maintained by the government. Such laws will come into force in the UK in 2016, for example, and an estimated 3,190,000 UK companies will need to register their beneficial owners.[216] The UK law builds on and responds to the adoption by the European Union in June 2015 of the Fourth EU Anti-Money Laundering Directive introducing a central UBO-register, a public register which identifies the ultimate beneficial owners (UBOs) of companies and trusts. There have previously been multiple efforts to introduce similar legislation in the United States Congress and Senate, though such efforts have failed.

Although there are certainly implications for the privacy of company owners, this is arguably a field in which there is a clear need to prioritise access to information over privacy concerns. The impact of greater transparency in this field on public accountability, corruption and transparency in fiscal and political processes is overwhelmingly necessary to justify any correlative interference with privacy. Nevertheless, the form in which such information is made accessible to the public will continue to be relevant from the perspective of privacy; the written publication in full of beneficial ownership records in a newspaper, for example, may have a different impact on privacy than the existence of a database accessible to the public, particularly after the decision in *Satakunnan Markkinaporssi Oy and Satamedia Oy v Finland.*[217]

---

[213] *News-Press v. U.S. Dept. of Homeland Sec.*, 489 F.3d 1173 (11th Cir. 2007).
[214] *Forest Guardians v. Fed. Emergency Mgmt. Agency*, 410 F. 3d 1214 (10th Cir. 2005).
[215] David A Fahrenthold, "Sarah Palin emails: What was redacted?", *The Washington Post,* 10 June 2011, available at https://www.washingtonpost.com/politics/sarah-palin-e-mails-what-was-redacted/2011/06/10/AGC9D9OH_story.html.
[216] Alexandra Wrage, "Ownership of Privately-held Companies: Privacy v Transparency," *Forbes*, 18 August 2015, available at http://www.forbes.com/sites/alexandrawrage/2015/08/18/ownership-of-privately-held-companies-privacy-versus-transparency/
[217] App. No. 931/13, 21 July 2015.

Balancing protection of personal data with freedom of expression

Claims regarding the protection of personal information confound traditional understandings of privacy because they can apply to information that is already in the public domain, or in any event which is not "confidential". In this sense, they may give rise to particular conflicts with freedom of expression, which is grounded in the free flow and public dissemination of information. They also disregard traditional notions of public and private space, and legitimate expectation of privacy, which have long acted as touchstones when balancing privacy with freedom of expression.

In order to develop principles to assist in balancing claims to the protection of personal information, on the one hand, with freedom of expression concerns, on the other, we propose the following questions will be relevant:

- What was the character of the personal information in question? (i.e. contact information, sensitive data, etc)
- What was the intention of the person publishing or disclosing the personal information? Was there a public interest at stake?
- In what form and to whom had the personal information be made available?
- What was the degree and extent of the harm to the individual's privacy?
- What opportunities are there to mitigate the harm to the individual's privacy?

Sanctions and remedies for privacy violations

Some serious threats to freedom of expression and access to information are levied by courts and legislatures in their attempts to prevent and remedy privacy violations. Authority, particularly from the European Court of Human Rights, holds that sanctions and remedies for privacy violations will be legitimate when lawful, necessary and proportionate, with proportionality requiring a consideration of all of the circumstances of the case. However, particular sanctions and remedies have greater implications for freedom of expression than others, and some have such a wide-ranging and serious chilling effect that they can arguably never cross the proportionality threshold. Here, we seek to set out an exhaustive list of the types of sanctions and remedies imposed in response to violations and illustrate their impact on freedom of expression.

Pecuniary penalties and the compelled publication or retraction of statements

In the context of civil actions for defamation, breach of confidence and misuse of private information, and statutory data protection claims, the most common penalties levied by courts include the imposition of monetary penalties. Often, there will also be a requirement for the compelled publication of statements (such as an apology, or a copy of a court judgment) or retractions. From the perspective of privacy, such remedies may be an essential means of deterring further infractions and, particularly in the context of data protection, altering business practices to ensure future compliance.

However, particularly when imposed on the media or content providers, neither of these penalties are insignificant, given the potential chilling effect they could have on future reporting, and will only be viewed as necessary when the intrusion into the right to privacy is sufficiently serious, and in consideration of all of the circumstances.

The definitive position of the European Court in relation to pecuniary penalties is that

Although the penalty imposed on the author did not strictly speaking prevent him from expressing himself, it nonetheless amounted to a kind of censure, which would be likely to discourage him from making criticism of that kind again in future [...]. In the context of the political debate such a sentence would be likely to deter journalists from contributing to public discussion of issues affecting the life of the community. By the same token, a sanction such as this is liable to hamper the press in performing its tasks as purveyor of information and public watchdog.[218]

In *Couderc,* in which the sanction of EUR 50,000 and an order compelling the publication of statement detailing the judgment was held to be not "insignificant" the Court emphasised that:

> In the context of assessing proportionality, irrespective of whether or not the sanction imposed was a minor one, what matters is the very fact of judgment being given against the person concerned, including where such a ruling is solely civil in nature. Any undue restriction on freedom of expression effectively entails a risk of obstructing or paralysing future media coverage of similar questions."

In some cases, unsuccessful defendants in defamation or breach of confidence suits will be ordered to pay "success fees", where a litigant has entered into an arrangement with their legal counsel as to the payment of legal fees on success of the case, in circumstances in which those fees are considerably higher than base legal costs. Such a penalty is clearly an interference with Article 10 rights, one which pits the role of the press in engaging of matters of public concern against the need to ensure individuals have effective access to courts. Although the interference with Article 10 rights occasioned by success fee arrangements can be justified as necessary in a democratic society, it will not meet proportionality requirements where the relevant scheme is seriously flawed, as was the case with respect to the Conditional Fee Agreement scheme in the UK which gave rise to the case of *MGN Limited v the United Kingdom*.[219]

Prior restraint and prior notice

Under American law, the placement of prior restraints on the publication of material, either by government regulation or a court-issued injunction, will almost always constitute a violation of First Amendment free expression rights. Prior restraints are viewed by the U.S. Supreme Court as "the most serious and the least tolerable infringement on First Amendment rights," according to the Court's 1976 opinion in *Nebraska Press Association v. Stuart*.[220] In Ireland, there is also a strong presumption against the constitutional validity of a prior restraint prior to a final decision on the merits of the case.[221]

However, the European Court has not gone so far as to conclude that Article 10 would prohibit States from imposing prior restraints. Rather, it has said: [222]

> While Article 10 does not prohibit the imposition of prior restraints on publication, the dangers inherent in prior restraints are such that they call for the most careful scrutiny on

---

[218] *Lingens v. Austria*, App. No. 9815/82, judgment of 8 July 1986
[219] App. no. 29401/04, judgement of 18 January 2011 at [151].
[220] 427 U.S. 539, 559 (1976)
[221] *Bonnard v Perryman* [1891] 2 Ch 269
[222] *Mosley v the United Kingdom,* App. No. 48009/08, judgment of 10 May 2011, at [117].

> the part of the Court. This is especially so as far as the press is concerned, for news is a perishable commodity and to delay its publication, even for a short period, may well deprive it of all its value and interest. The Court would, however, observe that prior restraints may be more readily justified in cases which demonstrate no pressing need for immediate publication and in which there is no obvious contribution to a debate of general public interest.

In the seminal case of *Mosley v United Kingdom*, the applicant contended that media outlets should be required to notify individuals prior to publishing material about them, which would engage their right to privacy under Article 8. The rationale behind such an obligation was that in some cases damages would be inadequate to rectify the harm caused; in the case of *Moseley,* the domestic judge awarding Mr Moseley damages noted that "no amount of damages can fully compensate the Claimant for the damage done. He is hardly exaggerating when he says that his life was ruined. What can be achieved by a monetary award in the circumstances is limited."[223]

Mr Moseley applied to the European Court, arguing that the UK's positive obligations under Article 8 necessitated the imposition of a legislative requirement for prior notification. The Court considered both the margin of appreciation granted to the State in this regard, and the proposal put forward by the applicant. In respect of the former, the Court took into consideration that the UK "has chosen to put in place a system for balancing the competing rights and interests which excludes a pre-notification requirement", and that a parliamentary committee had recently considered and rejected the instigation of a prior notification requirement.[224] The Court also noted the absence of a European consensus as far as a pre-notification requirement is concerned. It concluded that, "having regard to the chilling effect to which a pre-notification requirement risks giving rise, to the significant doubts as to the effectiveness of any pre-notification requirement and to the wide margin of appreciation in this area" Article 8 does not require a legally binding prior notification requirement.[225]

Criminal prosecution

The prospect of criminal prosecution for the exercise of freedom of expression that infringes privacy rights may, in certain circumstances, be so severe as to impede the essence of the right. There is general consensus among international bodies, therefore, that criminal defamation laws are incompatible with human rights and should be abolished. In a 2002 joint statement, 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 declared that "[c]riminal defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws."[226] The ECtHR has refrained from so explicitly condemning criminal defamation laws, although the Court's reasoning suggests such laws may be necessary by reference to the interest of protecting public order rather than safeguarding the privacy and reputational rights of others.[227] Defamation remains a crime in a number of countries; for example, in Canada, defamatory libel is a crime in the Criminal Code punishable by up to five years in prison. In Colombia, dishonouring or falsely attributing

---

[223] *Mosley v News Group* [2008] EWHC 1777 at [236].
[224] *Mosley v the United Kingdom,* App. No. 48009/08, judgment of 10 May 2011, at [122].
[225] *Ibid.* para 132.
[226] The 2002 Joint Declaration of Special Mandates.
[227] *Castells v Spain* (1992) 14 EHRR 445

criminal conduct to another person can result in the offender's imprisonment for up to four years. Crimes related to the protection of honour and reputation are also to be found in the penal codes of many countries around the world (as explored above).

Other privacy violations are criminalised in some jurisdictions, such as:

- In France, Article 226-1 of the French Criminal Code criminalises the capture, recording and transmission of the image of a person in a private place without their consent, and Article 226-2 criminalises the archiving and direct or indirect broadcasting to the public or to a third party of a person's image and words obtained without their consent.
- Also in France, the offence of "happy-slapping", whereby a victim's image is captured while an assault is being committed and the evidence is broadcasted to the public, is criminalised in Article 222-3 of the Criminal Code.
- In Hong Kong, a new criminal offence was created in 2012 under section 64 of the Personal Data Protection Ordinance prohibiting data users from disclosing personal data, without the consent of the data subject, if made with the intention of gaining or causing loss or psychological harm to the data subject, attracting custodial sentences of up to five years.
- In September 2015, Clause 253 of China's Criminal Law was amended to include a crime of selling or providing to others citizen's personal information in serious situations, with a penalty of up to three years in prison, and if the situation is especially serious, up to seven years imprisonment can be imposed.
- Under Peruvian law, the crime of illegal commercialisation of personal data is committed when someone illegally commercialises or sells non-public information related to any part of the personal, family, patrimonial, working, financial or other similar sphere of a natural person.
- A Bill is currently under consideration in the Philippines that would criminalise cyberbullying, or the act of posting rude, offensive or insulting messages against an individual on the Internet.

Under international law, however, there is no clear guidance as to the proportionality of criminal sanctions for the protection of privacy rights.

Protection orders

One response to the increasing occurrence of online harassment and bullying is the creation of legal remedies in the form of protection orders, similar to that available in many jurisdictions regarding domestic violence. A number of jurisdictions have adopted legislation enabling individuals to obtain protection orders against those subjecting them to harassment online. For example, in 2011 South Africa adopted the Protection from Harassment Act, which enables protection orders to be granted where an individual is subject to "verbal, electronic or any other communication" which "causes harms or inspires the reasonable belief that harm may be caused to the complainant". Criminal penalties apply to those who fail to comply with the Act.

The implication of the Act for freedom of expression has recently been put to the test in the case of *Hofmeyr v Koch*, which involved statements made about actor Steve Hofmeyr by a Twitter account run by comedian Conrad Koch in the name of his ventriloquist puppet, Chester Missing. Hofmeyr obtained an interim protection order against Koch under the Protection from Harassment Act. In reviewing the decision of the Magistrates Court to issue the order, the Constitutional Court found that, in the circumstances, Koch's comments – which responded to racist tweets published by Hofmeyr – were "protected comment" and

"legitimate public engagement... deserving of the same protection in terms of the Constitution."[228]

Imposition of liability on Internet intermediaries

With increasing frequency, sanctions or remedies in response to privacy violations are taking the form of the imposition of liability on third party service providers.

- **Liability for unlawful content***:* A number of countries, such as Thailand and China, require internet intermediaries to effectively monitor and moderate content. In other countries, including Europe and to a lesser extent the US, internet intermediaries may be held liable for third-party content it if they fail to act expeditiously to remove it upon obtaining actual knowledge of its illegality (also known as notice-and-takedown). The operation of such liability schemes and their compliance with international human rights law have been examined at length by ARTICLE 19 in *Internet intermediaries: Dilemma of liability*[229] and will not be explored at length here, except to reiterate that all forms of intermediary liability create serious concerns from the perspective of freedom of expression. To the extent that take down notices constitute a form of censorship it is difficult to imagine how they might be a proportionate response to interferences with the right to privacy in the absence of adequate procedural safeguards.

  While many international standards support Internet intermediaries' immunity from liability as a basic tenet of the protection of freedom of expression online,[230] the most recent case on this issue from the European Court of Human Rights is a cause for concern. The case concerned "a large professionally managed Internet news portal run on a commercial basis which published news articles of its own and invited its readers to comment on them" and its application should be restricted to like actors and platforms. Remarks were published in the comments section of the website that were prima facie unlawful (defamatory and amounting to hate speech) by individuals whose identity was unknown to the platform provider. The provider argued that domestic regulations applying to media publishers were not applicable to it as regards third-party comments, for which it was a mere intermediary (an "Internet portal" in Estonian law). The domestic court disagreed, finding that the platform qualified as both a media publisher and an Internet portal because of the platform's economic interest in publishing the comments. The Strasbourg Court found nothing fundamentally wrong with the domestic court's analysis, it being within the margin of appreciation for States to legislate in this field, and found that the domestic court having applied the domestic legislation correctly.

  In order to resolve the question whether the domestic court's decisions holding the company liable for third parties' comments posted were in breach of its Article 10 rights, the Grand Chamber identified the following aspects as relevant for its analysis: the context of the comments, the measures applied by the applicant company in order to prevent or remove defamatory comments, the liability of the actual authors of the comments as an alternative to the applicant company's liability, and the consequences of the domestic proceedings for the applicant company. In conducting this analysis, the

---

[228] Philippa Marques, Court protects freedom of expression in Steve Hofmeyr Twitter battle, *The Write Candidate,* 5 November 2015.
[229] ARTICLE 19, Dilemma of Liability, 2013.
[230] The 2011 Report of the SR on FOE, *op.cit.*, paras. 74-77.

Court focused on the failure of the company to properly moderate comments in order to expeditiously respond to and remove comments amounting to hate speech, and the failure of the company to ensure a realistic prospect of the authors of such comments being held liable. Importantly, the Court found that because the company had not put in place measures to ensure the identity of commentators could be ascertained in order to provide remedies for potential future victims of hate speech, they assumed liability for those comments themselves [151]. The *Delfi* case can thus be read as deterring news sites from enabling their users to anonymously comment on their services lest they are held liable for any potential future unlawful acts of expression. This is very concerning not only from the perspective of freedom of expression, but also from the perspective of privacy, which underpins the right to remain anonymous online.[231]

- **Delinking search results***:* A more discreet but still concerning form of internet intermediary liability is the obligation of service providers to respond to user requests to delink search results from a search containing their name. The obligation to delink is often (mis)labelled the right to be forgotten or the right to erasure, although it does not involve the removal of content but rather the de-identification of content as being related to a particular person. Arising out of the 2014 decision of the Court of Justice of the European Union in *Google Spain v Mario Costeja González,*[232] the obligation to delink search results responds to increasing recognition that:

> The inclusion in the list of results, displayed following a search made on the basis of a person's name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information,[and therefore] is liable to constitute a more significant interference with the data subject's fundamental right to privacy than the publication on the web page itself.

As a result, search engines must respond to requests from individuals to remove a link from a list of search results where a search is made on the basis of a person's name, provided the individual can show that the data displayed by the search engine are inadequate, irrelevant or excessive in relation to purpose for which the search engine is processing the data, or is not kept up to date or is kept for longer than is necessary to be kept for historical statistical or scientific purposes. Furthermore, under the General Data Protection Regulation, failure to erase links in circumstances where they should have erased them will result in considerable fines.[233]

The emergence of the obligation to delink from search results has created considerable controversy and ignited a vigorous battle between privacy and free expression advocates. ARTICLE 19 has written at length on the drawbacks posed by the so called "right to be forgotten" for free expression and access to information, and this paper will not further contribute to that debate, other than to note that the *Google Spain* decision is providing cover for the extension of even more invasive forms of intermediary liability in other countries. The example of Brazil is apposite: the parliament is currently considering Bill PL215, which contains provisions which its authors state are an attempt to replicate the

[231] Case comment on the Grand Chamber decision in Delfi.
[232] C-131/12, judgment of 13 May 2014
[233] For more details on the impact of the draft General Data Protection Regulation on Freedom of Expression, see Daphne Keller, *The Final Draft of Europe's 'Right to be Forgotten' Law*, 17 December 2015.

European decision in Brazil. Yet the provisions of PL215 go considerably further, in the words of the Electronic Frontiers Foundation, giving "the courts a blanket ability to require any site to take down content, using the vaguest of justification, and with no requirement to take into account current public interest, newsworthiness, critical review, or the need for an accurate historical record. There's no process for the decision to be challenged, no put-back process, no requirement that the deletion be minimized, nor any assurance that erroneous or malicious deletion requests be penalized."[234]

- **Linking liability***:* in addition to the question of linked search results, there is also emerging attempts to place "linking liability" on an individual using hyperlinks to link related material that may contain defamatory or other speech that constitutes an interference with privacy. The use of hyperlinks has given rise to a considerable amount of litigation over the past decade, mainly in the context of defamation and copyright infringement claims.[235] In addition, several cases have addressed the question of criminal liability for linking to a site containing illegal content; in the *Radikal* case,[236] for example, the defendant was prosecuted for having provided a link to an online magazine that was banned in the Federal Republic of Germany, on the basis that the magazine had published guidance on how to sabotage railway lines. Ultimately, the prosecution failed because the defendant had created the link before the article in question was published. In particular, the court found that the defendant could not be found guilty for failing regularly to check the content of the online publication.

  Arguably, as is the case under British law, an individual should not be held liable for words published on a hyperlinked website, whether or not they had been notified of the defamatory or other nature of those words.[237] As ARTICLE 19 has argued elsewhere, hyperlinks are arguably a reference, which readers are free to follow or note, and individuals will not always not the entirety of the content to which they are linking nor be able to know the content of a website that can change over time.[238] Nevertheless, the European Court has previously upheld the decision of the Swiss domestic courts to prevent the publication of a poster which contained a link to a website containing unlawful material.[239] Although in that case the material was not related to the right to privacy, many other linking liability cases are to the extent that the hyperlink provided take the reader to material which impact upon a person's reputation.[240]

- **Compelled disconnection of Internet access***:* A final serious interference with freedom of expression emerging in the context of the protection of privacy rights is the compelled disconnection of Internet access. Under the Nova Scotia Cyber Safety Act, for example, if a judge is satisfied on the balance of probabilities that there are reasonable grounds to issue a protection order, they can make an order, inter alia, disconnecting the respondent's internet access, pursuant to section 9(1) of the Act. It is difficult to see how such a measure could be a proportionate response to even the most serious of privacy violations. Restricting access to the internet and to a particular technological device are

---

[234] EFF, Brazil's Politicians Aim to Add Mandatory Real Names, *op.cit*.
[235] For an overview of US cases, see for example Mark Sableman, Link Law Revisited: Internet Linking Law at Five Years (2001)/
[236] Amstgericht Berlin-Tiergarten, June 30, 1977, MMR, 1998/1, p. 49, note St. Htftig.
[237] *Design Technica Corporation v Google UK Ltd and Ors* [2009] EWHC 1765 (QB)1
[238] Intervenors brief in Mouvement Ralien Suisse v Switzerland, 2011.
[239] *Mouvement Ralien Suisse v Switzerland*, App. No. 16354/06, judgement of September 2011.
[240] See, for example, *Crookes v Wikimedia Foundation*, 2008 BCSC 1424.

punitive measures that have the simultaneous effect of limiting access to information and preventing the free expression of ideas, access to education, as well as the freedom to associate.

Balancing privacy and freedom of expression in the context of sanctions and remedies

In order to develop principles to assist in balancing claims to the protection of privacy, on the one hand, with freedom of expression concerns, on the other, we propose the following questions will be relevant to the proportionality of sanctions and remedies:

- What was the severity of the privacy violation for which remedies and sanctions are being sought?
- Did the privacy violation occur on the Internet, and if so what was its scope and reach?
- Can the privacy violation be effectively remedied due to its nature, or will compensation have to suffice?
- To whom will the proposed sanction/remedy be directed, and whom will it affect?
- What will be its temporal and geographic impact?
- What will be the medium primarily affected by the sanction/remedy?
- What might be the perverse impacts of the imposition of the sanction/remedy (e.g. its manipulation by others, chilling effect, etc) ?