INFORMATIONAL PRIVACY IN THE DIGITAL AGE

A Proposal to Update General Comment 16 (Right to Privacy) to the International Covenant on Civil and Political Rights

A Report by the American Civil Liberties Union

Photo: Maksim Kabakou/Shutterstock

February 2015

ACLU
AMERICAN CIVIL LIBERTIES UNION

Informational Privacy in the Digital Age

A Proposal to Update General Comment 16
(Right to Privacy) to the International Covenant
on Civil and Political Rights

A Report by the American Civil Liberties Union

Acknowledgments:

This report has been informed by research from
Oxford Pro Bono Publico of the Faculty of Law, University of Oxford

American Civil Liberties Union
125 Broad Street
New York, NY 10004
www.aclu.org

Contents

Executive Summary

The right to informational privacy has long been recognized in international law. Yet the combination of rapidly evolving digital technologies, expanding use of those technologies by people all over the world, and aggressive collection of personal information by many States has led to a substantial and rapid erosion of privacy rights—especially rights in one's personal information. In light of these developments, there is an urgent need for the United Nations Human Rights Committee to provide authoritative guidance on the nature and scope of privacy protections under Article 17. The principles that should inform such guidance lie close at hand—in the Committee's own commentaries and practice, the laws and practices of States, and the work of regional and UN human rights bodies. Together, these principles point the way towards a promising international platform for privacy protection that is at once modern and capable of securing the fundamental privacy interests that global citizens have always possessed.

The Time is Ripe to Update General Comment 16

The Human Rights Committee has superseded or supplemented existing General Comments where necessary to develop the content of protected rights, and to reflect changing realities. Updating General Comment 16 is necessary to ensure the ongoing relevance of the ICCPR in a rapidly changing world. The Internet has emerged as the world's primary platform for global communication. Sophisticated modern technologies have enabled States and private parties to encroach on informational privacy rights—both massively and cheaply—through the acquisition, retention, dissemination, and use of publicly available and private data. In an era of mass surveillance, concrete guidance on the circumstances under which States may legitimately interfere with informational privacy is required. Moreover, technological developments have raised questions as to what constitutes an "interference" in this context (given, for example, that modern technologies now enable States Parties and corporations to collect, store, and synthesize information in ways and on a scale unimaginable when General Comment 16 was drafted in the 1980's).

An update to the General Comment—in the form of a new Comment or an update to the existing Comment 16—would also reflect and incorporate developments in the law. There is a symbiotic relationship between data protection in the context of privacy rights and the freedoms of expression and association, the right to counsel, and other rights guaranteed by the ICCPR. The Human Rights Committee has also made determinations on individual petitions and issued Concluding Observations on Article 17 as it pertains to informational privacy. These and other relevant developments should be assimilated into a new General Comment or a comprehensive update to General Comment 16.

International Human Rights Law Requirements for Interferences with the Right to Privacy

Article 17 prohibits "unlawful or arbitrary" interferences with the right to privacy, and General Comment 16 provides important guidance on these terms.

In short, any interference with informational privacy must be:

a. Carried out pursuant to the requirements of domestic and international law, including the provisions, aims and objectives of the ICCPR;
b. Authorized by laws that the public can fully access, and that are precise, specific, and clearly defined such that an impacted individual can foresee any interference;
c. Necessary for and proportionate to the pursuit of legitimate State aims, such as law enforcement or national security;
d. Minimally intrusive of protected privacy interests, and in any event, never so invasive as to impair the essence of the right.

As Edward Snowden's recent revelations have shown, modern surveillance technologies have an especially far-reaching effect on privacy rights, and in particular, on informational privacy rights. At minimum, an update to General Comment 16 is necessary to reaffirm the continued relevance of human rights principles to current surveillance practices, making clear that:

a. Indiscriminate mass surveillance, including mass collection and retention of data, violates Article 17 because it is an unlawful and typically arbitrary interference with informational privacy;
b. Both metadata and communications content may trigger the protections of Article 17
c. Any interference with informational privacy should be subject to independent and effective oversight;
d. In relation to privacy rights, it is control over communications or relevant infrastructure, not custody of the person, that is the touchstone of State responsibility;
e. Laws on privacy and surveillance must not be discriminatory, and in particular, must not distinguish between people simply on the grounds of nationality; instead, differential treatment is only permissible when based also on acceptable grounds under the Covenant, and when there is a reasonable, objective purpose for drawing the distinction, and doing so supports a legitimate aim; and
f. States Parties have affirmative obligations to protect informational privacy from interference by private parties and other States, and to ensure effective remedies for victims of privacy breaches.

Why Update the General Comment on Privacy?

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) protects all persons from arbitrary or unlawful interferences with their "privacy, family, home or correspondence." In 1988, the Human Rights Committee ("Committee") issued General Comment 16, interpreting Article 17. As the Committee (and many others) have noted, the right to privacy encompasses a diverse range of important interests, such as bodily privacy (including reproductive rights and bodily integrity), territorial privacy (including limits on searches of one's property), privacy about the nature of one's personal relationships (including sexual orientation), protection of one's reputation, and the privacy of one's communications and personal data.

These dimensions of the right to privacy are as important as they are diverse, and recent developments have radically affected some while leaving others more or less untouched. Many long-standing principles governing the right to privacy that are reflected in General Comment 16 remain applicable today, while others require urgent elaboration. This report urges the Committee to elaborate on standards for the more effective protection of informational privacy by updating General Comment 16. New standards are necessary to address changing realities and to develop the content of the right to informational privacy in the digital age.

The Committee has previously responded to changing circumstances, such as those at issue now, by issuing new General Comments that revisit interpretations of articles of the ICCPR addressed in earlier General Comments. Sometimes these new General Comments have revised or completely replaced older ones,[1] though the Committee has also chosen to supplement a standing General Comment without replacing the original.[2]

Changing Technologies and Notions of Informational Privacy

Though it recognizes informational privacy as a component of the right to privacy protected by Article 17,[3] General Comment 16 was written long before informational

[1] For example, General Comment 20 replaced General Comment 7 (both on torture), and General Comment 28 replaced General Comment 4 (both on equality between men and women). *See* General Comment 20: Article 7, U.N. Human Rights Comm., 44th Sess., U.N. Doc. HRI/GEN/1/Rev.1 (1992), *available at* http://tbinternet.ohchr.org/_layouts/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11; General Comment 28: Article 3, U.N. Human Rights Comm., 68th Sess., U.N. Doc. HRI/GEN/1/Rev.9 (vol. I) (2000), *available at* http://tbinternet.ohchr.org/_layouts/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11.

[2] The Committee supplemented General Comment 6, on the right to life, with General Comment 14, which extended its original, broader discussion of the right to life to a specific and urgent context: the development and use of nuclear weapons. *See* General Comment 14: Article 6, U.N. Human Rights Comm., 23rd Sess., U.N. Doc. HRI/GEN/1/Rev.1 (1984), *available at* http://tbinternet.ohchr.org/_layouts/treatybodyexternal/TBSearch.aspx?Lang=en&TreatyID=8&DocTypeID=11.

[3] General Comment 16, ¶ 10, U.N. GAOR, 43rd Sess., Suppl. No. 40, U.N. Doc. A/43/40 (1988) [hereinafter General Comment 16].

privacy began to emerge as a distinct, fundamental right.[4] Both technology and our notions of informational privacy have changed enormously since 1988. As the UN High Commissioner for Human Rights ("OHCHR") recently observed, we have entered "the digital age."[5] Electronic communications and data storage, including mobile and computer technologies, have come to occupy a central role in the lives of billions.[6] Massively numerous and revealing data about many of us exist in electronic form, stored on servers and devices all over the world.

At the same time, State capacities to intercept and process large numbers of electronic data have grown exponentially, opening the door to unprecedented levels of intrusion into our private lives. Official documents, including some that were leaked to the press by NSA whistleblower Edward Snowden and others that were released in response to litigation, reveal that numerous governments have capitalized on this confluence of events to collect and analyze vast quantities of data on countless people, most of whom are not suspected of wrongdoing.

General Comment 16 predated the technological advances that led to this paradigm shift in electronic communications, data storage, and State surveillance. As a result, the General Comment does not fully address State responsibilities surrounding privacy in the digital age. Put another way, changes in technology and State practice have significantly outpaced authoritative pronouncements on certain elements of the right to privacy. There is thus an urgent need to update General Comment 16 to address the momentous shift in circumstances that has overturned certain assumptions about informational privacy that were accurate at the time it was originally drafted.

Developing the Content of the Right to Privacy

While States Parties can interfere with informational privacy in many ways—such as with data retention mandates, or the use of biometrics—the source of interference that has become the primary subject of recent worldwide concern is digital surveillance. The OHCHR recently highlighted the relationship between surveillance and informational privacy:

> [A] State's effectiveness in conducting surveillance is no longer limited by scale or duration. Declining costs of technology and data storage have eradicated financial or practical disincentives to conducting surveillance. The State now has a greater capability to conduct simultaneous, invasive,

[4] *See e.g., Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* ¶ 12, OHCHR, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009) (Martin Scheinin) [hereinafter Special Rapporteur 2009 Report].

[5] U.N. Human Rights Council, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, OHCHR, U.N. Doc. A/HRC/27/37 (June 30, 2014) [hereinafter *The Right to Privacy in the Digital Age*].

[6] By the end of 2013, over 2.8 billion people around the world had become Internet users. *See* Miniwatts Marketing Group, *World Internet Usage and Population Statistics*, INTERNET WORLD STATS (30 June, 2012), http://www.internetworldstats.com/stats.htm.

> targeted, and broad-scale surveillance than ever before. In other words, the technological platforms upon which global, political, economic, and social life are increasingly reliant are not only vulnerable to mass surveillance, they may actually facilitate it.[7]

Other parts of the UN system have also taken steps to expand on the same recent developments that create the need to update General Comment 16. For example, in December of 2013, the General Assembly adopted Resolution 68/167 on "The right to privacy in the digital age," and the OHCHR issued a report by the same name in June of 2014.[8] In contrast, the Committee has yet to weigh in on the new landscape for informational privacy in any comprehensive way.

As currently drafted, General Comment 16 also fails to address the close link between privacy interests and other rights—a link that has become more pronounced as a consequence of digital technologies. Other international and national bodies, however, have made this important connection. In his 2013 report, the Special Rapporteur on the protection and promotion of the right to freedom of expression and opinion, Frank La Rue, highlighted the nexus between general privacy protections (including those for informational privacy) and other rights. In particular, he noted that insufficient protection for privacy may chill the exercise of rights like the right to freedom of expression. (Individuals may be chilled into silence with respect to their online communications, for example, if they cannot be assured that their communications are private.)[9] More recently, the OHCHR expanded this list of potentially implicated rights to include: freedom of opinion, right to family life, right to health, and the right to be free from torture and cruel, inhuman, and degrading treatment.[10] President Obama's Review Group on Intelligence and Communications Technologies drew a similar connection, stating that: "[i]f people are fearful that their conversations are being monitored, expressions of doubt about or opposition to current policies and leaders may be chilled, and the democratic process itself may be compromised."[11] The European Court of Justice made the same point in *Digital Rights Ireland, Ltd. v. Minister for Communications, Marine and Natural Resources*.[12] The threat of a chilling effect is especially

---

[7] *The Right to Privacy in the Digital Age*, *supra* note 5, at ¶ 2.

[8] *Id.* at ¶¶ 5-6. The Council of Europe Commissioner for Human Rights has also issued a lengthy report on the relationship between human rights and the "digital world," though it does not focus exclusively on the ICCPR. COUNCIL OF EUROPE COMMISSIONER FOR HUMAN RIGHTS, THE ROLE OF LAW ON THE INTERNET AND IN THE WIDER DIGITAL WORLD (2014), https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=2654047&SecMode=1&DocId=2216804&Usage=2.

[9] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* at 4-7, OHCHR, U.N. Doc. A/HRC/23/40 (April 17, 2013) (by Frank La Rue) [hereinafter Special Rapporteur 2013 Report].

[10] The OHCHR notes "credible indications [that] digital technologies have been used to gather information that has then led to torture and other ill-treatment." *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 14.

[11] RICHARD A. CLARKE ET AL., THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 47 (Dec. 12, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[12] Case C-293/12 & C-594/12, Digital Rights Ireland, Ltd. v. Minister for Communications, Marine and Natural Resources, ¶ 28 (2014).

pronounced in the context of mass surveillance-based anti-terrorism legislation,[13] as the Committee recently observed in its 2014 Concluding Observations on the United States.[14]

Most importantly, General Comment 16 is rooted in a time when the Internet was in its infancy—long before the widespread use of certain forms of electronic communication (like email and instant messaging), and predating the birth of the World Wide Web and its discussion forums, blogs, social networking sites, and online shopping tools. In fact, General Comment 16 contains no reference to the Internet or to newer communication technologies, and it offers no examination of the impact of these technologies on privacy interests protected by the ICCPR. Nor does the General Comment explicitly anticipate the large-scale shift from fixed-line telephone systems to mobile telecommunications.[15]

Beyond changes in the behavior of the people protected by the Covenant, General Comment 16 also fails to reflect changes in the practices of States Parties—most notably with respect to their increasing and enormous capacity to conduct surveillance involving the acquisition, retention, dissemination, and use of personal data, including metadata.[16] Recent Committee petitions and Concluding Observations do reflect these technological evolutions. However, as pointed out by Manfred Nowak, former Special Rapporteur on torture and the author of a definitive commentary on the ICCPR, privacy has always "manifested itself in particular institutional structures";[17] and General Comment 16 is clearly wedded to traditional institutional structures, such as the family and the home. To maintain the relevance of Article 17, the Committee must take into account new institutional structures, such as the Internet. It must also make clear that Article 17 can accommodate a robust understanding of informational privacy, which has assumed incalculably greater significance in the digital age.

In short, technological developments are altering the borders of the private and public spheres,[18] and parts of the legal framework established by General Comment 16 now provide inadequate guidance to the Committee and Member States. Consequently, the

---

[13] Special Rapporteur 2009 Report, *supra* note 4, at ¶ 13.
[14] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, United States of America*, ¶ 22, U.N. Doc. CCPR/C/USA/CO/4 (2014) [hereinafter U.N. Human Rights Comm., 2014 Concluding Observations on the U.S] (noting concern at the privacy implications of the National Security Agency's programs, including those under Section 215 of the USA PATRIOT Act, Section 702 of the Foreign Intelligence Surveillance Act, PRISM, and UPSTREAM).
[15] *See* Special Rapporteur 2013 Report, *supra* note 9, at 3–20 (highlighting the development of metadata [data about data]; the relationships between Internet companies, service providers, and governments, entrenched through mandatory data-retention laws; and the ability on the part of States to track Internet activities on a large scale, through social media monitoring or analysis of IP addresses). Further information technologies that implicate privacy rights include the rise of biometric data-gathering (through, for example, finger-printing, facial recognition software, or other, even more sophisticated tools) and DNA databases.
[16] *See e.g.,* APC AND HIVOS, GLOBAL INFORMATION SOCIETY WATCH 2014: COMMUNICATIONS SURVEILLANCE IN THE DIGITAL AGE (2014), *available at* http://giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf.
[17] MANFRED NOWAK, U.N. COVENANT ON CIVIL AND POLITICAL RIGHTS: CCPR COMMENTARY 378 (2nd ed. 2005).
[18] *Id.* at 10.

passing discussion of modern technologies and modes of communication contained in General Comment 16, although still relevant in its own right, needs to be updated.[19]

Updating General Comment 16 will provide concrete guidance to States on the nature and scope of informational privacy rights in the digital age, and will further solidify the ICCPR as the primary international human rights treaty protecting those rights.

This report identifies some of the key principles that should underpin the right to informational privacy in the digital age. These principles are based primarily on the existing jurisprudence of the Committee, and are supplemented and augmented by the jurisprudence and practices of other international human rights bodies. A model General Comment focusing on the informational privacy component of Article 17 is included as an appendix to assist the Committee in updating General Comment 16.

[19] For example, General Comment 16 notes that "[s]urveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited"), yet State practice has developed rapidly in the opposite direction. General Comment 16, *supra* note 3, at ¶ 8. Current guidance from the Committee accurately reflecting that reality is essential.

Principles Underpinning Informational Privacy in the Digital Age

An update of General Comment 16 should more explicitly recognize a right to informational privacy, recognize protections for a person's digital identity, and provide greater specificity about the permissibility of limitations to the right. It should also address emerging issues by affirming the inherent illegality of mass surveillance and the nature and extent of a State's extraterritorial obligations to protect the right to privacy.

Article 17's Privacy Protections and Informational Privacy

Although the record of the drafting of Article 17 provides little guidance as to precisely what was intended for inclusion within the concept of "privacy," the Committee has recognized that the Article encompasses concepts beyond those explicitly listed.[20] Consistent with this broad notion of privacy, Article 17's privacy protections have evolved to encompass a right to informational privacy, including specific rights to access and control one's personal data.[21] General Comment 16 explicitly contemplates this development:

> The gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law. Effective measures have to be taken by States to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant. In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public [authorities] or private individuals or bodies control or may control their files. If such files contain incorrect personal data or have been collected or processed

[20] Coeriel et al. v. The Netherlands, U.N. Human Rights Comm., Communication No. 453/1991 at ¶ 10.2, U.N. Doc. CCPR/C/52/D/453/1991 (1994) (finding the right to privacy includes the right to freely express one's identity); *see also*, Mónaco de Gallicchio v. Argentina, U.N. Human Rights Comm., Communication No. 400/1990 at ¶ 10.4, U.N. Doc. CCPR/C/53/D/400/1990 (1995) (finding falsification of a baby's birth certificate resulting in a different legal identity constitutes a violation of Article 17). *See generally,* Toonen v. Australia, U.N. Human Rights Comm., Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (1994) (including the right to engage in consensual sexual activity in private); General Comment 16, *supra* note 3, at ¶ 8 (noting that the right to intimacy is a component of the right to privacy). Hertzberg et al. v. Finland, U.N. Human Rights Comm., Communication No. 61/1979, Appendix, U.N. Doc. CCPR/C/15/D/61/1979 (1982) (finding that the right to privacy includes the right to be different and to live accordingly); *see also*, Nowak, *supra* note 17; Fernando Volio, *Legal Personality, Privacy and the Family* in THE INTERNATIONAL BILL OF RIGHTS: THE COVENANT ON CIVIL AND POLITICAL RIGHTS 185, 192-193 (Louis Henkin ed., 1981).

[21] Nowak, *supra* note 17, at 388.

> contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[22]

In several of its Concluding Observations, the Committee has applied this framework. In 2009, the Committee recognized that a "State party should protect personal data and fully guarantee the right to privacy in accordance with the Covenant,"[23] which includes the assurance that the "gathering and holding of personal information on computers, databanks, and other devices, whether by public authorities or private individuals or bodies, is regulated by law."[24]

The Committee's practice is reflected in the jurisprudence of regional human rights bodies. The European Court of Human Rights ("European Court") has found that "private life," guaranteed by Article 8 of the European Convention, is "not susceptible to exhaustive definition";[25] and it has repeatedly held that "protection of personal data is of fundamental importance to a person's enjoyment of respect for his or her private and family life."[26] In its analysis, the Court has taken a broad view of what constitutes "personal data," recognizing that "private and family life" protects not just data that can be used for personal identification purposes, but any "data relating to the private life of an individual."[27] Accordingly:

> [Even] 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.[28]

In assessing the scope of the protections afforded by this notion of informational privacy, the European Court has also recognized the relevance of recent technological

---

[22] General Comment 16, *supra* note 3, at ¶ 10.
[23] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Spain*, ¶ 11, U.N. Doc. CCPR/C/ESP/CO/5 (2009) [hereinafter U.N. Human Rights Comm., Concluding Observations on Spain].
[24] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, France*, ¶ 22, U.N. Doc. CCPR/C/FRA/CO/4 (2008) [hereinafter U.N. Human Rights Comm., Concluding Observations on France]; U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Sweden*, ¶ 18, U.N. Doc. CCPR/C/SWE/CO/6 (2009) (encouraging the government to "take all appropriate measures to ensure that the gathering, storage, and use of personal data not be subject to any abuses, nor be used for purposes contrary to the Covenant)[hereinafter U.N. Human Rights Comm., Concluding Observations on Sweden]. *See also* U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Hungary*, ¶ 6, U.N. Doc. CCPR/C/HUN/CO/5 (2010).
[25] Bensaid v. the United Kingdom, App No. 44599/98, Eur. Ct. H.R., ¶ 47 (2001); *see also* Botta v. Italy, App. No. 21439/93, Reports of Judgments and Decisions, Eur. Ct. H.R., ¶ 32 (Feb. 24, 1998) (holding that "*a person's physical and psychological 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.").
[26] MK v. France, App. No. 19522/09, Eur. Ct. H.R., ¶ 35 (2013); S. and Marper v. the United Kingdom [GC], App. Nos. 30542/04 and 30566/04, Eur. Ct. H.R., ¶ 103 (2008); Gardel v. France, App. No. 16428/05, Eur. Ct. H.R., ¶ 62 (2009); M.B. v. France, App. No. 22115/06, Eur. Ct. H.R., ¶ 53 (2009); B.B. v. France, App. No. 5335/06, Eur. Ct. H.R., ¶ 61 (2009).
[27] *See* Marper, *supra* note 26, at ¶¶ 66-67.
[28] Rotaru v. Romania [GC], App No. 28341/95, Eur. Ct. H.R., ¶ 43 (2000).

developments. In *Malone v. the United Kingdom*, the Court observed:

> [T]he individual is more and more vulnerable as a result of modern technology . . . . [M]an in our times has a need to preserve his identity, to refuse the total transparency of society, to maintain the privacy of his personality.

Article 8 of the Charter of Fundamental Rights of the European Union recognizes an explicit right to protection of personal data distinct from the right to privacy protected by Article 7.[29] Additionally, the Inter-American Court of Human Rights has taken a broad reading of the interests protected by "private life," and understands that term to encompass multiple dimensions, including protections for informational privacy.[30] At the State level, too, there has been growing recognition of informational privacy rights. For example, in 2008, the German Constitutional Court expanded privacy protections into the realm of information technology when it interpreted its Basic Law[31] as providing every citizen with the fundamental right of integrity and confidentiality of information technology systems.[32] Accordingly, it held that secret searches of private computers were unconstitutional.[33]

In updating General Comment 16, the Committee should affirm that the protections contained in Article 17 apply broadly, and that informational privacy forms an important component of the right to privacy more generally.

Concepts of "Home" and "Correspondence" in the Digital Age

Article 17's protections for privacy of "home" and "correspondence" assume increasing importance in a world where modern technology can potentially interfere with those interests in ways that were not foreseeable during the drafting of General Comment 16. These developments should be reflected in an update to General Comment 16.

"Home" Includes Online Private Spaces

An individual's home may now encompass virtual spaces, such as social media websites and email inboxes. The Committee should recognize these online private spaces, as well as the personal computers and handheld electronic devices used to access them, as

[29] Charter of Fundamental Rights of the European Union, arts. 7, 8, Dec. 12, 2000, 2000/C 364/01.
[30] *See* Murillo v. Costa Rica, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 257, ¶ 143 (Nov. 28, 2012) (observing that, "[p]rivate life includes the way in which individual (sic) views himself and how he decides to project this view towards others, and is an essential condition for the free development of the personality. . . .". Informational privacy is indispensable to the projection of one's view of oneself to others.
[31] Basic Law for the Federal Republic of Germany, arts. 1 and 2, *available at* http://www.gesetze-im-internet.de/englisch_gg/basic_law_for_the_federal_republic_of_germany.pdf.
[32] Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 27 February 2008, reference number: 1 BvR 370/07, *available at* http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html (in German).
[33] *Id.*

subject to the same protections as a "home." Such an approach is consistent with the broad interpretation General Comment 16 affords "home" under Article 17, which it describes as encompassing "the place where a person resides or carries out their usual occupation."[34] A broad interpretation is also consistent with the practice of the European and Inter-American Human Rights systems. In *Halford v. the United Kingdom*, the European Court adopted a broad view on the parameters of "home" under Article 8 of the European Convention, holding that privacy protections applied equally to phone calls made from the applicant's office and home telephones.[35] More recently, in *Bernh Larsen Holding AS and Ors. v. Norway*, the Court found that "all data stored on a server" used by three corporations constitutes a space that should be afforded the same protections as a "home."[36] The Inter-American Court also defines protections afforded to the "home" expansively:

> [T]he sphere of privacy is characterized by being exempt from and immune to abusive and arbitrary invasion or attack by third parties or the public authorities. In this regard, an individual's home and private life are intrinsically connected, because the home is the space in which private life can evolve freely.[37]

If "home" is the "space in which private life can evolve freely" and privacy encompasses "the right to establish and develop relationships with other human beings and the outside world,"[38] "home," for the purposes of Article 17, should be interpreted in an updated General Comment to include privacy protections for personal online spaces as well as personal computers and handheld electronic devices.[39]

"Correspondence" Includes All Forms of Digital Communications

Although initially directed at maintaining the confidentiality of postal communications, "correspondence" under Article 17 should be interpreted to include all electronic forms of communication, such as email and instant messages, as well as "telephonic and telegraphic" forms of communication.[40] This position has roots in General Comment 16,[41] and in the recent practice of the Committee. In 2011, for example, in Concluding Observations, the Committee called on Iran to ensure that its Internet monitoring

---

[34] General Comment 16, *supra* note 3.
[35] Halford v. the United Kingdom, App. No. 20605/92, Judgment, Eur. Ct. H .R., ¶¶ 44, 46 (1997).
[36] Bernh Larsen Holding AS and Ors. v. Norway, App. No. 24117/08, Judgment, Eur. Ct. H .R., ¶ 106 (2013). *See also*, Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 27 February 2008, reference number: 1 BvR 370/07, *available at* http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html (in German) (finding that privacy of home life extends to privacy interests in personal information technology systems).
[37] Ituango Massacres v. Colombia, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 148, ¶¶ 193-194 (2006).
[38] Shimovolos v. Russia, App. No. 3019409/09, Judgment, Eur. Ct. H.R., ¶¶ 64–66 (June 21, 2011).
[39] *See generally*, G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Dec. 18, 2013) (recognizing that "the same rights people have offline must also be protected online, including the right to privacy") [hereinafter G.A. Res. 68/167].
[40] *Id.*
[41] General Comment 16, *supra* note 3, at ¶ 8.

complies with the State's obligations to respect the right to privacy.[42] And, in Concluding Observations on Bulgaria, the Committee equated telephone calls to "correspondence" under Article 17, implicitly recognizing that electronic communication qualifies as "correspondence."[43]

An update to General Comment 16 should also confirm that certain metadata—data about correspondence or transactions that excludes the content of what is communicated—are protected under Article 17. Metadata include, among other things: phone numbers dialed; the time, date and duration of calls made; location information for cellular phones (as recorded by cellular phone towers, for example); and the IP addresses or URLs visited while browsing the Internet. These data can allow the government and private organizations to "identify or infer new and previously private facts" about an individual, such as behavioral patterns and associational links, especially when collected, aggregated, and analyzed, or charted across time.[44] Indeed, in some instances, metadata can reveal information that is more sensitive than the contents of the underlying communication.[45] This kind of information can be gathered at little cost, easily shared, and processed rapidly through "algorithmic surveillance" in order to create digital profiles of individuals.[46] It can also be used to determine a person's location. Credible reports indicate that metadata obtained through electronic surveillance techniques have even been used to "identify the location of targets for lethal drone strikes."[47] Thus, from an informational privacy standpoint, there is often no functional

---

[42] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Iran*, ¶ 27, U.N. Doc. CCPR/C/IRN/CO/3 (2011).

[43] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant*, *Concluding Observations, Bulgaria*, ¶ 22, U.N. Doc. CCPR/C/BGR/CO/3 (Aug. 19, 2011); *see also*, U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14. The European Court has long equated all manner of digital communications as "correspondence" for purposes of Article 8 of the European Convention: Taylor-Sabori v. the United Kingdom, App. No. 47114/99, Judgment, Eur. Ct. H.R., ¶¶ 16-19, 22 (October 22, 2002) (pager messages); Weber and Saravia v. Germany, App. No. 54934/00, Decision As To Admissibility, Eur. Ct. H.R., ¶ 77 (June 29, 2006) (telephone communications); Copland v. the United Kingdom, App. No. 62617/00, Judgment, Eur. Ct. H.R., ¶¶ 43-44 (Apr. 3, 2007)(finding that email and internet usage falls within the ambit of Article 8 in the same way as telephone or postal communications).

[44] Felten Decl. at ¶ 62, *ACLU v. Clapper*, --- F. Supp. 2d ----, No. 13-cv-3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013), *available at* https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf; *see also*, AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA, METADATA: PIECING TOGETHER A PRIVACY SOLUTION (2014), *available at* https://www.aclunc.org/publications/metadata-piecing-together-privacy-solution; ELECTRONIC FRONTIER FOUNDATION, "The Principles," *International Principles on the Application of Human Rights to Communications Surveillance* (July 10, 2013), https://en.necessaryandproportionate.org/text; *see e.g.,* Special Rapporteur 2013 Report, *supra* note 9. (The U.N. Special Rapporteur on freedom of expression has observed—and the world's leading computer scientists have documented— that metadata, especially when collected and analyzed at scale, radically alters notions of privacy: "[w]hen accessed and analyzed, communications metadata may create a profile of an individual's life, including medical conditions, political and religious viewpoints, associations, interactions and interests, disclosing as much detail as, or even greater detail than would be discernible from the content of communications.").

[45] Special Rapporteur 2013 Report, *supra* note 9, at ¶¶ 40-41.

[46] Benjamin J. Goold, *Privacy, Identity, and Security* in SECURITY AND HUMAN RIGHTS 45, 56 (Benjamin J. Goold & Liora Lazarus eds., 2007).

[47] *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 14.

difference between metadata and communication content. Both may trigger Article 17 protections.[48]

Indeed, the Committee has recently recognized the privacy implications of metadata collection. In its 2014 Concluding Observations on the United States, the Committee expressed its concerns about a telephone metadata collection program, calling on the government to take "all necessary measures to ensure that its surveillance activities . . . conform to its [Article 17] obligations under the Covenant."[49] The European Court has taken a similar position. For example, in *Copland v. the United Kingdom*, the Court found that Internet usage falls within the ambit of Article 8 in the same way as telephone or postal communications.[50] The Court also determined that *information derived from* the monitoring of personal Internet usage—metadata—falls within the scope of "correspondence" under Article 8.[51] Specifically, the Court held:

> [C]ollection and storage of personal information relating to the applicant's telephone, as well as to her e-mail and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8.[52]

The European Court of Justice endorsed this same view when, on privacy grounds, it invalidated an EU directive that authorized collection of metadata only,[53] as did the OHCHR in its report on privacy in the digital age.[54] An update to General Comment 16 should reflect the international consensus that content and metadata can both implicate the right to privacy under Article 17.

---

[48] Hearing before the European Parliament, LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, 4 (Oct. 14, 2013), *available at* http://www.europarl.europa.eu/document/activities/cont/201310/20131017ATT72929/20131017ATT72929EN.pdf.

[49] U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14, at ¶ 22.

[50] Copland v. The United Kingdom, App. No. 62617/00, Judgment, Eur. Ct. H.R. ¶ 41 (2007).

[51] *Id.*

[52] *See also*, Malone v. the United Kingdom, App. No. 8691/79, Judgment, Eur. Ct. H.R., ¶¶ 83-84 (Aug. 2, 1984) (release of telephony metadata to law enforcement without the subscriber's consent amounts to an interference with privacy of correspondence); Uzun v. Germany, App. No. 35623/05, Judgment, Eur. Ct. H.R., ¶¶ 49-53 (Sept. 2, 2010)(concluding that GPS surveillance when conducted over a period of months constitutes an interference with private life under Article 8).

[53] Case C-293/12 & C-594/12, Digital Rights Ireland, Ltd. v. Minister for Communications, Marine and Natural Resources, ¶¶ 26, 69 (2014).

[54] *The Right to Privacy in the Digital Age*, *supra* note 5, at ¶ 19 (finding that there is no persuasive difference between the content of a communication and the data associated with that communication). *See also*, *United States v. Jones,* 132 S. Ct. 945 (2012) (Sotomayor, J., concurring) (recognizing the potential implication for privacy rights in the collection of metadata, particularly when it is aggregated over time).

Article 17 Protections for Informational Privacy

The right to informational privacy guaranteed by Article 17 is not absolute. Although Article 17 does not contain an explicit limitations clause, the Committee has interpreted the text narrowly to permit interferences that are both lawful and non-arbitrary.[55] Consistent with the practice of the Committee and other international authorities, to establish "lawfulness," the "interference" must meet several criteria, including being "prescribed by law, clearly defined, and subject to judicial review." The non-arbitrariness requirement mandates that any measure be "reasonable," which can be understood to require administering a four-part test, as described below.

"Interferences" with the Right to Informational Privacy

Article 17 prohibits any arbitrary or unlawful interference with privacy rights. As a threshold matter, therefore, Article 17 only protects against measures that interfere with recognized privacy interests. The Committee has defined "interference" broadly to include any measure that either directly or indirectly infringes on an individual's privacy interests.

An update to General Comment 16 should expressly state that laws or policies that produce a chilling effect on protected activity by affecting privacy interests thereby create an interference under the terms of Article 17, and that this interference is exacerbated where the laws or policies in question are vague, secret (even in part), or unclear.[56] This would reflect the practice of the Committee and the European Court. In *Toonen v. Australia*, the Committee considered whether provisions of the Tasmanian Criminal Code that criminalized various forms of sexual contact between men, including sexual contact between consenting adult homosexual men in private, violated Article 17.[57] Although the provisions had not been enforced for several years, and the government had a policy of not initiating criminal proceedings based on private homosexual conduct, that policy was no guarantee that the provisions would not be enforced in the future.[58] As a result, the Committee concluded that the "continued existence of the challenged provisions . . . continuously and directly" interfered with privacy.[59]

---

[55] U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14, at ¶ 22; Nowak, *supra* note 17, at 381. The *travaux preparatoires* for the ICCPR suggest that States sought the flexibility to determine what limitations could be imposed on privacy rights.

[56] G. ALEX SINHA, AMERICAN CIVIL LIBERTIES UNION & HUMAN RIGHTS WATCH, WITH LIBERTY TO MONITOR ALL: HOW LARGE-SCALE US SURVEILLANCE IS HARMING JOURNALISM, LAW, AND AMERICAN DEMOCRACY (2014), *available at* https://www.aclu.org/sites/default/files/assets/dem14-withlibertytomonitorall-07282014.pdf; Special Rapporteur 2013 Report, *supra* note 9.

[57] Toonen v. Australia, U.N. Human Rights Comm., Communication No. 488/1992 at ¶¶ 8.3, 2.1, U.N. Doc. CCPR/C/50/D/488/1992 (1994).

[58] *Id.* at ¶ 8.2.

[59] *Id.*

In *Weber v. Germany*, the European Court applied this same principle in assessing whether a German law authorizing surveillance constituted an interference as defined by Article 8 of the Convention:

> [T]he mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken . . . .[60]

An update should also reaffirm that States' collection and storage of personal information interferes with privacy interests even absent subsequent use or transmission of those data.[61] General Comment 16 implicitly recognizes this fact, noting that "gathering and holding of personal information on computers, databanks and other devices, whether by public authorities or private individuals or bodies, must be regulated by law."[62]

The Committee's practice is also consistent with the international consensus that "mere possibility of communications information being captured creates an interference with privacy."[63] The European Court has long recognized this principle. In *Leander v Sweden*, the European Court held that "[b]oth the storing and the release of . . . information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life."[64] In *Kopp v Switzerland,* the Court found that the "[i]nterception of telephone calls constitutes 'interference by a public authority,' within the meaning of article 8 section 2," adding that "subsequent use of the recordings made has no bearing on that finding."[65] In *Shimovolos v Russia*, a case involving the registration of a person in a surveillance database and the tracking of his travel movements, the Court held that "systematic collection and storing of data by security services" are interferences with the right to privacy. The Court also

---

[60] Weber and Saravia v. Germany, App. No. 54934/00, Decision as to Admissibility, Eur. Ct. H.R., ¶ 78 (2006).
[61] General Comment 16, *supra* note 3; Amann v. Switzerland, App. No. 27798/95 ¶ 69 (2010); Case C-293/12 & C-594/12, Digital Rights Ireland, Ltd. v. Minister for Communications, Marine and Natural Resources, ¶ 29 (2014); *see generally,* Liberty and Others v. United Kingdom, App. No. 58243/00, Judgment, Eur. Ct. H.R. (July 1, 2008) (reiterating this sentiment).
[62] General Comment 16, *supra* note 3, at ¶ 10. The OHCHR has taken a similar position in its recent report, indicating that this requirement issues from Article 17(2). *See, The Right to Privacy in the Digital Age*, *supra* note 5, at ¶ 28.
[63] *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 20.
[64] Leander v Sweden, App No. 9248/81, Judgment, Eur. Ct. H.R., ¶ 48 (1987).
[65] Kopp v Switzerland, App. No. 13/1997/797/1000, Judgment, Eur. Ct. H.R., ¶ 53 (Mar. 25, 1998); *see also*, Amann v Switzerland, App. No. 27798/95, Judgment, Eur. Ct. H.R., ¶ 45 (Feb. 16, 2000) (confirming that the interception and recording of a telephone call amounted to an interference with the right to privacy).

found that collection of data can amount to an interference with privacy even if those data are obtained from a public place or relate to professional or public activities.[66]

"Unlawful" Interferences with the Right to Informational Privacy

General Comment 16 makes clear that the prohibition on unlawful interference means that interference can occur only "on the basis of law"[67]—typically understood as domestic law.[68] However, those domestic laws must also be consistent with international standards, including "the provisions, aims and objectives of the Covenant."[69]

In addition, the lawfulness requirement provides that three further conditions must be satisfied: First, the domestic statutory framework must be accessible and must ensure that any interference is reasonably foreseeable to affected persons.[70] Second, and related, the domestic law must be "precise" and "clearly" defined.[71] Third, the law must contain adequate safeguards, such as mechanisms for oversight and redress for abuses.[72]

In its 2014 Concluding Observations on the United States, the Committee outlined this framework, stating that any interference with the right to privacy must be authorized by laws that:

a. Are publicly accessible;
b. Contain provisions that ensure that collection of, access to, and use of communications data are tailored to specific, legitimate aims;
c. Are sufficiently precise and specify in detail the circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limits on the duration of surveillance, and procedures for the use and storage of data collected; and

---

[66] Shimovolos v. Russia, App. No. 3019409/09, Judgment, Eur. Ct. H.R., ¶ 65 (June 21, 2011); Rotaru v. Romania [GC], App No. 28341/95, Eur. Ct. H.R., ¶¶ 43-44 (2000).
[67] General Comment 16, *supra* note 3, ¶ 3.
[68] *See* Escher et al. v. Brazil, Preliminary Objections, Merits, Reparations, and Costs, Inter-Am. Ct. H.R. (ser. C) No. 200, ¶ 116 (2009); Tristán Donoso v. Panamá, Preliminary Objections, Merits, Reparations and Costs, Inter-Am. Ct. H.R. (ser. C) No. 193, ¶ 56 (2009); Kennedy v. the United Kingdom, App. No. 26839/05, Judgment, Eur. Ct. H.R., ¶ 151 (2010); Malone v. the United Kingdom, App. No. 8691/79, Judgment, Eur. Ct. H.R., ¶¶ 66, 68 (1984). Whilst the language of the Inter-American Court and the European Court is distinguishable from that of the ICCPR, the differences are not material in this context.
[69] *See id.,* at ¶ 3 ("interference authorized by States can only take place on the basis of law, which itself must comply with the provisions, aims and objectives of the Covenant.").
[69] S.W. v. the United Kingdom, App. No. 20166/92, Judgment, Eur. Ct. H.R. (ser. A no. 335-B), ¶¶ 44-48 (1995); K.-H.W. v. Germany [GC], App. No. 37201/97, Judgment, Eur. Ct. H.R., ¶¶ 72-76 (2001) (extracts).
[70] *Id.*
[71] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Jamaica*, ¶ 20, U.N. Doc. CCPR/C/79/Add.83 (Nov. 19, 1997) [hereinafter U.N. Human Rights Comm., Concluding Observations on Jamaica]; U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Comments, Russian Federation*, ¶ 19, U.N. Doc. CCPR/C/79/Add.54 (July 26, 1995); General Comment 16, *supra* note 3, at ¶¶ 3, 8.
[72] U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14.

d. Provide for effective safeguards against abuse.[73]

The requirements of lawfulness mirror the test developed by the Committee in General Comment 34 (addressing the freedoms of opinion and expression protected by Article 19), and the "quality of law" test developed by the European Court in interpreting various articles of the European Convention that refer to the need for limitations on rights to be "prescribed by law."[74] Special Rapporteur on counter-terrorism and human rights, Ben Emmerson, has emphasized the importance of the "quality of law" test in the context of the ICCPR, describing it as encompassing the requirements that measures interfering with the right to privacy have a basis in the domestic law, where that law is itself compatible with the Covenant as well as publicly accessible, clear, and precise.[75] These sources are all instructive in elaborating the terms of an update to General Comment 16.

Consonance with Domestic and International Law

General Comment 16 clarifies that the term "unlawful" "means that no interference can take place except in cases *envisaged by the law*" (emphasis added).[76] As noted above, the term "unlawful" must be interpreted in light of both domestic and international law, including the terms of the ICCPR.[77] As a result, serious curtailment of human rights is not permissible simply because it is dictated or countenanced by "traditional, religious, or other such customary law."[78]

Accessibility and Foreseeability

Publicly accessible laws and regulations help people to foresee the legal consequences of their actions and to regulate their conduct accordingly.[79] Limitations provided exclusively within secret rules or secret interpretations (judicial, executive, or otherwise) are

[73] U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14.
[74] Kafkaris v. Cyprus [GC], App. No. 21906/04, Judgment, Eur. Ct. H.R., ¶ 118 (2008).
[75] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* ¶ 35-40, OHCHR, U.N. Doc. A/HRC/69/397 (Sept. 23, 2014) (Ben Emmerson) [hereinafter Emmerson 2014 Report]. Elsewhere Emmerson endorses the other parts of this test, such as the need for measures that interfere with privacy to be properly calibrated toward a legitimate aim (para 58), and the importance of independent oversight of such measures (para 61).
[76] General Comment 16, *supra* note 3, at ¶ 3.
[77] U.N. Human Rights Comm., Concluding Observations on France, *supra* note 24, at ¶ 22 ("The State party should take all appropriate measures to ensure that the gathering, storage and use of sensitive personal data are consistent with its obligations under article 17."); U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, United States of America*, ¶ 21, U.N. Doc. CCPR/C/USA/CO/5 (2006) (calling on the US to ensure the Patriot Act complied with the ICCPR) [hereinafter U.N. Human Rights Comm., 2006 Concluding Observations on the U.S.]; Jorgic v. Germany, App. No. 74613/01, Judgment, Eur. Ct. H.R., ¶¶ 67-68 (July 12, 2007); Kononov v. Latvia [GC], App. No. 36376/04, Judgment, Eur. Ct. H.R., ¶¶ 232-244 (2010).
[78] General Comment 34, ¶ 24, U.N. HRC, 102d Sess., U.N. Doc. CCPR/C/GC/34 (2011) (citing General Comment 32) [hereinafter General Comment 34].
[79] Kafkaris v. Cyprus [GC], App. No. 21906/04, Judgment, Eur. Ct. H.R., ¶¶ 150-152 (2008); Hashman and Harrup v. the United Kingdom [GC], App. No. 25594/94, Judgment, Eur. Ct. H.R., ¶ 31 (1999); Malone v. the United Kingdom, App. No. 8691/79, Judgment, Eur. Ct. H.R., ¶ 67 (1984).

incompatible with the ICCPR,[80] as are laws that allow governments and intelligence bodies to route data through States with more lax laws in order to gain advantages in data processing.[81] This requirement also provides a measure of legal protection against the possibility of interference through executive acts and discretion.[82]

In its Concluding Observations on the United States in 2014, the Committee noted that all laws that interfere with privacy must be "publicly accessible."[83] Thus, if the creation, maintenance, or operation of a surveillance database is governed by an administrative or judicial order or interpretation that is not accessible to the public, it does not satisfy the lawfulness test.[84]

Specificity and Precision

The requirement of specificity and precision is essential to support foreseeability, and is impossible without publicity. It derives support from General Comment 16, and Committee practice on wiretapping.[85] General Comment 16 specifies that, even in cases of lawful interference with the right to privacy, "relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted."[86] This requirement is also described in General Comment 34, which provides that any law "must be formulated with sufficient precision to enable an individual to regulate his or her conduct accordingly and it must be accessible to the public."[87] Additional protections are provided through the requirement that the executive must not have overbroad discretion to determine the scope and applicability of a law.[88] The Committee affirmed the need for this criterion in *Van Hulst v. Netherlands*, observing that "the relevant legislation authorizing interference with one's communications must specify in detail the precise circumstances in which such interference may be permitted."[89]

Likewise, in *Escher et al. v. Brazil*, the Inter-American Court found a Brazilian surveillance law compliant with Article 11 of the Inter-American Convention (right to privacy) where the law was both highly specific and targeted. The Court noted that a permissible

---

[80] U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14, at ¶ 22.
[81] *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 30 (noting that routing of data through a third party States renders the data collection and analysis unforeseeable to a resident of the first State).
[82] *See also* Emmerson 2014 Report, *supra* note 75, at ¶ 35 (noting that "the exercise of executive discretion must be circumscribed with reasonable clarity by the applicable law or binding published guidelines.").
[83] U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14, at ¶ 22.
[84] Shimovolos v. Russia, App. No. 3019409/09, Judgment, Eur. Ct. H.R. (June 21, 2011).
[85] U.N. Human Rights Comm., Concluding Observations on Russia, *supra* note 71, at ¶ 19; U.N. Human Rights Comm., Concluding Observations on Jamaica, *supra* note 71, at ¶ 20.
[86] General Comment 16, *supra* note 3, at ¶ 8.
[87] General Comment 34, *supra* note 78, at ¶ 25.
[88] *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 29.
[89] Van Hulst v. The Netherlands, Human Rights Comm., Communication No. 903/1999 at ¶ 7, U.N. Doc. CCPR/C/82/D/903/1999 (2004). *See also*, U.N. Human Rights Comm., 2014 Concluding Observations on the U.S, *supra* note 14, at ¶ 22 (requiring that an interference with privacy rights be "sufficiently precise and specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, [and] the limit on the duration of surveillance").

limitation of Article 11 must be pursuant to, and in accordance with, an enacted law.[90] The Court determined that the Brazilian law met this criterion because of its highly specific, targeted nature. The law allowed for surveillance only in those cases where such surveillance was necessary for a criminal investigation.[91] Further, the law required that "in any of these circumstances, reasonable indications of the authorship or participation in a criminal offense of the individual subjected to the measure must be provided, in addition to showing that the evidence cannot be obtained by other means."[92]

Thus, surveillance is impermissible under international law unless it is specific and targeted. In the law-enforcement context, the government must justify its surveillance activities by reference to a specific criminal investigation already underway—and consequently, the surveillance must be targeted at people reasonably suspected of being involved in specific offences. Surveillance in the intelligence context must be similarly discriminate.[93] Bulk or mass surveillance with no grounds for such suspicion would plainly fail such a test.[94]

Sufficient Safeguards

Oversight

The Committee has repeatedly and forcefully emphasized that surveillance and other measures that interfere with the right to privacy should be subject to effective administrative and judicial oversight. In General Comment 16, for example, the Committee observes that "reports [from States Parties] should include information on the authorities and organs set up within the legal system of the State which are competent to authorize interference allowed by the law."[95] Additionally, the Committee notes that "[i]t is also indispensable to have information on the authorities which are entitled to exercise control over such interference with strict regard for the law. . . ."[96] These statements reflect the Committee's long-standing view of the importance of oversight to ensure accountability for policies that interfere with privacy. In *Al-Gertani v.*

[90] Escher et al. v. Brazil, Preliminary Objections, Merits, Reparations, and Costs, Inter-Am. Ct. H.R. (ser. C) No. 200, ¶ 116 (2009).
[91] *Id.* at ¶ 132.
[92] *Id.*
[93] Recently, it has become clear that the US has adopted a very loose definition of "targeting" for some of its surveillance activities, under which it can search essentially everyone's international correspondence for references to certain information associated with its "targets." This sort of targeting is so broad that it results in the deliberate searches of millions of communications that are not to or from a target. *See, e.g.,* Jameel Jaffer, Submission to PCLOB Public Hearing on Section 702 of the FISA Amendment's Act, Mar. 19, 2014, pp. 14,15, *available at* https://www.aclu.org/sites/default/files/assets/pclob_fisa_sect_702_hearing_-_jameel_jaffer_testimony_-_3-19-14.pdf. The ICCPR does not countenance such broad surveillance measures, which lack the requisite specificity and precision, and leave countless people suspected of no wrongdoing vulnerable to arbitrary and unlawful interferences with their privacy. "Targeting" must be understood more narrowly, as conducting surveillance *of* a target, such as collecting the communications sent to and from that target.
[94] *See infra,* Mass Surveillance Operations are Inherently Unlawful and Practically Always Disproportionate, p. 25.
[95] General Comment 16, *supra* note 3, at ¶ 6.
[96] *Id.*

Bosnia and Herzegovina, the Committee determined that the surveillance operations at issue complied with Article 17 in part because they "were considered and reviewed in a fair and thorough manner by the administrative and judicial authorities."[97] Likewise, in *Van Hulst v. The Netherlands*, the Committee recognized that Dutch law met Article 17's requirements because the interception of communications had to be "based on a written authorization by the investigating judge."[98]

In its 1999 Concluding Observations on Poland, the Committee noted its concern at the lack of independent monitoring of the State's system of telephone tapping.[99] In its 2006 Concluding Observations on the United States, this concern was extended to the lack of independent oversight at the monitoring of telephone, email, and fax communications.[100]

Other authoritative voices have also underscored the importance of oversight as a safeguard, including Martin Scheinin, former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, and Ben Emmerson, the current Special Rapporteur on counter-terrorism and human rights. For example, in his 2009 report, Scheinin observed that "[s]urveillance systems require effective oversight to minimize harm and abuses,"[101] and called for "increased internal oversight to complement the process for independent authorization and external oversight." [102] In his September 2014 report, Emmerson observed that requisite safeguards typically include some form of oversight, and "the absence of adequate safeguards can lead to a lack of accountability for arbitrary or unlawful intrusions on the right to Internet privacy."[103]

In 2013, U.N. Resolution 68/167, "The Right to Privacy in the Digital Age," called upon States "to establish or maintain existing independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance or communications, their interception and the collection of personal data."[104] In June of 2014, the OHCHR emphasized the need for a multi-pronged government surveillance oversight program utilizing all branches of government to ensure true independence and impartiality,[105] and criticized judicial review mechanisms for surveillance practices that amount in essence to "rubber-stamping."[106]

---

[97] Al-Gertani v. Bosnia & Herzegovina, U.N. Human Rights Comm., Communication No. 1955/2010 at ¶ 5.7, U.N. Doc. CCPR/C/109/D/1955/2010 (2010).
[98] Van Hulst v. The Netherlands, Human Rights Comm., Communication No. 903/1999 at ¶ 7.7, U.N. Doc. CCPR/C/82/D/903/1999 (2004); *see also,* U.N. Human Rights Comm., Concluding Observations on Sweden, *supra* note 24, at ¶ 18 (requiring "review and supervision by an independent body" to prevent abuses in the gathering, storage and use of personal data).
[99] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Poland,* ¶ 22, U.N. Doc. CCPR/C/79/Add.110 (1999).
[100] U.N. Human Rights Comm., 2006 Concluding Observations on the U.S, *supra* note 77, at ¶ 21.
[101] Special Rapporteur 2009 report, *supra* note 4, at ¶ 51.
[102] *Id.* at ¶ 53.
[103] Emmerson 2014 Report, *supra* note 75, at ¶ 45.
[104] G.A. Res. 68/167, *supra* note 39, at ¶ 4(d).
[105] *The Right to Privacy in the Digital Age, supra* note 5, at ¶¶ 37-38.
[106] *Id.* at ¶ 38.

Redress

Safeguards are not just about mechanisms that prospectively constrain interferences with privacy. General Comment 16 goes further, noting the importance of access to redress for victims of improper interferences.[107] Specifically, the Committee observed that "it is indispensable . . . to know in what manner and through which organs persons concerned may complain of a violation of the right provided for in article 17 of the Covenant."[108] The Committee has applied this requirement in assessing the practices of States Parties. For example, in 2014, the Committee explicitly called for reforms of the United States' surveillance system that would ensure effective remedies for affected persons.[109]

The OHCHR has recently identified two essential features that characterize access to redress in the context of informational privacy—whether pursued through "judicial, legislative or administrative forms."[110] The first criterion is that "[the] remedies must be known and accessible to anyone with an arguable claim that their rights have been violated," which also implies that States must ensure some combination of notice of interference with informational privacy, and legal standing to challenge that interference.[111] The second criterion is that the remedies must "involve prompt, thorough and impartial investigation of alleged violations."[112]

An update to General Comment 16 should elaborate on the "minimum safeguards" that must be established to prevent abuse, as well as the necessary features of the tribunal responsible for oversight—in particular looking at what constitutes a "fair and public hearing by a competent, independent and impartial tribunal established by law."[113] It should also address the issue of effective remedies for victims when arbitrary or unlawful interferences occur.

---

[107] The notion that victims of ICCPR violations should generally have a right to redress is required by the treaty itself. *See* ICCPR, art. 2(3). Other instruments have similar provisions. *See* ECHR art. 13; ACHR, art. 25; American Declaration, art. 18.

[108] General Comment 16, *supra* note 3, at ¶ 6. The Committee reaffirmed the need for remedies for violations of informational privacy in its Concluding Observations on the United States in 2014, encouraging the State to "[e]nsure that affected persons have access to effective remedies in cases of abuse [of NSA surveillance]." U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14, at ¶ 22.

[109] U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14, at ¶ 22.

[110] *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 40. The European Court of Human Rights has similarly found that, as a general matter, access to redress need not be through the courts in all instances. *See* Leander v Sweden, App No. 9248/81, Judgment, Eur. Ct. H.R., ¶ 77 (1987). For more on the treatment of the right to redress under other systems, *see* SARAH ST. VINCENT, CENTER FOR DEMOCRACY & TECHNOLOGY, INTERNATIONAL LAW & SECRET SURVEILLANCE 18-19 (Sept. 9, 2014), https://d1ovv0c9tw0h0c.cloudfront.net/files/2014/09/CDT-IL-surveillance.pdf.

[111] *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 40.

[112] *Id.* at ¶ 41. More generally, the Committee has recently reaffirmed the need for "an effective remedy" for violations of the right to privacy. Bulgakov v. Ukraine, U.N. Human Rights Comm., Communication No. 1803/2008 at ¶ 9, U.N. Doc. CCPR/C/106/D/1803/2008 (2012).

[113] General Comment 32, ¶ 3, U.N. Human Rights Comm., 90th Sess., U.N. Doc. CCPR/C/GC/32 (2007).

"Arbitrary" Interferences with the Right to Informational Privacy

In addition to requiring that all interferences with privacy be lawful, Article 17 stipulates that such interferences must also be non-arbitrary. The Committee has long viewed the "non-arbitrary" requirement of Article 17 as requiring policies that interfere with privacy to be reasonable. In General Comment 16, the Committee stated that:

> [T]he introduction of the concept of arbitrariness is intended to guarantee that even interference provided for by law should be in accordance with the provisions, aims and objectives of the Covenant and should be, in any event, *reasonable in the particular circumstances*.[114]

The reasonableness analysis endorsed by the Committee and others mirrors the limitation requirements established by the Committee in General Comment 34. At various points, the Committee has elaborated on the idea of reasonableness, observing that it includes some combination of legitimacy, necessity, and proportionality.[115]

One of the Committee's fuller descriptions of the relevant limitation standards is set forth in General Comment 34. That Comment describes the two areas in which the limitation of a right may be permitted: 1) the limitation relates to the "rights or reputations of others"; and 2) the limitation relates to the "protection of national security or of public order (*ordre public*) or of public health or morals."[116] To ensure compliance with the Covenant, States Parties that invoke a legitimate ground for the restriction of a protected right must "demonstrate in specific and individualized fashion the precise nature of the threat and the necessity and proportionality of the specific action taken, in particular by establishing a direct and immediate connection between the [restricted right] and the threat."[117] Further, a limitation on a Convention right must not "put in jeopardy the right itself."[118]

Martin Scheinin, the former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, and Frank La Rue, the former Special Rapporteur on freedom of expression and opinion, have both emphasized the value of structuring the reasonableness test in terms of legitimacy, necessity and proportionality.[119] For example, in his 2009 report, Scheinin noted that the

---

[114] *Id.* (emphasis added).

[115] *See, e.g.,* Toonen v. Australia, U.N. Human Rights Comm., Communication No. 488/1992 at ¶ 8.3, U.N. Doc. CCPR/C/50/D/488/1992 (1994); Antonius Cornelis Van Hulst v. Netherlands, U.N. Human Rights Comm., Communication No. 903/1999 at ¶ 3.7, 7.6, U.N. Doc. CCPR/C/82/D/903/1999 (2004); U.N. Human Rights Comm., 2006 Concluding Observations on the U.S, *supra* note 77, at ¶ 21; U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14, at ¶ 22.

[116] General Comment 34, *supra* note 78, at ¶ 21, 30 (noting, however, that a government may not invoke laws that limits a right to "suppress or withhold from the public information of legitimate public interest that does not harm national security…").

[117] *Id.* at ¶ 35 (citing Shin v. Republic of Korea, Communication No. 926/2000).

[118] *Id.* at ¶ 21.

[119] *See*, Special Rapporteur 2009 Report, *supra* note 4, at ¶¶ 14-19; Special Rapporteur 2013 Report, *supra* note 9, at ¶¶ 28-29. *See also*, Nowak, *supra* note 17, at 383.

infrequent and generic derogations from Article 17 indicate that States generally view the framework of Article 17 to be "flexible enough to enable necessary, legitimate, and proportionate restrictions to the right to privacy by means of permissible limitations, including when responding to terrorism."[120] Although the text of Article 17 does not contain an express limitations clause, Scheinin noted that the permissible limitations test set forth by the Committee in General Comment 27 applies equally to Article 17.[121] In Scheinin's formulation, this test requires, among other things, that:

a. Any restrictions must be provided by the law (paras. 11-12);
b. The essence of a human right is not subject to restrictions (para. 13);
c. Restrictions must be necessary in a democratic society (para. 11);
d. Any discretion exercised when implementing the restrictions must not be unfettered (para. 13);
e. For a restriction to be permissible . . . it must be necessary for reaching the legitimate aim (para. 14);
f. Restrictive measures must conform to the principle of proportionality; they must be appropriate to achieve their protective function; they must be the least intrusive instrument amongst those which might achieve the desired result; and they must be proportionate to the interest to be protected (paras. 14-15);
g. Any restrictions must be consistent with the other rights guaranteed in the Covenant (para. 18).[122]

In his 2013 report, La Rue observed that "communications surveillance measures [must be] strictly and demonstrably necessary to achieve a legitimate aim; and [must a]dhere to the principle of proportionality, and [not be] employed when less invasive techniques are available or have not yet been exhausted."[123] The OHCHR has described similar conditions in its digital privacy report, noting that:

> [Any] limitation [on the right to privacy] must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right . . . must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination.[124]

The Special Rapporteur on human rights while countering terrorism, Ben Emmerson, has also identified the very same prongs to the test of non-arbitrariness:

---

[120] Special Rapporteur 2009 Report, *supra* note 4, at ¶¶ 14-15.
[121] *Id.* at ¶¶ 17-18.
[122] *Id.* at ¶ 17 (citing General Comment 27).
[123] Special Rapporteur 2013 Report, *supra* note 9, at ¶ 83.
[124] *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 23.

> It is incumbent upon States to demonstrate that any interference with the right to privacy under article 17 of the Covenant is a necessary means to achieving a legitimate aim. This requires that there must be a rational connection between the means employed and the aim sought to be achieved. It also requires that the measure chosen be "the least intrusive instrument among those which might achieve the desired result" (see CCPR/C/21/Rev.1/Add.9; and A/HRC/13/37, para. 60). The related principle of proportionality involves balancing the extent of the intrusion into Internet privacy rights against the specific benefit accruing to investigations undertaken by a public authority in the public interest.[125]

The European Court of Human Rights, the European Court of Justice, and the Inter-American Court of Human Rights all have endorsed similar approaches. In *S. and Marper v. United Kingdom*, the European Court noted that interferences with privacy must be, among other things, "proportionate to the legitimate aim pursued."[126] The European Court of Justice applied the same proportionality assessment in a 2014 data retention case, additionally emphasizing that measures interfering with informational privacy must be strictly necessary in pursuit of a legitimate aim.[127] Consistent with these rulings, in *Tristán Donoso v. Panamá*, the Inter-American Court observed that "such restriction[s] [on privacy] must be statutorily enacted, serve a legitimate purpose, and meet the requirements of suitability, necessity, and proportionality which render it necessary in a democratic society."[128]

The Requirements of a Non-Arbitrary Interference with the Right to Informational Privacy

These various articulations of the standards for non-arbitrary interferences with the right to informational privacy can be distilled into a four-part test. Under that test, interference with the interests protected by Article 17 is arbitrary unless it is: 1) conducted in pursuit of a legitimate aim; 2) necessary for achieving that aim; 3) tailored for minimal intrusion on a protected interest; and 4) acceptable under a fair balancing of the value of the interference and the magnitude of the intrusion it causes (i.e., proportionate). An update to General Comment 16 should adopt and articulate this same test.

---

[125] Emmerson 2014 Report, *supra* note 75, at ¶ 51.
[126] S. and Marper v. United Kingdom, App. Nos. 30562/04 and 30566/04, Judgment (Grand Chamber), Eur. Ct. H.R. 1581, ¶ 101 (2008).
[127] Case C-293/12 & C-594/12, Digital Rights Ireland, Ltd. v. Minister for Communications, Marine and Natural Resources, ¶ 65 (2014).
[128] Tristán Donoso v. Panamá, Preliminary Objections, Merits, Reparations and Costs, Inter-Am. Ct. H.R. (ser. C) No. 193, ¶ 56 (2009).

Legitimate Aim

A State must first show that any interference with the right to privacy pursues a legitimate, legal aim, consistent with a State's ICCPR obligations.[129] Although limitations related to the protection of national security, public order, public health, or public morals all may qualify as legitimate aims, the State should not have unfettered discretion to define those terms.[130] As the former Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has noted:

> Vague and unspecified notions of 'national security' have become an acceptable justification for the interception of and access to communications in many countries . . . . The use of an amorphous concept of national security to justify invasive limitations on the enjoyment of human rights is of serious concern.[131]

An update to General Comment 16 should elaborate on what constitutes a legitimate aim, and impose appropriate restrictions on the scope of States' authority to define limitations, especially in the national security context.[132]

Necessity

A State must also show that the policies or practices it has implemented in pursuit of a legitimate aim are in fact necessary for bringing about that aim, a point emphasized repeatedly by the Committee, the OHCHR, multiple special rapporteurs, and both the European and Inter-American Courts of Human Rights.[133] An update to General Comment 16 should reinforce the universality of this prong of the test, and provide further guidance on its strictness.

Minimal Intrusiveness

Third, States must ensure that interferences are narrowly tailored to avoid needless intrusion on protected privacy interests (such as, but not limited to, informational privacy). For example, in General Comments 27 and 34, the Committee noted that any restriction on human rights must (among other things) "be the least intrusive instrument amongst those which might achieve their protective function."[134] Other UN bodies have

---

[129] General Comment 34, *supra* note 78, at ¶ 26.
[130] *Id.* at ¶ 29.
[131] Special Rapporteur 2013 report, *supra* note 9, at ¶¶ 58, 60.
[132] Certain soft law principles already exist concerning the proper scope of national security limitations on relevant rights. *See generally*, *e.g.*, Global Principles on National Security and the Right to Information ("The Tshwane Principles") (June 12, 2013), *available at* http://fas.org/sgp/library/tshwane.pdf; The Johannesburg Principles on National Security, Freedom of Expression and Access to Information ("The Johannesburg Principles") (Nov. 1996), *available at* http://www.article19.org/data/files/pdfs/standards/joburgprinciples.pdf.
[133] *See supra,* "Arbitrary" Interferences with the Right to Informational Privacy, pp. 20-22.
[134] General Comment 34, *supra* note 78, at ¶ 34.

reached the same conclusions.[135] This requirement ensures that limitations on the right to privacy do not interfere with the object and purpose of the ICCPR, and do not dilute rights any more than they absolutely must.[136] As the Committee observed in the context of freedom of movement, "the restrictions [on a particular right] must not impair the essence of the right . . . ; the relation between right and restriction, between norm and exception, must not be reversed."[137]

An update to General Comment 16 should note that this prong of the test is crucial, even though a common, casual articulation of the non-arbitrariness test ("necessary and proportionate to a legitimate aim") does not explicitly address it.

Proportionality

Finally, in addition to guaranteeing that their minimally intrusive interferences with informational privacy are necessary for pursuit of a legitimate aim, States must ensure that those interferences are proportionate. In other words, such interferences must fairly balance the value of the policies or practices that intrude on informational privacy against the magnitude of the intrusion.

The proportionality requirement derives from repeated statements by the Committee, numerous special rapporteurs, the OHCHR, and the European and Inter-American Courts of Human Rights.[138] The Committee has also confirmed that the proportionality assessment is not solely for the State to determine.[139] Further, the OHCHR noted recently that, in the context of informational privacy, proportionality must take into account what is to be done with collected data, and who will have access to them.[140]

An update to General Comment 16 should reaffirm the importance of a fair proportionality assessment in evaluating State laws and practices that interfere with informational privacy. It should also provide guidance to States on how to undertake that judgment properly, especially in light of the Committee's earlier conclusion that States may not make such assessments unilaterally.

---

[135] Special Rapporteur 2009 report, *supra* note 4, at ¶ 49 (stating that States must have exhausted less-intrusive interferences with fundamental right before resorting to others).
[136] *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 23. Minimal intrusiveness is not necessarily implied by proportionality alone, for a strong, legitimate interest could, in theory, justify an interference with privacy even if it is not the most narrowly tailored.
[137] General Comment 27, ¶¶ 11-16, U.N. Human Rights Comm., 67th Sess., U.N. Doc. CCPR/C/21/Rev.1/Add.9 (1999).
[138] *See supra*, "Arbitrary" Interferences with the Right to Informational Privacy, pp. 20-22.
[139] Robert Gauthier v. Canada, U.N. Human Rights Comm., Communication No. 633/1995 at ¶ 13.6, U.N. Doc. CCPR/C/65/D/633/1995 (1999). From this decision, it appears that even the necessity analysis may require independent input.
[140] *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 27.

Mass Surveillance Operations are Inherently Unlawful and Practically Always Disproportionate

Recent developments invite specific Committee guidance on the practice of mass surveillance. In June of 2013, media outlets began reporting on enormous surveillance programs run by the United States and various allies, courtesy of leaked documents taken from the United States' National Security Agency (NSA) by whistleblower and former NSA contractor Edward Snowden. Snowden's documents revealed a wide range of programs—aimed both at people inside and outside the U.S.—that threaten the right to informational privacy in an unprecedented way. The data collected by the NSA as part of various programs include phone call records; cell phone location information; internet activity; the content of phone conversations; the content of chats and emails; photographs of millions of people's faces; and more.

The outcry following these revelations has triggered a response from a number of international bodies, including the UN General Assembly, which issued a resolution in December of 2013 (entitled "The right to privacy in the digital age") "[r]eaffirming the human right to privacy. . . ."[141] In June of 2014, the OHCHR issued a report that articulated concerns about the human rights implications of widespread electronic surveillance—many of which fall under Article 17 of the ICCPR.[142]

Crucially, some of the programs revealed by Snowden aim to gather enormous volumes of information regardless of whether the people whose informational privacy interests are at stake are suspected of any wrongdoing. This "mass" surveillance raises distinctive and urgent human rights questions, such as whether mass surveillance is almost always arbitrary, given that in practice it is extremely unlikely to pass the four-part non-arbitrariness test, and whether it inherently fails the lawfulness requirement of Article 17.

The governments implicated in the Snowden revelations defend their mass surveillance programs as designed to aid in the pursuit of a legitimate aim—namely, protecting national security. Yet even if mass surveillance provides certain advantages in pursuit of that aim, it will typically be extremely intrusive and wildly disproportionate. The mass, untargeted collection of information on entire populations is perhaps the greatest single act of intrusion into informational privacy interests available to a State. At the same time, there is no evidence available that mass surveillance has noticeably improved the national security of any State that undertakes it.[143] Accordingly, there is no known mass

---

[141] G.A. Res. 64/167, *supra* note 39, at 1.

[142] *The Right to Privacy in the Digital Age*, *supra* note 5. The European Parliament also issued a lengthy report on the practice of mass surveillance. EUROPEAN PARLIAMENT, SCIENCE AND TECHNOLOGIES OPTIONS ASSESSMENT, MASS SURVEILLANCE: PART 1- RISKS AND OPPORTUNITIES RAISED BY THE CURRENT GENERATION OF NETWORK SERVICES AND APPLICATIONS (2014), http://www.europarl.europa.eu/RegData/etudes/STUD/2015/527409/EPRS_STU(2015)527409_REV1_EN.pdf.

[143] *See, e.g.*, Michael Isikoff, *NSA program stopped no terror attacks, says White House Panel member*, NBC NEWS (Dec. 20, 2013), *available at* http://www.nbcnews.com/news/other/nsa-program-stopped-no-terror-attacks-says-white-house-panel-f2D11783588. In fact, the volume of information collected through mass

surveillance program that could even arguably satisfy the proportionality test of the Article 17 arbitrariness assessment.[144]

Additionally, the lawfulness requirement of Article 17 demands that interferences with the right to informational privacy comply with domestic and international law. Even if a domestic statute in a particular State authorizes a mass surveillance program, that program could not be lawful under the ICCPR, as mass surveillance eviscerates the very essence of the human right to privacy.[145] If anything is anathema to the purpose of Article 17, it is the wholesale and deliberate collection of personal data or metadata about millions of people under no suspicion whatsoever.

An update to General Comment 16 should clearly explain the impermissibility of mass surveillance under Article 17, emphasizing the importance of this categorical prohibition in light of troubling, recent patterns in State practice. Article 17 prohibits indiscriminate data collection, and this position is supported by General Comment 16,[146] the practice of the Committee,[147] the European Court of Human Rights,[148] and most recently, an opinion of the European Court of Justice. [149]

Article 17 Obligations Extend Extraterritorially

The surveillance revelations described above have also raised pressing questions as to the territorial scope of State obligations under Article 17. The U.S., for example, conducts surveillance both inside and outside of its borders. It factors in the location of those subject to its surveillance (that is, whether they are within U.S. borders or overseas) when determining the extent of the safeguards it must impose. People outside the U.S. generally receive substantially less protection from surveillance, at least based on those laws and regulations that are publicly available.[150]

---

surveillance is so great that it may weaken national security by overwhelming the analytical capacities of the agencies tasked with defending a given State.

144 The only conceivable configurations that make mass surveillance not arbitrary are fanciful examples, where the data to be collected on everyone are particularly limited and the harm to be prevented is particularly certain and great. *See also*, Emmerson 2014 Report, *supra* note 75, at ¶ 59 (noting a similar point: "The prevention and suppression of terrorism is a public interest imperative of the highest importance and may in principle form the basis of an arguable justification for mass surveillance of the internet. However, the technical reach of the programmes currently in operation is so wide that they could be compatible with article 17 of the covenant only if relevant States are in a position to justify as proportionate the systematic interference with the internet privacy rights of a potentially unlimited number of innocent people located in any part of the world.").

145 *See also*, Emmerson 2014 Report, *supra* note 75, at ¶ 18 (noting that "[t]he very essence of the right to privacy of communication is that infringements must be exceptional, and justified on a case-by-case basis."

146 General Comment 16, *supra* note 3, at ¶ 10.

147 *See e.g.,* U.N. Human Rights Comm., Concluding Observations on Sweden, *supra* note 24, at ¶ 18.

148 *See e.g.,* S. and Marper v. the United Kingdom [GC], App. Nos. 30542/04 and 30566/04, Eur. Ct. H.R., ¶ 119 (2008) (finding that "the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offenses […] fails to strike a fair balance between the competing public and private interests …").

149 Case C-293/12 & C-594/12, Digital Rights Ireland, Ltd. v. Minister for Communications, Marine and Natural Resources, ¶¶ 65-66, 69, 2014.

150 *See* ACLU Submission to the Privacy and Civil Liberties Oversight Board, Section 702, pp. 13-14, *available at* https://www.aclu.org/sites/default/files/assets/aiusaaclusubmissiontopclob.pdf.

Yet all major international bodies that have considered the territorial scope of human rights obligations, including the Committee, have concluded that a State's extraterritorial exercise of effective control over a person or a territory places that person or territory within a State's "jurisdiction."[151] In applying obligations extraterritorially, none of these institutions have drawn a bright-line distinction between State responsibilities toward those located within a State's borders and those located without; indeed, in the modern world of instant global communications, categorical restrictions based on territory are unworkable.[152]

The effective control test is not limited to cases of physical custody or control. Rather, the determining factor is the nature of the right protected.[153] Thus the right to liberty depends to a large extent on custody or power over the individual.[154] However, for obligations to apply in relation to other rights, such as the right to life,[155] the right to property,[156] and nondiscrimination,[157] there is no custodial requirement. A State can interfere with and potentially violate these rights without physical custody. For example,

---

[151] *See* General Comment 31, ¶ 10, U.N. HRC, 80th Sess., U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004) [hereinafter General Comment 31]. In at least thirteen other instances the Committee has upheld the extraterritorial application of the ICCPR, *see* Letter from Amnesty International to Office of the High Commissioner for Human Rights, AI Index: ACT 30/003/2014 (Apr. 1, 2014), *available at* http://www.amnesty.org/en/library/info/ACT30/003/2014/en. For the ICJ, *see* Legal Consequences of the Construction of a Wall in Occupied Palestinian Territory, Advisory Opinion, 2004 I.C.J. 136, ¶ 111 (July 9); *see also*, Armed Activities on Territory of Congo (Dem. Rep. Congo. v. Uganda), 2005 I.C.J. 168, 234 (Dec. 19). For regional human rights bodies, *see* Al-Skeini and Others v. United Kingdom, App. No. 55721/07, Judgment, Eur. Ct. H.R. (July 7, 2011); Issa and Others v. Turkey, App. No. 31821/96, Judgment, Eur. Ct. H.R. (Mar. 30, 2005); Öcalan v. Turkey, App. No. 46221/99, Judgment, Eur. Ct. H.R. ¶¶ 91, 190 (May 12, 2005); Ilascu and Others v. Moldova and Russia, App. No. 48787/99, Judgment, Eur. Ct. H.R., ¶ 311 (Jul. 8, 2004); Victor Saldaño v. Argentina, Inter- Am. Ct. H.R., Petition, Report No. 38/99 ¶ 18 (Mar. 11, 1999); *see also* Coard v. United States, Case 10.951, Inter-Am. Comm'n H.R., Report No. 109/99, OEA/Ser.L/V/II.106, doc. 3 rev. ¶ 37 (1999) (suggesting that the important issue is not the victim's nationality or presence within "a particular geographic area" but whether under the circumstances the government observed rights of those subject to its "authority and control"); Armando Alejandre Jr. and Others v. Cuba ('Brothers to the Rescue'), Case 11589, Inter-Am. Comm'n H.R., Report No. 86/99 (1999).

[152] *See* Sarah Cleveland, *Embedded International Law and the Constitution Abroad*, 110 COLUM. L. REV. 225, 248 (2010).

[153] *See* Manfred Nowak, *What does extraterritorial application of human rights treaties mean in practice?*, JUST SECURITY (Mar. 11, 2014, 8:06 AM), http://justsecurity.org/8087/letter-editor-manfred-nowak-extraterritorial-application-human-rights-treaties-practice/ (stating that "[a] correct interpretation of "effective control" over a person must […] take the specific right at issue into account").

[154] *Id.*

[155] *See* European Court of Human Rights in Issa v. Turkey, App. No. 31821/96, Judgment, Eur. Ct. H.R. (Mar. 30, 2005) (concerning the killing of Iraqi shepherds by Turkish military forces in Iraq); Pad and others v. Turkey, App. No. 60167/00, Eur. Ct. H.R., ¶¶ 53-55 (June 28, 2007). In Pad, some Iranian nationals had been killed by fire from Turkish helicopters, and Turkey was found to have jurisdiction. Whether the events had occurred on the Iranian or Turkish side of the border remained in dispute, but the Court decided that it was not necessary to determine the exact location of the incident, as Turkey had already admitted that its forces had caused the killings by firing upon the victims from helicopters. This decision contradicts the Court's decision in Bankovic, where it found that jurisdiction did not apply in similar circumstances. *See* Bankovic et al. v. Belgium et al., App. No. 52207/99, Grand Chamber Decision, Eur. Ct. H.R. (Dec. 12, 2001).

[156] For example, in Bosphorous Hava Yollari Turizm Ve Ticaret Anonim Sirketi v. Ireland, the European Court of Human Rights held that the seizure in Ireland of an airplane belonging to the applicant, who did not reside within Ireland, meant that the government had jurisdiction over the applicant and was therefore accountable for potential violations. Sirketi v. Ireland, App. No. 45036/98, Eur. Ct. H.R. (June 30, 2005).

[157] *Id.*

a State may exercise power over the right to life (via the ability to kill a person from the air) or the power to expropriate a person's property without having custody of the person.[158]

Another example involves fair trial guarantees and trials in absentia. Even if a defendant is absent and abroad during trial, a State is still obligated to provide that defendant with a fair trial. The right to a fair trial applies not because the person is in the government's physical control, but because the government has exerted control over the person in subjecting them to a criminal trial.[159]

The Human Rights Committee,[160] the Inter-American Commission on Human Rights,[161] the African Commission on Human Rights,[162] the UN Committee on the Elimination of Racial Discrimination,[163] and the UN Committee on the Elimination of Discrimination against Women[164] have all applied their respective human rights instruments to situations in which a State did not have physical custody over the relevant persons, or control over the territory where those persons were located, but rather had power over the rights at issue.[165]

In the context of informational privacy, the extraterritorial reach of the ICCPR is essential. As noted above, recent revelations of large-scale surveillance show that States bound by the ICCPR engage in substantial behavior outside of their own territory (as well as inside of it) that would constitute an interference with the right to informational privacy of the people whose data are collected. An update to General Comment 16

---

158 *See also* Montero v. Uruguay, U.N. Human Rights Comm., Communication No. 106/1981, U.N. Doc. CCPR/C/OP/2 (1983); Mbenge v. Zaire, U.N. Human Rights Comm., Communication No. 16/1977, U.N. Doc. CCPR/C/OP/2 (1983).

159 As one scholar has explained in relation to privacy rights: "If virtual methods can in principle exact the same exact result as physical ones, then there seems to be no valid reason to treat them differently and insist on some kind of direct corporeal interventions." Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in a Digital Age*, HARV. INT'L L.J 58 (forthcoming), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418485.

160 *See* Gueye et al. v. France, U.N. Human Rights Comm., Communication No. 196/1985, U.N. Doc. CCPR/C/35/D/196/1985 (1989).

161 *See* Armando Alejandre Jr. and Others v. Cuba ('Brothers to the Rescue'), Case 11589, Inter-Am. Comm'n H.R., Report No. 86/99 (1999); Saldaño v. Argentina, , Inter- Am. Ct. H.R., Petition, Report No. 38/99 ¶ 18 (Mar. 11, 1999) (holding that, 'a state party to the American Convention may be responsible under certain circumstances for the acts and omissions of its agents which produce effects or are undertaken outside that state's own territory.').

162 African Comm'n. H.R., Association Pour la Sauvegarde de la Paix au Burundi v. Tanzania, Kenya, Uganda, Rwanda, Zaire and Zambia (2003-2004), ¶ 75, Communication No. 157/96 (2003). In that case, the Commission examined whether States imposing the sanctions on Burundi were compliant with the African Charter, even though they had no territorial control or presence in Burundi.

163 U.N. Comm. on the Elimination of Racial Discrimination, *Consideration of Reports Submitted by States Parties Under Article 9 of the Convention, Concluding Observations, United States of America,* ¶ 30, U.N. Doc. CERD/C/USA/CO/6 (2008).

164 UN Committee on the Elimination of Discrimination Against Women, *General Recommendation 28 on the Core Obligations of States Parties under Article 2*, U.N. Doc CEDAW/C/GC/28 (2010) ("States parties are responsible for all their actions affecting human rights, regardless of whether the affected persons are in their territory.").

165 Similar findings by the Committee on Economic, Social and Cultural Rights and the Committee on the Rights of the Child are not listed here as those extraterritorial obligations are partially founded on obligations of international cooperation and assistance contained in the relevant treaties.

should emphasize this point. It should also note that modern developments illustrate that if States' Article 17 obligations did not extend extraterritorially, and each State were able to interfere with the informational privacy interests of countless foreigners, then no State would be able to live up to its ICCPR obligations to protect the right to privacy for those within its territory and jurisdiction.[166]

Discrimination is Sharply Restricted under Article 17

In addition to differentiating between surveillance conducted inside and outside of their borders, States have also been offering different levels of protection to individuals affected by surveillance based on their citizenship or residency status.[167] Those who are not citizens or residents of the U.S., for example, are vulnerable to an extraordinarily powerful surveillance apparatus and are protected by very few safeguards.[168]

This is deeply troubling, for non-discrimination and equal protection of the law are fundamental requirements of human rights,[169] and they combine with the extra-territorial reach of the ICCPR to impose meaningful restrictions on State practices that have particularly significant implications for informational privacy.[170] The ICCPR prohibits discrimination with regard to all rights and benefits recognized by law, including between citizens and non-citizens.[171] The Committee has identified privacy, freedom of expression, and freedom of association as rights for which "[t]here shall be no discrimination between aliens and citizens."[172]

Thus, measures aimed at restricting interferences with informational privacy should, as a general matter, be extended equally to everyone regardless of nationality.[173] Under the ICCPR, it is impermissible to treat people differently based purely on prohibited grounds (such as those listed in Article 2(1)); differentiating among people is only permissible if

---

166 G. Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. 861, 902-3 (2014); *The Right to Privacy in the Digital Age, supra* note 5, at ¶ 33 (failing to include effective control would undermine the essence of the right).

167 These countries include the United States, Australia, New Zealand and the United Kingdom. *See* Milanovic, *supra* note 159; IRA RUBENSTEIN ET AL., CENTER FOR DEMOCRACY & TECHNOLOGY, SYSTEMATIC GOVERNMENT ACCESS TO PERSONAL DATA: A COMPARATIVE ANALYSIS (2013), https://www.cdt.org/files/pdfs/govaccess2013/government-access-to-data-comparative-analysis.pdf.

168 *See, e.g.,* Emmerson 2014 Report, *supra* note 75, at ¶ 23. Under some regulations, non-citizens and non-residents that the government believes are located inside the U.S. receive better protections than their overseas counterparts, however.

169 General Comment 18, ¶ 1, U.N. HRC, 37th Sess., U.N. Doc. HRI/GEN/1/Rev. 1 (1994) [hereinafter General Comment 18]. *See also* Emmerson 2014 Report, *supra* note 75, at ¶ 62.

170 *See* Emmerson 2014 Report, *supra* note 75, at ¶ 43 (making this connection as well).

171 ICCPR, art. 26; General Comment 15, ¶ 2, U.N. HRC, 27th Sess., U.N. Doc. HRI/GEN/1/Rev.1 (1986) ("The general rule is that each one of the rights of the Covenant must be guaranteed without discrimination between citizens and aliens").

172 *Id.* at ¶ 7 ("[Aliens] may not be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence. They have the right to freedom of thought, conscience and religion, and the right to hold opinions and to express them. Aliens receive the benefit of the right of peaceful assembly and of freedom of association. Aliens are entitled to equal protection by the law. There shall be no discrimination between aliens and citizens in the application of these rights. These rights of aliens may be qualified only by such limitations as may be lawfully imposed under the Covenant.").

173 Emmerson 2014 Report, *supra* note 75, at ¶ 43; *The Right to Privacy in the Digital Age*, *supra* note 5, at ¶36.

the criteria for doing so are reasonable, objective, and based on a legitimate purpose.[174] The Committee has already criticized States Parties for failure to observe this requirement. For example, in its March 2014 report on the U.S., the Committee expressed concern about U.S. law's "limited protection against excessive surveillance" for non-citizens.[175] It called on the U.S. "to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity *regardless of the nationality or location of individuals whose communications are under direct surveillance*."[176]

The Committee has also noted that "the enjoyment of Covenant rights is not limited to citizens of States parties but must also be available to all individuals . . . who may find themselves in the territory or subject to the jurisdiction of the State party."[177] There is no territorial limit on the equal protection provision of the ICCPR; the issue of the jurisdictional scope of the ICCPR is a separate one.

An update to General Comment 16 should reaffirm the applicability of this non-discrimination principle specifically in the context of informational privacy.

Conclusion

There is a pressing need for the Committee to modernize General Comment 16 to address informational privacy. Although General Comment 16 provides some important analysis of the components of Article 17 protections, it is a limited exposition of a complex right—a right that has taken on a new meaning in recent years. General Comment 16 understandably fails to anticipate or account for modern technological developments that have rapidly, drastically, and fundamentally changed the nature of privacy and the relationship between public and private spheres. Without an update to General Comment 16 that addresses informational privacy, the international community risks further erosion of important privacy protections, seriously undermining the object and purpose of the ICCPR.

The foregoing analysis lays down the building blocks for such an update. In sum, the update should reflect the values underlying informational privacy; provide an explanation of what the concepts of "privacy," "home" and "correspondence" mean in light of new technologies; and provide a framework for what constitutes "interference" with informational privacy that is "unlawful" or "arbitrary." The update should also address current, controversial, and complicated issues that have implications for informational privacy in the modern era, such as surveillance, and other forms of data collection, retention, and use. These principles, and the accompanying appendix, are offered primarily to provide a starting point for further Committee discussion. Any finalized update arising out of the debate will, of course, be the sole responsibility of the

[174] General Comment 18, *supra* note 169, at ¶ 13.
[175] U.N. Human Rights Comm., 2014 Concluding Observations on the U.S., *supra* note 14, at ¶ 22.
[176] *Id.* (emphasis added).
[177] General Comment 31, *supra* note 151, at ¶ 10 (emphasis added).

Committee, guided by the jurisprudence it has developed through Views and Concluding Observations, and enriched by references to global trends in privacy protection.

If privacy is to remain protected in today's rapidly changing world, and if the ICCPR is to retain its resonance as a leading instrument to ensure that protection, it is imperative that the Committee begins the process of updating General Comment 16 today.

Appendix 1: A Model General Comment Highlighting the Right to Informational Privacy

I. General remarks

1. This General Comment updates General Comment 16 (thirty-second session).

2. The right to privacy, including informational privacy, is foundational for the healthy development of self and community. The right ensures a proper balance between the public and private spheres.

3. Paragraph 1 of Article 17 protects both the right to privacy and the right not to have one's honor and reputation attacked. The reference to "privacy, home, family, or correspondence" aims to express a continuous range of privacy protections rather than to provide for individuated rights. These terms are meant to be construed broadly. Paragraph 2 of Article 17 underscores that everyone is entitled to the protection of the law in relation to both rights listed in paragraph 1.

4. Article 17 has a wide reach. Paragraph 1 states that "no one" shall have their right to privacy arbitrarily or unlawfully interfered with, or their honor or reputation unlawfully attacked. Paragraph 2 maintains that "everyone" has the right to protection of the law in this context.

"Privacy"

5. Privacy serves a constellation of values. The right to privacy ensures a sphere is reserved for self-expression of identity.[1] In this way, the right is closely connected to the right to freedom of expression in Article 19 of the Covenant, as discussed further below. The right to privacy also protects intimacy[2] and dignity.[3] Further, it extends to the right to make choices about how to live,[4] and the right to autonomy more broadly. The right to privacy encompasses informational privacy,

[1] Coeriel et al. v. The Netherlands, U.N. Human Rights Comm., Communication No. 453/1991 at ¶ 10.2, U.N. Doc. CCPR/C/52/D/453/1991 (1994); *see, e.g.,* Ituango Massacres v. Colombia, Judgment, Inter-Am. Ct. of H.R., ¶¶ 193-194 (2006); Article 11 of the ACHR contains a similar, but not identical, protection of privacy to Article 17 of the ICCPR.
[2] Toonen v. Australia, U.N. Human Rights Comm., Communication No. 488/1992 at ¶ 7.6, U.N. Doc. CCPR/C/50/D/488/1992 (1994).
[3] Clement Boodoo v. Trinidad and Tobago, U.N. Human Rights Comm., Communication No. 721/1996 at ¶ 6.7, U.N. Doc. CCPR/C/74/D/721/1996 (2002). *See, e.g.*, Murillo v. Costa Rica, Judgment, Inter-Am. Ct. H.R., ¶ 143 (2012): "The protection of private life encompasses a series of factors associated with the dignity of the individual, including, for example, the ability to develop his or her own personality and aspirations, to determine his or her own identity and to define his or her own personal relationships.". As noted above, the right to privacy is expressed differently in the ACHR, but the difference is slight – and the conceptual analysis remains valuable.
[4] Hertzberg et al. v. Finland, U.N. Human Rights Comm., Communication No. 61/1979, Appendix, U.N. Doc. CCPR/C/15/D/61/1979 (1982).

including the right to access and control one's personal information, whether in electronic form or otherwise.[5] These subcomponents of privacy are not exhaustive; rather, they guide future elaboration of privacy protections.

6. No artificial distinctions ought to be drawn when defining "privacy." In particular, both the metadata related to communications or transaction, and the contents of communications can warrant protection under Article 17. In an age when modern information technologies allow for cost-effective mass collection, storage, and synthesis of personal data, as well as monitoring of individuals wherever they are located (including monitoring of their online activities), metadata and content can both be important to an individual's maintenance of a sphere of private life.[6]

"Home" and "correspondence"

7. In addition to "privacy," paragraph 1 of Article 17 assures the protection of the "family," the "home," and "correspondence." Those terms should be understood broadly to ensure the protection of informational privacy in the digital age.[7] The term "home," for example, should be given a generous construction to include virtual and online personal spaces, as well as personal computers and handheld electronic devices.[8] Additionally, the term "correspondence" highlights the importance of the protection of privacy of a broad array of communications, including electronic communications, and the need to curb controls or censorship of such communications.[9] Indeed, the Committee has long equated telephone calls with "correspondence."[10]

8. The General Assembly has confirmed that "the same rights people have offline must also be protected online, including the right to privacy."[11] Accordingly, it is important that, where concepts of "family," "home," and "correspondence" have

[5] General Comment 16, ¶ 10, U.N. GAOR, 43rd Sess., Suppl. No. 40, U.N. Doc. A/43/40 (1988) [hereinafter General Comment 16].
[6] Case C-293/12 & C-594/12, Digital Rights Ireland, Ltd. v. Minister for Communications, Marine and Natural Resources, ¶¶ 26, 69 (2014); Felten Decl. at ¶ 62, *ACLU v. Clapper*, --- F. Supp. 2d ----, No. 13-cv-3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013) *available at* https://www.aclu.org/files/pdfs/natsec/clapper/2013.08.26%20ACLU%20PI%20Brief%20-%20Declaration%20-%20Felten.pdf (J. Pettiti, concurring).
[7] Soo Ja Lim et al. v. Australia, U.N. Human Rights Comm., Communication No. 1175/2003 at ¶ 4.10, U.N. Doc. CCPR/C/87/D/1175/2003 (2006).
[8] *See, e.g.*, Peiris v. Sri Lanka, U.N. Human Rights Comm., Communication No. 1862/2009, U.N. Doc. CCPR/C/103/D/1862/2009 (2012). *See also*, Bernh Larsen Holding AS and Ors. v. Norway, App. No. 24117/08, Judgment, Eur. Ct. H .R., ¶ 106 (2013).
[9] Miguel Angel Estrella v. Uruguay, U.N. Human Rights Comm., Communication No. 74/1980 at 150, U.N. Doc. Supp. No. 40 (A/38/40) (1983).
[10] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant*, *Concluding Observations, Bulgaria*, ¶ 22, U.N. Doc. CCPR/C/BGR/CO/3 (Aug. 19, 2011). Additionally, "private life" and "correspondence" as defined by Article 8 of the European Convention have been interpreted to include e-mails and information derived from monitoring personal Internet usage. Copland v. the United Kingdom, App. No. 62617/00, Judgment, Eur. Ct. H.R., ¶¶ 43-44 (Apr. 3, 2007).
[11] G.A. Res. 68/167, U.N. Doc. A/RES/68/167 (Dec. 18, 2013).

digital or virtual equivalents, equal protection is afforded both to online and offline manifestations of these concepts. Thus, email and electronic communications that constitute "correspondence" must receive the same protection as letters and other communications that have previously been the subject of Committee jurisprudence.[12]

Implementing these rights

9. The rights guaranteed in Article 17 are to be protected from all unlawful and arbitrary interferences and attacks, whether these emanate from States Parties or private actors. States must also adopt legislative and other measures to give effect to the prohibitions on these interferences and attacks.[13] Paragraph 2 of Article 17 underscores the need for protection of the law and also reaffirms that discretionary powers (for example, those exercised by executive authorities) ought to be regulated by law where privacy interests might be engaged. It also highlights the need for safeguards to prevent abuse, and the establishment of independent and effective judicial or administrative oversight of any conduct that may potentially implicate privacy interests.[14]

10. The obligations imposed by the Covenant may extend extraterritorially. It is necessary to reinforce this point in particular for informational privacy, given the nature of digital communications networks and the consequent increased potential for cross-border violations of the right. As noted in Article 2(1) of the Covenant, States must respect and ensure rights for all individuals subject to their territory or jurisdiction.[15] Therefore a State Party must ensure protection of rights to everyone within its territory, and to everyone within the power or effective control (including virtual power or effective virtual control) of that State Party outside of its territory.[16] Individuals subject to surveillance by a foreign State Party are within the power of that State Party for the purposes of Article 17.[17] The view that the Covenant has no extraterritorial reach is contrary to the consistent interpretation of the Covenant.[18]

---

[12] Pinkney v. Canada, U.N. Human Rights Comm., Communication No. 27/1978 at ¶ 34, U.N. Doc. CCPR/C/OP/1 (1985).
[13] *See, e.g.*, General Comment 16, *supra* note 5.
[14] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, The Netherlands*, ¶ 15, U.N. Doc. CCPR/C/NLD/CO/4 (2009) [hereinafter U.N. Human Rights Comm., Concluding Observations on the Netherlands].
[15] *See also*, General Comment 31, ¶ 10, U.N. HRC, 80th Sess., U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004) [hereinafter General Comment 31].
[16] *Id.*
[17] *See* Manfred Nowak, *What does extraterritorial application of human rights treaties mean in practice?*, JUST SECURITY (Mar. 11, 2014, 8:06 AM), http://justsecurity.org/8087/letter-editor-manfred-nowak-extraterritorial-application-human-rights-treaties-practice/(stating that "[a] correct interpretation of "effective control" over a person must […] take the specific right at issue into account").
[18] General Comment 31, *supra* note 15, at ¶ 10. In at least thirteen other instances the Committee has upheld the extraterritorial application of the ICCPR, *see* Letter from Amnesty International to Office of the High Commissioner for Human Rights, AI Index: ACT 30/003/2014 (Apr. 1, 2014), *available at* http://www.amnesty.org/en/library/info/ACT30/003/2014/en.

11. Article 2(1) of the Covenant also makes clear that rights must be respected and ensured in a manner consistent with the principle of non-discrimination. Distinctions based purely on national origin, for example, are prohibited.

12. States Parties must also ensure effective remedies to victims where arbitrary or unlawful interferences with privacy occur, or where there are unlawful attacks on a person's honor or reputation.[19]

II. Limitations on the right to privacy

13. Privacy is not an absolute right under Article 17. Although the Covenant does not enumerate the permissible reasons for limiting a person's right to privacy, paragraph 1 requires that an interference with the privacy, family, home, and correspondence of a person be neither "arbitrary" nor "unlawful."

14. Paragraph 2 of Article 17 provides for every person's right to the "protection of the law" against arbitrary or unlawful interference of privacy. Respect for legal norms, including those laid out in the ICCPR, must characterize any governmental activity that engages privacy interests.

15. Unlike Article 19, paragraph 3 of the ICCPR (relating to freedom of expression), or Article 8, paragraph 2 of the European Convention of Human Rights (relating to privacy), the text of Article 17 does not contain any specific exceptions limiting the enjoyment of privacy. The absence of built-in restrictions highlights the need for the robust protection of privacy under the ICCPR. Under Article 17, States must narrowly interpret the permissible interferences with the right to privacy.[20]

16. While Article 17 does not list the valid limitations on the right to privacy, the reasons for limiting the right are widely understood to encompass only the standard reasons countenanced by the ICCPR (as listed, for example, in Article 19). Those include: respect of the rights or reputations of others, the protection of national security, the protection of public order, or the protection of public health or morals. If States Parties seek further reasons for limiting the right to privacy, they must derogate from the right, as permitted under Article 4 of the Covenant, or they must propose a relevant amendment to the right that takes effect under the procedures detailed in Article 51 of the Covenant.

---

[19] Bulgakov v. Ukraine, U.N. Human Rights Comm., Communication No. 1803/2008 at ¶ 9, U.N. Doc. CCPR/C/106/D/1803/2008 (2012).

[20] *See generally*, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, ¶¶ 14-19, OHCHR, U.N. Doc. A/HRC/13/37 (Dec. 28, 2009) (Martin Scheinin) [hereinafter Special Rapporteur 2009 Report].

"Interference"

17. The interpretation of "interference" under Article 17 must account for recent advances in information technology, the now-artificial distinction between metadata and content, the erosion of boundaries between the public and private spheres, and the modern day capacities of States Parties to infringe persons' rights to privacy by tracking Internet and other electronic activities, and collecting, storing, and synthesizing electronic data.

18. The term "interference" includes, among other things, the simple collection or storage of protected personal information or communications, as well as any manual or automated searching, review, obstruction, duplication, or diversion of protected information or communications.[21]

19. The term "interference" encompasses indirect interference or the threat of interference if a person is able to show that the challenged action or legislative provision poses a reasonably probable threat to the enjoyment of their privacy, or produces a chilling effect on other protected activity by implicating their privacy.[22] This applies, for example, to cases where a person is able to show good reason for which he or she may be (or is communicating with someone who may be) the subject of surveillance, even if, in fact, the person (or his or her contact) turn out not to have been such a subject. In these cases a person shall be deemed a "victim" within the meaning of Article 1 of the Optional Protocol to the Covenant.

20. The collection of protected data about communications, or metadata, also constitutes a prima facie interference with the right to privacy.[23]

"Unlawful"

21. Interference with the privacy of a person must not be "unlawful." Four conditions must be met for interference to be lawful. First, the interference must occur pursuant to, and in accordance with, valid, enacted law that complies with international standards, such as the aims and objectives of the Covenant itself.[24] Second, the applicable statutory framework must be accessible to ensure that any

[21] General Comment No. 16, *supra* note 5, at ¶ 10; Copland v. the United Kingdom, App. No. 62617/00, Judgment, Eur. Ct. H.R., ¶ 43 (2007).
[22] Toonen v. Australia, U.N. Human Rights Comm., Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (1994).
[23] Malone v. the United Kingdom, App. No. 8691/79, Judgment, Eur. Ct. H.R., ¶ 67 (1984); Uzun v. Germany, App. No. 35623/05, Judgment, Eur. Ct. H.R., ¶¶ 49-53 (Sept. 2, 2010).
[24] Escher et al. v. Brazil, Preliminary Objections, Merits, Reparations, and Costs, Inter-Am. Ct. H.R. (ser. C) No. 200, ¶ 116 (2009); Tristán Donoso v. Panamá, Preliminary Objections, Merits, Reparations and Costs, Inter-Am. Ct. H.R. (ser. C) No. 193, ¶ 56 (2009); Kennedy v. the United Kingdom, App. No. 26839/05, Judgment, Eur. Ct. H.R., ¶ 151 (2010); Malone v. the United Kingdom, App. No. 8691/79, Judgment, Eur. Ct. H.R., ¶¶ 66, 68 (1984). Whilst the language of the ACHR and the ECHR is distinguishable from the ICCPR, the differences are not material in this context.

interference with privacy interests is reasonably foreseeable to those who suffer that interference.[25] Third, applicable law must be "precise" and "clearly" defined.[26] Fourth, the surveillance must be subject to sufficient safeguards, which includes, among other things, adequate oversight and access to redress for victims of impermissible interferences.

22. These lawfulness requirements mirror the test established by the Committee in General Comment 34 and the "quality of law" test developed by the European Court of Human Rights in interpreting various articles of the European Convention, which refer to the need for limitations on rights to be "prescribed by law."[27] These same tests should guide the meaning of "unlawful" under Article 17 of the ICCPR.

23. The term "unlawful" "means that no interference may take place except in cases *envisaged by the law*."[28] Interferences with the right to privacy must therefore occur under laws that are duly enacted. Further, the lawfulness assessment also encompasses the very laws that govern interferences; such laws must always conform to the requisite international standards, including the aims and objectives of the Covenant itself.[29]

24. Accessibility and foreseeability jointly require that laws and regulations governing privacy interests be available to the public. Foresight of the potential consequences of given conduct allows individuals to regulate their conduct in accordance with the law, and to empower them to avoid unnecessary interferences with their privacy.[30] Clarity and precision of the applicable laws is also essential for foreseeability, and impossible without publicity. Both are required by General Comment 16.[31] Together, these second and third requirements provide some measure of protection against the possibility of

[25] S.W. v. the United Kingdom, App. No. 20166/92, Judgment, Eur. Ct. H.R. (ser. A no. 335-B), ¶¶ 44-48 (1995); K.-H.W. v. Germany [GC], App. No. 37201/97, Judgment, Eur. Ct. H.R., ¶¶ 72-76 (2001) (extracts).
[26] U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Jamaica*, ¶ 20, U.N. Doc. CCPR/C/79/Add.83 (Nov. 19, 1997) [hereinafter U.N. Human Rights Comm., Concluding Observations on Jamaica]; U.N. Human Rights Comm., *Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Comments, Russian Federation*, ¶ 19, U.N. Doc. CCPR/C/79/Add.54 (July 26, 1995) [hereinafter U.N. Human Rights Comm., Concluding Observations on Russia]; General Comment 16, *supra* note 5, at ¶¶ 3, 8.
[27] Kafkaris v. Cyprus [GC], App. No. 21906/04, Judgment, Eur. Ct. H.R., ¶¶ 150-152 (2008).
[28] General Comment 16, *supra* note 5, at ¶ 3 (emphasis added).
[29] Jorgic v. Germany, App. No. 74613/01, Judgment, Eur. Ct. H.R., ¶¶ 67-68 (July 12, 2007); Kononov v. Latvia [GC], App. No. 36376/04, Judgment, Eur. Ct. H.R., ¶¶ 232-244 (2010).
[30] Kafkaris v. Cyprus [GC], App. No. 21906/04, Judgment, Eur. Ct. H.R., ¶¶ 150-152 (2008); Hashman and Harrup v. the United Kingdom [GC], App. No. 25594/94, Judgment, Eur. Ct. H.R., ¶ 31 (1999); Malone v. the United Kingdom, App. No. 8691/79, Judgment, Eur. Ct. H.R., ¶¶ 83-84 (Aug. 2, 1984).
[31] General Comment 16, *supra* note 5, at ¶ 8 ("relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted.").

interference through executive acts, which might otherwise be undertaken or enacted absent adequate public knowledge or understanding.[32]

25. The fourth requirement, which demands adequate safeguards for activities that threaten privacy, serves as a check on the potential for abuse of power. It is essential for States to maintain prospective and retrospective accountability for those with the power to interfere with privacy, even as provided for under a legal framework that meets the first three requirements. Adequate oversight and access to redress are required by the Covenant.

"Arbitrary"

26. The requirement for non-arbitrariness is distinct from the requirement that interference be lawful.

27. Within the meaning of paragraph 1 of Article 17, the term "arbitrary" should be construed to incorporate a structured proportionality review. A non-arbitrary privacy-infringing measure must satisfy the following criteria. First, the interference must have a legitimate purpose, understood in the context of the Covenant. Second, the interference must be necessary to achieving its stipulated aim. Third, the interference must represent the least intrusive means of realizing its aim. Fourth, the magnitude of the interference must be proportionate—that is, fairly balanced against the purpose to be achieved.[33]

28. A proportionality test is the correct method of interpreting "arbitrary" in relation to Article 17 because it incorporates a clear framework; has been developed across multiple jurisdictions;[34] and, when used properly, ensures that interferences with privacy will be consistent with the aims, objectives, and purposes of the Covenant. In short, it requires States to give adequate weight to the rights listed in Article 17 when devising measures that stand to interfere with privacy.

29. This proportionality test applies even in cases where national security concerns are implicated. Thus, it is helpful to recall paragraph 1 of Article 5 of the Covenant, which prohibits States Parties or any person from engaging in an

---

[32] *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* ¶ 35, OHCHR, U.N. Doc. A/HRC/69/397 (Sept. 23, 2014) (Ben Emmerson).
[33] Toonen v. Australia, U.N. Human Rights Comm., Communication No. 488/1992 at ¶ 14, U.N. Doc. CCPR/C/50/D/488/1992 (1994); Dudgeon v. United Kingdom, App. No. 7525/76, Judgment, Eur. Ct. H.R., ¶¶ 53, 59 (1981); Klass and Others v. Germany, App. No. 5029/71, Judgment, Eur. Ct. H.R. (Series A no. 28), ¶¶ 42, 59 (Sep. 6, 1978). *See also,* Special Rapporteur 2009 Report, *supra* note 20, at ¶¶ 14-18.
[34] *See, e.g.* R. (Daly) v. Secretary of State for the Home Department, [2001] 2 AC 532, ¶ 547; Federal Constitutional Court (*Bundesverfassungsgericht*) decision of 27 February 2008, reference number: 1 BvR 370/07, *available at* http://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html (in Germany); STC 7/2004 and STC 261/2005 (in Spain).

activity that limits rights to "a greater extent than provided for in the present Covenant."

III. Mass Surveillance

30. Mass (or bulk) surveillance, whether of the contents of protected communications or of protected metadata, violates the spirit or purpose of the right to privacy by entailing the wholesale collection of protected information concerning many people suspected of no wrongdoing whatsoever. Such surveillance cannot be authorized by a law that conforms to the aims and objectives of the Covenant, and is therefore inherently unlawful. The acquisition or accessing of protected data or metadata constitutes mass surveillance when it occurs on a large scale and is insufficiently discriminate in whose privacy interests it harms.

31. Mass surveillance will almost always be an arbitrary interference with the right to privacy as well, for by collecting protected information on countless people who are not suspected of wrongdoing, it typically involves a massive intrusion into privacy rights that will practically never be proportionate to the State's pursuit of a legitimate aim.[35]

IV. Relationship of Article 17 and other articles of the Covenant

32. Article 17 overlaps and interacts with many other articles in the Covenant. The right to liberty and security of person, expressed in Article 9, rests on some of the same values as Article 17. In particular, both Article 9 and Article 17 respect interests in liberty and a protected sphere of action. In addition, paragraph 1 of Article 9 emphasises the importance of legal procedures and protections, bearing some resemblance to paragraph 2 of Article 17.

33. Violations of Article 17 threaten other rights in the Covenant as well. For example, as observed by the Special Rapporteur on the protection and promotion of the right to freedom of expression and opinion, insufficient privacy protections for communications may have a chilling effect on such communications, undermining the right to freedom of expression under Article 19 of the Covenant.[36] In addition, harms to privacy rights also jeopardize freedom of thought (Article 18 of the Covenant), freedom of association (Article 22), and participation in public affairs (Article 25). The linkages between these rights are especially pronounced in online communications. Concern over the

[35] *See e.g.*, S. and Marper v. the United Kingdom [GC], App. Nos. 30542/04 and 30566/04, Eur. Ct. H.R., ¶ 103 (2008); Case C-293/12 & C-594/12, Digital Rights Ireland, Ltd. v. Minister for Communications, Marine and Natural Resources, ¶¶ 65-66, 69 (2014).

[36] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, OHCHR, U.N. Doc. A/HRC/23/40, ¶¶ 24-27 (Apr. 17, 2013) (by Frank La Rue). *See also*, U.N. Human Rights Council, *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, OHCHR, U.N. Doc. A/HRC/27/37 (June 30, 2014).

privacy of online activity may deter an individual from engaging at all online, thereby significantly limiting that individual's rights to freedom of speech, freedom of thought, freedom of association, and political participation.