PRIVACY RIGHTS IN THE DIGITAL AGE

A Proposal for a New General Comment on the Right to Privacy under Article 17 of the International Covenant on Civil and Political Rights:

A Draft Report and General Comment by the American Civil Liberties Union

March 2014

ACLU
AMERICAN CIVIL LIBERTIES UNION

Privacy Rights in the Digital Age

A Proposal for a New General Comment
on the Right to Privacy under Article 17 of the
International Covenant on Civil and Political Rights:

A Draft Report and General Comment 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	3
Introduction	5
The Role of General Comments	7
The Need to Revise or Replace General Comment 16	8
Principles for a Modern Right to Privacy under the ICCPR	12
Conclusion	30
Appendix 1: A Draft Revised General Comment	32

Executive Summary

Article 17 of the International Covenant on Civil and Political Rights (ICCPR) protects everyone from arbitrary or unlawful interferences with their "privacy, family, home or correspondence." Since the ICCPR came into force in 1976, new information technologies have emerged and both governments and private companies have at times employed them outside of any legal framework and without regard to individual privacy. Billions of people worldwide now use the Internet as their primary mode of communication in conducting their private and professional affairs. Internet companies collect information about us for advertising and marketing purposes. Other companies use sophisticated tools to create detailed personal profiles from this information, which they sell to yet other companies that seek to monetize everything from our habits to our health, from our sexual orientation to our finances. And, as Edward Snowden has revealed, modern technologies to secretly collect and store massive amounts of data on the most intimate details of people worldwide.

The international human rights community has begun the process of responding to the erosion of privacy rights that these information technologies have facilitated. The U.N. Human Rights Committee should assist in this process by issuing a new General Comment on the right to privacy under Article 17 of the ICCPR.

The Need for A New General Comment

General Comments serve an important function. They elaborate on, and develop, open-textured rights language; they collate jurisprudence on a right; and they clarify the application of a right to specific contexts. They ensure that the treaty monitoring body properly and consistently interprets the right in its practice of reviewing individual petitions and country reports. General Comments also provide a framework that allows State Parties to ensure their compliance with protected rights.

To achieve these aims, the existing General Comment on Article 17—General Comment 16—should be replaced. In its practice, the Committee has superceded existing General Comments where necessary and appropriate to develop the content of protected rights and to more accurately reflect changing realities and developments in the law and policy.

Adopted by the Human Rights Committee in 1988, General Comment 16 establishes important human rights principles and guarantees against state intrusions on privacy. Yet a new General Comment to replace it is warranted, for four main reasons:

- the Internet has emerged as the world's primary mode of global communication;
- sophisticated modern technologies can infringe on privacy rights through the collection, storage, analysis, and dissemination of publicly available and private information;
- there is an increasingly symbiotic relationship between the protection of privacy rights and the freedom of expression, freedom of association and other rights guaranteed by the ICCPR; and
- the Human Rights Committee has made determinations on individual petitions and made Concluding Observations on Article 17 that should be reflected in a new General Comment.

A new General Comment is required to clarify use of the terms "privacy," "home," and "correspondence" as used in Article 17 so that they more accurately describe their meaning in a society in which billions of people worldwide increasingly communicate and otherwise conduct their personal and working lives online.

Clarification on what constitutes an "interference" with privacy rights is also required. Modern technologies now enable State Parties and corporations to collect, store, and synthesize information on a scale unimaginable in the 1980s. State Parties have enacted new laws or interpreted existing laws to facilitate these processes, often without sufficient regard for privacy interests. General Comment 16 was written well before these laws and practices developed—indeed, in many cases, even before they could have been anticipated. Yet international human rights bodies, including the Committee, have made clear that such legislation or practices may infringe on privacy, and that the mere collection and storage of data—even data that is publicly accessible—may constitute an "interference" that is subject to the constraints imposed by Article 17.

Privacy protections under Article 17 are not absolute, but may be restricted in certain, narrowly defined circumstances. A new General Comment would provide more concrete guidance on those circumstances, taking into consideration the increased capacity of State Parties and corporations to interfere with privacy interests through use of modern information technologies.

International Human Rights Law Requirements for Interferences With Privacy Interests

Article 17 prohibits "arbitrary or unlawful" interferences with the right to privacy. General Comment 16 provides important guidance on these terms, but a new General Comment could additionally reflect the Committee and other international human rights bodies' consideration of recent state practices and new technologies. A growing catalogue of human rights jurisprudence and commentary outlines conditions that must be met for an interference with privacy to be lawful and non-arbitrary.

In short, any interference with the right to privacy must be:

(1) consistent with the provisions, aims, and objectives of the ICCPR;
(2) carried out pursuant to the requirements of domestic and international law;
(3) established by laws that the public can fully access, with measures that are precise, specific, and clearly defined, such that an impacted individual can foresee any interference; and
(4) proportionally and rationally connected to a legitimate state aim, such as law enforcement or national security, minimally impairing the right to privacy, and striking a fair balance between pursuit of the aim and limitation on the right.

As recent revelations have made clear, modern surveillance technologies allow for the most far-reaching impact on privacy rights. A new General Comment should reaffirm the relevance of human rights principles to current surveillance practices, by making clear that:

- indiscriminate mass surveillance contravenes Article 17 because it is an arbitrary interference with privacy and that mass collection and retention of data violates Article 17 because it is an arbitrary or a disproportionate measure;
- any interference with the right to privacy should be subject to independent and effective judicial oversight, a position emphasized by Article 17(2);
- Article 17 applies extraterritorially and must be respected whenever individuals are within a State's "jurisdiction" (that is, power or effective control—including virtual power or virtual control);
- laws on privacy and surveillance must not be discriminatory and must protect both non-nationals and nationals; and that
- states have positive duties to protect the right to privacy from interferences by private parties and to ensure effective remedies for victims of privacy breaches.

Introduction

Privacy is a concept central to our identities, our ability to control information and our senses of self, and our interactions with other individuals and communities. Yet recent developments have called into question the extent to which traditional understandings of privacy remain viable in modern times. Documents leaked by Nobel Prize-nominated whistleblower Edward Snowden's have exposed vast global surveillance programs conducted by governments, commercial entities, and others—with seemingly little regard for the privacy interests of innocent individuals around the world.

In the wake of Snowden's leaks, lawyers and commentators have recognized that while surveillance and information technologies have developed rapidly, the law of privacy has not kept pace with these changes. Although privacy law, at the international human rights level, is grounded in robust and pedigreed principles, it seems not to have been developed or adapted to fit the needs of 21st century society. To take just a few examples, the original General Comment on privacy, published in 1988, did not anticipate: the development of different forms of electronic communication, including mobile and computer technologies, which now play such a central part in our lives; the emergence of State capacities to intercept and process large quantities of electronic data; the explosion of social media websites such as Facebook; or the fact that almost 2.5 billion people around the world are now Internet users.[1]

[1] *See, e.g.*, Miniwatts Marketing Group, *World Internet Usage and Population Statistics*, INTERNET WORLD STATS (30 June, 2012), http://www.internetworldstats.com/stats.htm. Regional and international statements have also taken into account changing circumstances: *see, e.g.,* U.N. GAOR, 68th Sess., 3rd comm. mtg., U.N. Doc. A/RES/68/167 (Dec. 18, 2013); *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* at 3-20, OHCHR, U.N. Doc. A/HRC/23/40 (April 17, 2013) (by Frank La Rue), [hereinafter Special Rapporteur 2013 Report]; Inter-American Commission on Human Rights' 28 October 2013 hearing on NSA surveillance and human rights; European Parliament Committee on Civil Liberties, Justice and Home Affairs, *Draft Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs* (Jan. 8, 2014) *available at*

This report reviews the work of the United Nations Human Rights Committee (HRC) with respect to the right to privacy under the International Covenant on Civil and Political Rights (ICCPR) in light of these developments, and it recommends that the HRC publish a new General Comment on privacy rights under Article 17 of the ICCPR. Article 17 articulates a complex right, which is partly elucidated in General Comment 16. However, General Comment 16 is brief and rooted in an outdated understanding of modern communications infrastructure, and it is therefore imperative that the HRC review, update, and replace it. The HRC has been willing to replace other General Comments (on freedom of expression and liberty and security of the person, for instance) to account for the evolving realities of modern life. The principles for the new General Comment are sourced primarily in the work of United Nations human rights bodies—in the HRC's views, the HRC's country reports, and in the related work of various Special Rapporteurs—but they can also be informed by developments in the law on privacy in regional and national jurisdictions, such as the European Court of Human Rights.

The report takes the following structure. First, the report offers theoretical sections that address the role of General Comments generally and the present need to update General Comment 16 in particular. Next, the report discusses and analyzes the principles that ought to underpin a new General Comment on privacy. Finally, a draft revised General Comment on the right to privacy, to replace General Comment 16, is included as an appendix.

In an era of increasingly sophisticated information technology with the capacity to collect, store and analyze huge amounts of information, there is an urgent need for the HRC to replace General Comment 16 to provide authoritative guidance to the Committee and State Parties on the nature and scope of privacy protections under Article 17. What is also clear, though, is that the principles underlying 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 United Nations 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.

States patently have an interest in maintaining security and protecting their citizens, and those rival interests have also developed in the years since the drafting of General Comment 16. But for those interests to be properly considered against the need for privacy protection, the legal framework around the right to privacy must be updated and strengthened. This report seeks to initiate that ambitious—but very necessary—project.

---

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-526.085%2b02%2bDOC%2bPDF%2bV0%2f%2fEN.

A. The Role of General Comments

General Comments are issued by treaty-based bodies that are established by the treaty itself. The HRC is mandated by Article 28 of the ICCPR.

In 1989, the HRC clarified that the General Comments are meant to make the experience of States "available for the benefit of all States parties in order to promote their implementation of the Covenant; to draw their attention to insufficiencies disclosed by a large number of reports . . . ."[2] In practice, the HRC, through the General Comments, has been instrumental in fleshing out the meaning and implications of the relatively bare norms codified in the text.

General Comments serve three broad functions: (1) to guide the Committee in its practice of monitoring and enforcing compliance with the treaty; (2) to provide State Parties with an authoritative interpretation and guiding framework for compliance with their treaty obligations; and (3) to provide direction for State Parties on the information the Committee expects to see in the periodic reports.[3]

Although General Comments have been described as highly persuasive authorities[4] and "of considerable practical importance for the interpretation of rights,"[5] they are not legally binding interpretations of the treaty. Nor are they considered to be amendments or subsidiary text.

In short, General Comments play a crucial role in elaborating and clarifying provisions of the ICCPR. In particular, they provide certainty and guidance for State Parties, and they add conceptual weight to the language of the ICCPR.

B. The Need to Replace General Comment 16

1. Precedent for revising or replacing General Comments

From time to time, it is the practice of the HRC to update or replace General Comments. In 2011, for example, the HRC replaced General Comment 10 (written in 1983) with General Comment 34 on Article 19, protecting the right to freedom of expression. Very recently, in January 2013, the HRC replaced General Comment 8 (written in 1982) with General Comment 35 on Article 9, protecting liberty and security of the person. And there are other examples, including the replacement of General Comment 3 (written in 1981) with General Comment 31 on Article 2, protecting the nature of State obligations.

---

[2] U.N. Human Rights Comm., *General Comments Adopted by the Human Rights Committee,* U.N. Doc. CCPR/C/C/21/Rev.1 (1989).

[4] Simone Cusack & Lisa Pusey, *CEDAW and the Right to non-discrimination and equality*, 14 MELB. J. INT'L. L. 54, 58 (2013).

[5] PHILIP ALSTON & RYAN GOODMAN, INTERNATIONAL HUMAN RIGHTS: THE SUCCESSOR TO INTERNATIONAL HUMAN RIGHTS IN CONTEXT: LAW, POLITICS AND MORALS at 691 (2013).

No explicit reasons have been given in the new General Comments for the replacement process, but grounds for revision can be easily inferred. First, in these updated General Comments the HRC has provided greater detail and authoritative guidance on the content of particular articles. It has sought to explain further the interrelationship between individual articles and the broader Covenant, and it has noted additional practical applications of articles. The point is illustrated by the fact that the original General Comment 10 on freedom of expression was one page in length; the new General Comment 34 (from 2011) is 12 pages long. In a similar vein, the original General Comment 8 on liberty and security of the person was one page long; the new General Comment 35 (2013) runs to 21 pages.

The second reason for replacement or revision is to ensure that General Comments reflect changing realities. One commentator said of the original General Comment on freedom of expression that it "did not anticipate the current reality of a globalised communications environment dominated by Internet-based technologies"—and the new General Comment explicitly attempted to address this reality.[6] Thus, replacement General Comments can ensure the ongoing relevance of the ICCPR in a rapidly changing world.

Third, new General Comments are adopted to reflect and incorporate developments in the law. As Article 19 noted in relation to the recent publication of General Comment on freedom of expression, "[t]he General Comment reflects developments in law, practice and understanding of the right, as well as technological advances (notably the internet) . . . "[7]

Fourth, on occasion the HRC has added a further General Comment on an article to express a firm view about the application of the ICCPR to a specific context. A case in point is General Comment14 on the right to life. Rather than elaborating on General Comment 6, which articulated general principles relating to the right to life, General Comment 14 focused on why the right to life in Article 6 required States to take actions towards nuclear disarmament.

2. Why General Comment 16 needs to be replaced

These reasons for revision of General Comments apply with particular force to General Comment 16 on the right to privacy. The General Comment was written during the early phase of the HRC's work, in 1988, and—while useful in its insights about the core concepts in Article 17—is just over two pages long. There is much room for elaboration

[6] Tarlach McGonagle, *Human Rights Committee: New General Comment on Freedom of Expression*, IRIS LEGAL OBSERVATIONS OF THE EUROPEAN AUDIOVISUAL OBSERVATORY (Oct., 2011), *available at* http://merlin.obs.coe.int/iris/2011/10/article1.

[7] *UN: Article 19 Welcomes General Comment on Freedom of Expression*, ARTICLE 19 (Aug. 5, 2011), http://www.article19.org/resources.php/resource/2631/en/un:-article-19-welcomes-general-comment-on-freedom-of-expression.

of the content of this right, especially given recent increased concerns over privacy protections. In light of recent revelations, which demonstrate the enormous capacities of State Parties to interfere with privacy through the conduct of sophisticated mass surveillance programs.

There is no discussion in General Comment 16 of how Article 17 relates to other rights in the ICCPR, other than a slightly vague reference to "the protection of privacy" being "necessarily relative" (at [7]). The relationship between privacy and freedom of expression (Article 19) or liberty and security (Article 9) is not analyzed. The Special Rapporteur on the protection and promotion of the right to freedom of expression and opinion, Frank La Rue, has recently and forcefully observed that insufficient protection of privacy may have a chilling effect on other rights, such as the right to freedom of expression: individuals may be chilled into silence in their online communications, for example, if they cannot be assured that their communications are private.[8] The same connection has been drawn by President Obama's Review Group on Intelligence and Communications Technologies, which said: "[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."[9] This same point was made by the European Union Advocate-General in *Digital Rights Ireland Ltd v The Minister for Communications, Marine and Natural Resources*.[10] These connections are not, however, discussed in General Comment 16.

Most importantly, General Comment 16 is rooted in a context in which the Internet was in its infancy—long before the possibility of near-instant communication through electronic mail and instant messaging, and predating the birth of the World Wide Web and its multitudes of discussion forums, blogs, social networking, and online shopping. It is thus no surprise that General Comment 16 does not explore in detail how privacy should be conceived in a world now dominated by such technologies; the world has changed significantly in this respect since 1988.[11] The General Comment does reference some modern technologies and modes of communication, but those references are made only in passing and appear quite quaint in light of the present state of global surveillance infrastructure. At [8], it 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.

---

[8] Special Rapporteur 2013 Report, supra note 1, at 4, 7.
[9] Richard A. Clarke et al, *Liberty and Security in a Changing World* at 47, President's Review Group on Intelligence and Communications Technologies at 47 (Dec. 12, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[10] Digital Rights Ireland Ltd v The Minister for Communications, Marine and Natural Resources [2013] C-203/12, C-594/12, (H. Ct.) (Ir.) *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=683832.
[11] See, e.g., http://m.wimp.com/theinternet/ (a news-clip from 1981 describing a new technology – the Internet - that may in the future allow for the prospect of reading newspapers on your computer screen)

Paragraph [10] also references the collection, storage, and use of personal data on electronic data-bases:

> The gathering and holding of personal information on computers, data banks 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.

However, there is no reference to the Internet or even newer communication technologies and no examination of their impact on privacy interests protected by the treaty. There is no explicit anticipation of the evolution from fixed-line telephone systems to mobile telecommunications on a large scale; the development of metadata (data about data); the relationships between Internet companies, service providers, and governments, entrenched through mandatory data-retention laws; the ability on the part of States to track Internet activities on a large scale, through social media monitoring or analysis of IP addresses;[12] or the rise of biometric data-gathering (through, for example, finger-printing, facial recognition software, or other, even more sophisticated tools) and DNA databases in many jurisdictions.

The advent of these new information technologies and the resultant increased capacities of State Parties and corporations to interfere with privacy protections require a re-examination of the nature and scope of General Comment 16. Take just one example of a privacy concern generated by modern information technology: metadata. Metadata consists of information other than the content of one's communications, and includes such categories of data as the phone numbers one has dialed, the time, date and duration of the calls one makes, location information for cellular phones (as recorded by cell phone towers), and the IP addresses or URLs one visits while browsing the Internet. The U.S. government and other State Parties afford little protection to this sort of information.[13] Yet, as the U.N. Special Rapporteur on freedom of expression has observed—and as the world's leading computer scientists have documented—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."[14] This kind of

---

[12] Special Rapporteur 2013 Report, supra note 1, at 3–20.

[13] *ACLU v. Clapper*, --- F. Supp. 2d ----, No. 13-cv-3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013).

[14] 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 1; 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*, Metadata: Piecing Together a Privacy Solution, American

information can often be gathered at little cost, shared more easily than ever before, and processed rapidly through "algorithmic surveillance," to create categorical identities for individuals.[15] JUSTICE's report on surveillance reform highlights another relevant issue: that new forms of electronic surveillance now make it impossible for a human being even to know that their privacy is being infringed, or to know what information is being held about them—facts that require revision of the protecting legal framework.[16]

In a similar vein, Manfred Nowak has pointed out that privacy has always "manifested itself in particular *institutional structures*."[17] General Comment 16 is clearly wedded to traditional institutional structures such as the family and the home, and the right to privacy must be developed to take into account new institutional structures such as the Internet. It must also be developed to more fully accommodate a new dimension of privacy—informational privacy—which has assumed incalculably greater significance in the digital age.

The technological developments are altering the borders of the private and public spheres,[18] and it is precisely as these disruptive changes are occurring that international human rights law ought to stake out the contours of privacy in a modern world. General Comment 16 says baldly that surveillance of all kinds are prohibited—yet the HRC has gone on to authorize surveillance in some conditions, as long as certain safeguards exist.[19] This uncertainty in position is a further reason for the Committee to endeavor upon a replacement General Comment.

That there is a need for an update of international human rights law in light of new times is confirmed by, amongst other things, the Third Committee of the General Assembly's 2013 approval (without a vote) of a resolution on the right to privacy in the digital age, which called on States to review various legislation on surveillance in order to protect privacy interests. This need is reinforced by the development of civil society-produced International Principles on the Application of Human Rights to Communications Surveillance, released in July 2013.

Updating and replacing General Comment 16 will strengthen the credibility of the Committee and further solidify the ICCPR as the primary international human rights treaty protecting the right to privacy.

Civil Liberties Union of Northern California *available at* https://www.aclunc.org/publications/metadata-piecing-together-privacy-solution.

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

[16] Eric Metcalfe, *Freedom from Suspicion: Surveillance Reform for a Digital Age* at 7, JUSTICE (2011), *available at* http://www.justice.org.uk/data/files/resources/305/JUSTICE-Freedom-from-Suspicion-Surveillance-Reform-for-a-Digital-Age.pdf.

[17] MANFRED NOWAK, U.N. COVENANT ON CIVIL AND POLITICAL RIGHTS: CCPR COMMENTARY at 378 (2nd ed., 2005).

[18] *Id.* at 10.

[19] See, e.g., U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Sweden, U.N. Doc. CCPR/C/SWE/CO/6 (2009) [hereinafter U.N. HUMAN RIGHTS COMM., Concluding Observations on Sweden].

Additionally, the strength of international human rights law on privacy erodes when its protections only derive meaning from a world without modern electronic communications and technology. Updating the General Comment on the right to privacy to take such modern developments into account would redress this problem, allowing individuals to reclaim the degree of control over their identities envisioned by the treaty.[20] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression has said: "[i]nadequate national legal frameworks create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications."[21] The same is true of inadequate international legal frameworks.

Overall, then, replacing General Comment 16 is necessary:

1. to clarify the contours of the protections now afforded by the right to privacy;
2. to reflect changing realities; and
3. to ensure continued protection of privacy and other related rights in the world today.

Having established the need for a new General Comment on privacy, this report will now discuss and analyze the principles that should underpin it. 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.

C. Principles for a Modern Right to Privacy under the ICCPR

1. Reaffirming Article 17's broad scope of privacy protection

A new General Comment should reaffirm that Article 17's protections apply broadly, identifying the protections for bodily privacy, home, communications, and information privacy that the HRC and regional human rights bodies have recognized in jurisprudence and commentary on emerging State practice.

Article 17, which is based on Article 12 of the Universal Declaration on Human Rights,[22] provides that:

1. no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation; and

[20] See Goold, supra note 15, at 52.
[21] Special Rapporteur 2013 Report, supra note 1, at 3.
[22] Article 12 provides that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." U.N.GAOR, *Universal Declaration of Human Rights*, U.N. Doc. A/810, 71 (1948).

2. everyone has the right to the protection of the law against such interference or attacks.

Although the record of the drafting of Article 17 provides little guidance as to precisely what was intended to be included within the concept of "privacy," the HRC and other experts have recognized that it encompasses rights beyond those listed. For example, in *Coeriel and Aurik v. The Netherlands*, the Committee observed that the right to privacy protects the right to freely express one's identity.[23] And in *Toonen v. Australia*, the Committee confirmed that the Article 17 privacy right includes the right to engage in consensual sexual activity in private.[24] A right to intimacy as a component of the right to privacy can also be discerned from paragraph [8] of General Comment 16.[25] Finally, in *Leo Hertzberg et al. v. Finland*, three members of the Committee observed that Article 17 protects "the right to be different and live accordingly."[26]

As the Secretary-General of the United Nations has emphasized:

> [T]he very existence of an internationally recognized right to privacy presupposes agreement that there are certain areas of the individual's life that are outside the concern of either governmental authorities or the general public, areas which may vary in size from country to country, but which do possess a common central core.[27]

The Committee's practice finds support in the jurisprudence of the European Court of Human Rights, which has also found that "private life" guaranteed by Article 8 of the European Convention incorporates numerous facets, including rights to bodily privacy and identity. In *Botta v. Italy,* the Court found that "private life"

> includes *a person's physical and psychological integrity*: the guarantee afforded by Article 8 of the Convention is primarily intended to ensure the

[23] Coeriel et al. v. The Netherlands, U.N. HUMAN RIGHTS COMM., Communication No. 453/1991at ¶ 10.2, U.N. Doc. CCPR/C/52/D/453/1991 (1994); see also, 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).

[24] Toonen v. Australia U.N. HUMAN RIGHTS COMM., Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (1994); See also, Dergachev v. Belarus, U.N. HUMAN RIGHTS COMM., Communication No. 721/1996, U.N. Doc. CCPR/C/74/D/721/1996 (2002) at ¶¶ 2.7, 2.8, 6.7. (describing invasive strip search of prisoner and the requirement that he apply for permission before writing to anyone as "attacks on [the author's] privacy and dignity", and finding resultant violation of Article 17).

[25] U.N. GAOR, 43rd Sess., Suppl. No. 40, ¶ 8, U.N. Doc. A/43/40 (1988) [hereinafter General Comment 16].

[26] 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).

[27] U.N. Doc E/CN.4/1116 (1976); see also, Nowak supra note 19; 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).

> development, without outside interference, of the personality of each individual in his relations with other human beings.[28]

And, in *Peck v. the United Kingdom*, the Court identified a "right to identity and personal development, and the right to establish and develop relationships with human beings and the outside world."[29] Significantly, in a world where an increasing number of our personal and business transactions take place on-line, the Court added that "[t]here is . . . . a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life."[30] In short, the European Court has concluded that the concept of "private life" is "not susceptible to exhaustive definition."[31]

The Inter-American Court of Human Rights, too, has identified a broad range of rights inherent in "private life" guaranteed by Article 11 of the American Convention, including rights to bodily autonomy, identity, and personal and social development:

> 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. The concept of private life encompasses aspects of physical and social identity, including the right to personal autonomy, personal development and the right to establish and develop relationships with other human beings and with the outside world. The effective exercise of the right to private life is decisive for the possibility of exercising personal autonomy on the future course of relevant events for a person's quality of life. Private life includes the way in which individual views himself and how he decides to project this view towards others, and is an essential condition for the free development of the personality . . . .[32]

2. Recognizing Information Privacy

The right to privacy has evolved to include specific rights to access and control of one's personal data.[33] General Comment 16 explicitly contemplates this concept of information privacy:

---

[28] Botta v Italy, App. No. 21439/93, Reports of Judgments and Decisions, Eur. Ct. H.R., ¶ 32 (Feb. 24, 1998).
[29] See also, Shimovolos v Russia, App. No. 3019409/09, Judgment, Eur. Ct. H.R., ¶¶ 64–66 (June 21, 2011).VI (noting that privacy includes "the right to establish and develop relationships with other human beings and the outside world")
[30] Peck v. the United Kingdom, App. No. 44647/98, Eur. Ct. H.R., ¶ 57 (2003).
[31] Bensaid v. the United Kingdom, App No. 44599/98, Eur. Ct. H.R., ¶ 47, (2001).
[32] Murillo v. Costa Rica, Inter-Am. Ct. H.R., Judgment, ¶ 143 (Nov. 28, 2012); see also Rosendo Cantu v. Mexico, Inter-Am. Ct. H.R., Judgment (Aug. 31, 2010); Atala Riffo v. Chile, Inter-Am. Ct. H.R., Judgment, (Feb. 24, 2012).
[33] Nowak, supra note 19, at 388.

> 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 contrary to the provisions of the law, every individual should have the right to request rectification or elimination.[34]

The European Court has repeatedly found that "protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life."[35] 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."[36] 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.[37]

Recognition of a right to information privacy is especially important in an era when sophisticated modern technologies now allow cost-effective mass collection, storage, use and transmission of data electronically, and when personal lives and business transactions are increasingly conducted online. As the European Court observed in *Malone v. the United Kingdom*:

> the 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.

---

[34] General Comment 16, supra note 28, at ¶ 10.
[35] 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).
[36] See supra note 28, Marper at ¶¶ 66-67.
[37] Rotaru v. Romania [GC], App No. 28341/95, Eur. Ct. H.R., ¶ 43, (2000).

"[T]he sphere of a person's life in which he or she can freely express his or her identity" now includes online spaces, and identity now includes a person's digital identity. "Digital identity" is an emergent legal concept in the United States and Australia, and refers to "an individual's identity which is composed of information stored and transmitted in digital form."[38] Protection of the right to digital identity has become increasingly important given the move to online transactions and the rise of social media.[39] As the Australian government has recently noted:

> In an era where our online identity is central to accessing information and services, ensuring the integrity of that identity is increasingly important. The loss of compromise of our online identity can have wide-ranging implications . . . . [T]here would be value in revisiting the distribution of responsibility among individuals, businesses and governments . . . .[40]

3. Updating the concepts of family, home and correspondence

Article 17's protections for privacy of "family," "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.

a. "Family" and "Home" Include Online Private Spaces

An individual's home may now encompass virtual spaces, such as social media websites and email inboxes. A new General Comment should recognize that these online private spaces, as well as personal computers and handheld electronic devices used to access them, are protected under the privacy concepts of "family" and "home."

General Comment 16 provides that the terms "family" and "home" be given a broad interpretation. "Family" includes all those comprising a family, as understood in the society of the State Party concerned, and the HRC has determined that Article 17 protects "the privacy of individual family members, *as expressed in family life*, against unlawful or arbitrary interference".[41] The meaning of "home" includes "the place where a person resides *or carries out his usual occupation*." In *Halford v. the United Kingdom*, the European Court took the same broad view on the parameters of "home" under the European Convention, holding that Article 8's privacy protections applied equally to phone calls made from the applicant's office and home telephones.[42] More recently, in *Bernh Larsen Holding AS and Ors. v. Norway*, the European Court found that "all data

---

[38] Claire Sullivan, *Digital identity and* mistake, MELB. J. INT'L. L. 223, 225 (2011).
[39] *Id,* at 226.
[40] AUSTRALIAN GOVERNMENT, *Connecting with Confidence: Optimising Australia's Digital Future*, A Public Discussion Paper (2011), cited in Sullivan, *id*, at 228-229.
[41]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); Nowak, supra note 17, at 393 (emphasis added).
[42] Halford v. the United Kingdom, App. No. 20605/92, Judgment, Eur. Ct. H .R., ¶¶ 44, 46 (1997).

stored on a server" used by three corporations constitute a space that should be afforded the same protections as a "home."[43]

While extending broad protections to personal spaces other than one's residence, the HRC requires that any interference with those spaces (including a "search"), be narrowly tailored to minimize the intrusion on privacy.[44]

The Inter-American Court also defines the protection 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.[45]

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,"[46] "home" for the purposes of Article 17 should be interpreted to include privacy protections for personal online spaces, as well as personal computers and handheld electronic devices used to access them. [47]

b. "Correspondence" Includes All Forms of Communication

General Comment 16 provides that:

> [c]ompliance with Article 17 requires that the integrity and confidentiality of correspondence should be guaranteed de jure and de facto. Correspondence should be delivered to the addressee without interception and without being opened or otherwise read.[48]

Although specifically directed at maintaining the confidentiality of postal communications, "correspondence" also includes all electronic forms of communication, such as electronic mail and instant messages, as well as "telephonic and telegraphic" forms of communication,[49] as earlier statements of the Committee[50] and decisions of the

---

[43] Bernh Larsen Holding AS and Ors. v. Norway, App. No. 24117/08, Judgment, Eur. Ct. H .R., ¶ 106 (2013)

[44] Garcia v. Colombia, U.N. HUMAN RIGHTS COMM., Communication No. 687/1996, U.N. Doc. CCPR/C/71/D/687/1996 (2001).

[45] Ituango Massacres v. Colombia, Preliminary Objections, Merits, Reparations and Costs, Judgment, Inter-Am. Ct. H.R. (ser. C) No. 148, ¶¶ 193-194 (2006).

[46] Shimovolos supra note 32.

[47] See generally, U.N. GOAR, 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")

[48] General Comment No. 16, supra note 28, at ¶ 8.

[49] *Id.*

European Court interpreting "correspondence" under Article 8 of the European Convention reflect.[51]

A new General Comment should also confirm that metadata—data providing information about one or more aspects of the correspondence—is owed the same privacy protections as the content of the communication itself. Metadata, especially when it is collected, aggregated, and analyzed for information across time, can "identify or infer new and previously private facts" about an individual, such as behavioral patterns and associational relationships.[52] Indeed, in some instances, metadata can reveal information "that is even more sensitive than the contents of the communication."[53] Thus any interference with metadata through surveillance can have the same impact on privacy interests as interference with the content of communications. It should therefore be subject to the same limitations. The European Court has long eschewed such artificial distinctions, focusing instead on the substance of the privacy intrusion affected by a particular manner of surveillance. 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.[54] The Court also determined that *information derived from* the monitoring of personal internet usage—metadata—also falls within the scope of "correspondence" under Article 8.[55] The Court held that

> collection 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.[56]

---

[50] U.N. HUMAN RIGHTS COMM., *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant*, Concluding Observations, Bulgaria, U.N. Doc. CCPR/C/BGR/CO/3 at ¶ 22 (Aug. 19, 2011) (equating telephone calls to "correspondence" under Article 17).

[51] 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).

[52] 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*, Metadata: Piecing Together a Privacy Solution, American Civil Liberties Union of Northern California *available at* https://www.aclunc.org/publications/metadata-piecing-together-privacy-solution.

[53] *Id.*

[54] Copeland v. The United Kingdom, App. No. 62617/00, Judgment, Eur. Ct. H.R. (2007).

[55] *Id.*

[56] 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).

D. Limitations on the right to privacy

Of course, the right to privacy is not absolute. The European Convention on Human Rights and the Inter-American Convention on Human Rights contain express limitation clauses, but there is no such clause in Article 17. The *travaux preparatoires* for the ICCPR suggest that States sought the flexibility to determine what limitations could be imposed on privacy rights. The HRC has interpreted the text of Article 17 as incorporating robust privacy protections that do not allow for any restrictions other than those listed—non-arbitrary and lawful interferences.[57] "Lawfulness" should be interpreted to mean "prescribed by law, clearly defined, and subject to judicial review." The non-arbitrariness requirement mandates that any measure also meet a four-part proportionality test.

1. "Interference"

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

A new General Comment should expressly state that laws—especially if they are vague and unclear—may interfere with privacy interests where they produce a chilling effect on protected activity. In *Toonen v. Australia*, the Committee considered whether provisions of the Tasmanian Criminal Code criminalized various forms of sexual contact between men, including sexual contact between consenting adult homosexual men in private, violated Article 17.[58] Although the provisions had not been enforced for several years, and the state had a policy of not initiating criminal proceedings based on private homosexual conduct, the Committee concluded that the continued existence of the challenged provisions continuously and directly "interfere[d]" with the author's privacy.[59]

In *Weber v Germany*, the European Court applied this same principle in assessing whether a German law authorizing surveillance constituted "interference" as defined by Article 8 of the Convention:[60]

> [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 . . . .

---

[57] Nowak, supra note 17, at 381.
[58] Toonen v. Australia, supra note 27, at ¶¶ 8.3, 2.1.
[59] *Id.* at ¶ 8.2.
[60] Weber and Saravia v. Germany, App. No. 54934/00, Decision as to Admissibility, Eur. Ct. H.R., ¶ 78 (2006).

A new General Comment should also reaffirm that collection and storage of personal information interferes with privacy interests even absent subsequent use or transmission of that data. General Comment 16 [10] recognizes this, 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." The European Court has repeatedly reaffirmed 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."[61] 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 § 2," adding that "subsequent use of the recordings made has no bearing on that finding."[62] In *Shimovolos v Russia*, a case involving the registration of a person on a surveillance database and the tracking of his travel movements, the Court held that "systematic storage and collection of data by security services" are interferences with the right to privacy. The Court also found that collection of data can also amount to an interference with privacy, even if that data is obtained from a public place or relates to professional or public activities.[63]

A new General Comment should clarify that the collection and storage of personal data, even if it is available in the public domain, amounts, *prima facie,* to an "interference" with the right to privacy under Article 17, even absent its subsequent use or transmission.

2. "Unlawful"

The wording of Article 17(1) establishes two different levels of protection. Privacy, family, home and correspondence are protected from "arbitrary or unlawful interference," whereas honor and reputation are protected only from "unlawful attacks." Thus, the protection afforded to privacy is arguably more comprehensive than that afforded to reputation—it may be neither arbitrary nor unlawful.[64]

Lawfulness Test

- Consistent with the provisions, aims, and objectives of the Covenant
- Pursuant to domestic and international law
- Accessible and foreseeable
- Precise, specific and clearly defined

[61] Leander v Sweden, App No. 9248/81, Judgment, Eur. Ct. H.R., ¶ 48 (1987).
[62] 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).
[63] Shimovolos, supra note 32; *Rotaru v Romania*,supra note 40.
[64] Nowak, *supra* note 17, at 381.

General Comment 16 makes clear at [3] that the prohibition on unlawful interference means that interference can only occur "on the basis of law." However, that law must also be consistent with "the provisions, aims and objectives of the Covenant."

In addition to consistency with the purpose of the Covenant, three further conditions must be met for lawfulness to be satisfied, as illustrated by General Comment 16, the practice of the HRC, and case law of the European and Inter-American Courts. First, the interference must be pursuant to, and in accordance with, enacted domestic law.[65] Second, the domestic statutory framework must be accessible and must ensure that any interference is reasonably foreseeable to the person concerned.[66] Third, domestic law must be "precise" and "clearly" defined.[67] These conditions find support in paragraph [3] of General Comment 16 , which states that "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."[68]

The requirements of lawfulness accordingly mirror 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."[69] Although the ICCPR and European Convention are worded differently, the European Court's "quality of law" test is instructive.

a. Pursuant to domestic and international law

The first requirement is supported by paragraph [3] of General Comment 16, which clarifies that the term 'unlawful' "means that no interference can take place except in cases *envisaged by the law*" (emphasis added).[70] It provides a measure of legal protection against the possibility of interference through executive acts and discretion. The term

[65] 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.
[66] S.W. v. the United Kingdom, App. No. 20166/92, Judgment, Eur. Ct. H.R. ¶¶ 44-48, Series A no. 335-B (1995); K.-H.W. v. Germany [GC], App. No. 37201/97, Judgment, Eur. Ct. H.R. ¶¶ 72-76 (2001) (extracts).
[67] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Jamaica, U.N. Doc. CCPR/C/79/Add.83 at ¶ 20 (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, U.N. Doc. CCPR/C/79/Add.54 at ¶ 19 (July 26, 1995) [hereinafter U.N. Human Rights Comm., Concluding Observations on Russia]; General Comment No. 16, supra note 28, ¶¶ 3, 8.
[68] General Comment 16, supra note 28, ¶ 3.
[69] Kafkaris v. Cyprus [GC], App. No. 21906/04, Judgment, Eur. Ct. H.R.(2008).
[70] General Comment 16, supra note 28, ¶ 3.

"unlawful" should also be interpreted in light of international rules and international law.[71]

b. Accessible and foreseeable

Publicly accessible laws and regulations help a person ascertain the applicable legal regime in advance. Foreseeing the consequences of a given action allows them to regulate their conduct in accordance with the law—a necessary protection against unlawful interference. [72] Thus, if the creation, maintenance, and operation of a surveillance database are governed by a administrative order, which is not accessible to the public, it does not satisfy the lawfulness test.[73]

c. Specificity and precision

The third additional requirement of specificity and precision is a safeguard against abuse of power. It derives support from HRC comments on wire-tapping[74] and from paragraph [8] of General Comment 16, which 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."[75] The HRC 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."[76]

Likewise, the Inter-American Court emphasized the highly specific, targeted nature of a Brazilian surveillance law it upheld in *Escher*. In determining permissible limitations to the Inter-American Convention's Article 11, the Court noted that any limitation must be pursuant to, and in accordance with, an enacted law. Thus, a large part of the Court's inquiry turned upon whether the surveillance action accorded with domestic Brazilian law. The Court ultimately found that it was not, deciding the case on that ground. What is particularly instructive, however, is that the Court *also* found that Brazilian domestic law was in conformity with the principles of the American Convention 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.[77] Furthermore, "in any of these circumstances, reasonable indications of the authorship or participation in a

[71] 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).
[72] Kafkaris v. Cyprus [GC]. supra note 73, ¶¶ 150-152; 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).
[73] Shimovolos, supra note 32.
[74] U.N. HUMAN RIGHTS COMM., Concluding Observations on Russia, ¶ 19; U.N. HUMAN RIGHTS COMM., Concluding Observations on Jamaica, ¶ 20.
[75] General Comment No. 16, supra note 62, ¶ 8.
[76]Van Hulst v. The Netherlands, HUMAN RIGHTS COMM., Communication No. 903/1999, ¶ 7, U.N. Doc. CCPR/C/82/D/903/1999 (2004).
[77]Escher, supra note 68, ¶ 132.

criminal offense of the individual subjected to the measure must be provided, and also that the evidence cannot be obtained by other means."[78]

Thus, surveillance cannot be sustained 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 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. Bulk mass surveillance with no grounds for such suspicion would, logically and obviously, fail such a test.

In addition, lawfulness requires that there be no more-narrow, less-intrusive way of reasonably achieving the same results available to the government—and that the burden of proving as much lies upon the government. This reinforces the notion that a specific legal foundation is required for any interference with privacy interests under Article 17.

3. "Non-Arbitrary"

For an interference with privacy to be "non-arbitrary," it must pursue a legitimate aim, have a rational connection to that aim, minimally impair the right to privacy, and strike a fair balance between pursuit of the aim and limitation of the right. In other words, it must satisfy a proportionality test. This is widely reflected in the HRC's jurisprudence, the position of UN experts, and the jurisprudence of regional human rights bodies.

a. "Arbitrary" Requires a Proportionality Assessment

In its practice, the HRC has interpreted "non-arbitrary" under Article 17 to include a notion of reasonableness, although the *travaux prepartories* reflect disagreement among delegates about this.[79] In General Comment 16, the Committee states that:

> the 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* (emphasis added).[80]

The Committee has emphasized that non-arbitrariness requires that an interference is "reasonable in the particular circumstances," suggesting in *Rojas Garcia v. Colombia* that even if an interference is within the scope a domestic law, the State needs a clear justification for it.[81] Similarly, in *Canepa v. Canada*, the Committee found that

---

[78] *Id.*

[79] General Comment No. 16, supra note 28, at ¶ 4.

[80] *Id.*

[81] At 2:00am, a group of armed and hooded men from the Public Prosecutor's Office forcibly entered the author's house through the roof. The Colombian Government argued that the entry into the author's house fulfilled all of the legal requirements of the Code of Criminal Procedure, and was therefore within

"arbitrariness within the meaning of Article 17 is not confined to procedural arbitrariness, but extends to the reasonableness of the interference with the person's rights under Article 17 and its compatibility with the purposes, aims and objectives of the Covenant."[82]

In *Toonen v. Australia*, the Committee discussed the issue of reasonableness further, and noted that reasonableness requires proportionality:

> The Committee interprets the requirement of reasonableness to imply that any interference with privacy *must be proportional to the end sought and be necessary in the circumstances of any given case* (emphasis added).[83]

The Committee also equated reasonableness and proportionality in *Van Hulst v. Netherlands*. There, the Committee noted in passing that both parties argued for proportionality based on the traditional four-part test, which requires a legitimate aim to be pursued, there to be a rational connection between the measure and the aim, there to be minimal impairment of the right to privacy, and there to be a fair balance struck between the aim and the right.[84]

The former Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, and the current Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, have both emphasized that this four-part test is the most structured way of approaching the inquiry into whether a limitation on the right to privacy is arbitrary.[85] The *Tristan Donoso* case also supports the use of a proportionality test. Consistent with the jurisprudence of the European Court, the 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."[86]

Thus, a limitation on the right to privacy will only be considered non-arbitrary when all four parts of the proportionality test are met.

b. Provide Guidance on Application of Arbitrariness and Lawfulness Standards to Surveillance and other Measures for the Collection and Storage of Personal Data

---

the scope of the law. The Committee found that this conduct constituted arbitrary interference, as the State party had failed to justify the violent conduct. U.N. HUMAN RIGHTS COMM., Communication No. 687/1996, U.N. Doc. CCPR/C/71/D/687/1996 (2001).

[82] Canepa v. Canada, U.N. HUMAN RIGHTS COMM., Communication No. 558/1993, U.N. Doc. CCPR/C/59/D/558/1993, ¶ 11.4 (1997).

[83] Toonen v. Australia, supra note 27, at ¶ 8.3.

[84] Van Hulst, supra note 79.

[85] See, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* OHCHR, A/HRC/13/37 at ¶ ¶ 14-19 (Dec. 28, 2009); Special Rapporteur 2013 Report, supra note 1, at ¶ ¶ 28-29. See also, Nowak, supra note 17, at 383.

[86] Donoso, supra note 68, at ¶ 56.

Given the recent widespread concern over State powers of surveillance and uncertainties over the scope of these powers, and other measures for the collection and storage of personal data, a new General Comment should provide explicit guidance on the application of arbitrariness and lawfulness standards to such laws, policies, and practices.

The key lessons arising from modern jurisprudence on arbitrariness, and that should serve as a framework for a new General Comment, are:

- for an interference with privacy to be non-arbitrary, it must pursue a legitimate aim, have a rational connection to that aim, minimally impair the right to privacy, and strike a fair balance between pursuit of the aim and limitation of the right—in other words, it must satisfy a proportionality test;
- surveillance and data collection practices must ensure minimum safeguards to prevent abuse and arbitrary interferences with privacy interests;
- indiscriminate mass surveillance is a disproportionate interference with the right to privacy and violates Article 17;
- mass collection and retention of personal data is a disproportionate interference with the right to privacy and violates Article 17; and
- surveillance and other measures for the collection and storage of personal data must be subject to judicial oversight and victims of privacy violations should be provided effective access to a remedy.

c. Human Rights Committee's Views on State Surveillance Practices

Providing the foregoing guidance in a General Comment would reflect the HRC's observations on emerging state practice.[87]

In Concluding Observations on the Russian Federation, the Committee expressed concern that intrusion into telephone communication was possible "without clear legislation setting out the conditions of legitimate interferences with privacy and providing for safeguards against unlawful interferences."[88] Concluding Observations on Jamaica also reference the need to "adopt precise legislation" in relation to wire-tapping.[89] These statements from 1995 and 1997 suggest that heightened clarity, specificity, and precision are required in relation to surveillance legislation—and they also point to the necessity for safeguards.

[87] *See generally,* JOSEPH, SCHULTZ & CASTAN, THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS: CASES, MATERIALS, AND COMMENTARY at 536, 548 (2d ed. 2005)..
[88] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Russia ¶ 19 (2004) [hereinafter U.N. Human Rights Comm., Concluding Observations on Russia].
[89] U.N. HUMAN RIGHTS COMM., Concluding Observations on Jamaica, supra note 71, at ¶ 20.

Statements on surveillance practices in Poland, Sweden, and the Netherlands between 1990 and 2009 indicate that the Committee may be developing a more stringent posture towards surveillance and other measures involving the collection, storage, and use of personal data as we have entered the new millennium.

In Concluding Observations on Poland, the Committee stated at [22] that it was "concerned (a) that the Prosecutor (without judicial consent) may permit telephone tapping, and (b) that there is no independent monitoring of the use of the entire system of tapping telephones."[90] It is clear from this language that some kind of independent monitoring is needed to satisfy Article 17, but the Committee may have been expressing the view that telephone tapping without prior judicial consent is never permitted under the treaty.

In 2009, in its Concluding Observations on the Netherlands, the Committee stated at [14] that "[t]he Committee is aware that [the Netherlands] considers wire and telephone tapping to be an important investigative tool," but that "[the Committee] is concerned that any use of wire and telephone taps should be minimized so that only pertinent evidence is gathered and that a judge should supervise its use."[91] At the very least, therefore, surveillance should be confined to "pertinent evidence" and should be subject to judicial supervision. It is also clear from this comment that surveillance must only minimally impair the right to privacy (the third part of the proportionality test) for it to be considered non-arbitrary.

More broadly, in its Concluding Observations on Sweden in 2009, the Committee stated at [18] that whenever there was State information-gathering of personal data, in addition to the need for "review and supervision by an independent body," "all appropriate measures [should be taken] to ensure that the gathering, storage and use of personal data not be subject to any abuses, not be used for purposes contrary to the Covenant, and be consistent with obligations under article 17 of the Covenant."[92] These are important qualifications on how personal data ought to be used, regardless of the means by which it was acquired: it must not be subject to abuse, must not be used for purposes contrary to the Covenant, and must be used consistently with Article 17 obligations.

d. Confront and Reject Mass Surveillance Operations

Thus "blanket and indiscriminate" surveillance operations—given their scope for abuse—ought to be entirely prohibited, if States are to comply with Article 17. And targeted surveillance operations are only lawful if they are proportionate. That conclusion is supported by the views of the Committee and European Court case law. In *Van Hulst*

[90] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Poland, U.N. Doc. CCPR/C/79/Add.110 (1999) [hereinafter U.N. HUMAN RIGHTS COMM., Concluding Observations on Poland].
[91] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, The Netherlands, U.N. Doc. CCPR/C/NLD/CO/4 (2009) [hereinafter U.N. Human Rights Comm., Concluding Observations on the Netherlands].
[92] U.N. HUMAN RIGHTS COMM., Concluding Observations on Sweden, supra note 21.

v. Netherlands, the Committee observed—in the context of phone-tapping—that "the decision to allow such interference can only be taken by the authority designated by law, on a case-by-case basis."[93]

The European Court has adopted a similar approach. In *Liberty v United Kingdom*, a case concerning a British law authorizing surveillance of telephone communications, the Court noted that relevant legislation provided an "extremely broad discretion," with "no limit to the type of external communications" caught by surveillance or caught by what the State could listen to or read.[94] Consequently, the court held that the law did not provide "adequate protection against abuse of power."[95] Subsequently, in *Kennedy v United Kingdom*, the Court held that the surveillance regime then in place was compliant with Article 8, but only because it specified in some detail those categories of individuals targeted and the process surrounding their surveillance. In other words, the law provided with "sufficient clarity the procedures for the authorisation and processing of interception warrants as well as the processing, communicating and destruction of intercept material collected."[96]

A new General Comment should also provide that these same requirements apply equally to measures (other than surveillance) resulting in the "blanket and indiscriminate" collection and storage of personal data—however obtained and regardless of any subsequent use. Article 17 prohibits such measures because they amount to a disproportionate interference with the right to privacy. This position is supported by General Comment 16,[97] the practice of the Committee,[98] the European Court,[99] and most recently, an opinion of the European Union Advocate-General. [100]

e. Reaffirm the Requirement of Effective Judicial and Administrative Oversight of Surveillance and Related Measures

The HRC has repeatedly and forcefully highlighted that surveillance and other measures that interfere with privacy interests should be subject to effective judicial and administrative oversight. This view is supported by General Comment 16 and the jurisprudence of other international bodies, including the European Court. Thus, in *Al-Gertani v 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."[101]

---

[93] Van Hulst, supra note 79, at ¶ 7.7.
[94] Liberty v. United Kingdom, App. No. 58243/00, Judgment, Eur. Ct. H.R., ¶¶ 64–65 (2008).
[95] *Id.*, ¶ 69.
[96] Kennedy v United Kingdom, App. No. 26839/05, Judgment, Eur. Ct. H.R., ¶ 169 (2010).
[97] General Comment No. 16 at ¶ 10.
[98] See e.g., U.N. HUMAN RIGHTS COMM., Concluding Observations on Sweden, supra note 21, at ¶ 18.
[99] See e.g., S. and Marper, supra note 38 (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 …")
[100] *Digital Rights Ireland Ltd*, supra note 10, at ¶ 72.
[101] Al-Gertani v. Bosnia & Herzegovina, U.N. HUMAN RIGHTS COMM., Communication No. 1955/2010 (2010) U.N. Doc. CCPR/C/109/D/1955/2010 at ¶ 5.7.

Likewise, in *Van Hulst*, 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."[102] Similarly, in *S and Marper v. the United Kingdom*, the European Court emphasized that surveillance and other data collection regimes required

> minimum safeguards concerning, *inter alia*, duration, storage, useage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction [to] guarantee[] against the risk and abuse and arbitrariness.[103]

Given the importance of judicial and administrative oversight as a guarantee against potential abuse and arbitrariness in the collection, storage, or use of personal data, a new General Comment should spell out what "minimum safeguards" Article 17 incorporates. In particular, the Committee should address the prerequisites of the tribunal responsible for oversight, and the requirements of a fair and public hearing by a competent, independent and impartial tribunal established by law" established in General Comment 32, concerning Article 14 of the ICCPR.[104] The new General Comment should also highlight the obligation on such a tribunal to ensure effective remedies to victims when arbitrary or unlawful interferences with privacy occur, a principle recently recognized by the Committee in *Bulgakov v Ukraine*.[105]

f. Extraterritorial application of the right to privacy

- Article 17 (together with other Convention rights) applies extra-territorially, so that States must respect the right to privacy whenever individuals are within their "jurisdiction" as well as their "territory";
- the term "jurisdiction" must be applied broadly and in light of modern developments to mean within the virtual power or virtual control of a State; and
- states must respect the right to privacy consistently with the principle of non-discrimination, giving equal protection to the rights of nationals and non-nationals alike.

Given the now-global and -interconnected nature of communications and information technology, a new General Comment should clarify that Article 17 obligations have extraterritorial reach. The HRC has repeatedly acknowledged the extraterritorial

[102] Van Hulst, supra note 79, at ¶ 7.7; see also U.N. HUMAN RIGHTS COMM., Concluding Observations on Sweden, supra note 21, n. at ¶ 18 (requiring "review and supervision by an independent body" to prevent abuses in the gathering, storage and use of personal data).
[103] S and Marper, supra note 38.
[104] U.N. HUMAN RIGHTS COMM., General Comment No. 32, *Article 14: Right to equality before courts and tribunals and to a fair trial*, U.N. Doc. CCPR/C/GC/32 (2007).
[105] Bulgakov v Ukraine, U.N. HUMAN RIGHTS COMM., Communication No. 1803/2008, ¶9 U.N. Doc. CCPR/C/106/D/1803/2008 (1985); See also, General Comment 31.

application of the ICCPR.

Article 2(1) of the ICCPR provides that "[e]ach State Party . . . undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant." Interpreting the scope of these protections in General Comment 31, the Committee has said that:

> a State party must respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, *even if not situated within the territory of the State Party*. As indicated in General Comment 15 adopted at the twenty-seventh session (1986), the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons, who may find themselves *in the territory or subject to the jurisdiction of the State Party*. This principle also applies to those within the power or effective control of the forces of a State Party acting outside its territory, regardless of the circumstances in which such power or effective control was obtained, such as forces constituting a national contingent of a State Party assigned to an international peace- keeping or peace-enforcement operation.

The Committee has also made its position clear in decisions in individual communications, and concluding observations on States Parties' reports. In *Lopez Burgos v. Uruguay,* a 1981 decision concerning a Uruguayan man subject to torture and cruel treatment by Uruguayan authorities while he was in Argentina, the Committee said that Article 2(1):[106]

> does not imply that the State party concerned cannot be held accountable for violations of rights under the Covenant which its agents commit upon the territory of another State, whether with the acquiescence of the Government of that State or in opposition to it.

Citing Article 5(1), the Committee added that:[107]

> it would be unconscionable to so interpret the responsibility under article 2 of the Covenant as to permit a State party to perpetrate violations of the Covenant on the territory of another State, which violations it could not perpetrate on its own territory.

In *Montero v. Uruguay,* a case in which Uruguayan authorities' refused to issue a passport in Berlin, the Committee observed that "article 2(1) of the Covenant cannot be interpreted as limiting the obligations of Uruguay under article 12(2) to citizens within its

---

[106] Lopez Burgos v. Uruguay, U.N. HUMAN RIGHTS COMM., Communication No. 52/1979, ¶ 12.3 U.N. Doc. CCPR/C/13/D/52/1979 (1981).
[107] *Id.*

own territory."[108] The Committee has twice expressed this same view in its Concluding Observations on the United States of America. In 1995, it stated that (emphasis added):[109]

> [t]he Committee does not share the view expressed by the Government that the Covenant lacks extraterritorial reach under all circumstances. Such a view is contrary to the *consistent interpretation* of the Committee on this subject, that, in special circumstances, *persons may fall under the subject-matter jurisdiction of a State party even when outside that State's territory.*

A new General Comment should affirm the extraterritorial reach of privacy obligations under Article 17. Extraterritoriality is especially important in the context of privacy interests. Breaches of those interests will occur increasingly in more than one jurisdiction. If Article 17's obligations do not apply extraterritorially, privacy interests would be rendered meaningless because member states could do nothing to protect their own citizens' rights from interferences by other States, and the objects and purposes of the treaty as regards privacy would be defeated.[110]

4. Non-Discrimination

Finally, a new General Comment should clarify that member states have an obligation, consistent with Article 2(1) of the ICCPR, to ensure that privacy protections are realized without discrimination of any kind. General Comment 31 makes this clear, emphasizing that:

> the enjoyment of Covenant rights is not limited to citizens of States Parties but must also be available to all individuals, regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons, who may find themselves in the territory or subject to the jurisdiction of the State Party.[111]

Conclusion

There is a clear need for the Committee to replace the extant General Comment on the right to privacy. This report has explained the functional role of General Comments—as sources of authoritative guidance on a right in the ICCPR, documents that provide further detail about a right, and statements regarding specific policy applications—and has also outlined why General Comment 16 on the right to privacy is inadequate in its current form to perform those functions today. Although General Comment 16 provides some important analysis of the components of Article 17 protections, it is a limited

---

[108] Mabel Pereira Montero v. Uruguay, U.N. HUMAN RIGHTS COMM., Communication No. 106/1981, ¶ 9.4, U.N. Doc. CCPR/C/18/D/106/1981 (1983).
[109] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, United States at ¶ 284, U.N. Doc. CCPR/C/79/Add.50 (1995) [hereinafter U.N. HUMAN RIGHTS COMM., Concluding Observations on the United States of America].
[110] Alex Sinha, *NSA Surveillance Since 9/11 and the Human Right to Privacy*, 59 LOY. L. REV. (forthcoming Winter 2014).
[111] General Comment 31 at ¶ 10.

exposition of a complex right. Understandably, it 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 the General Comment on privacy, the international community risks a further erosion of privacy protections that will seriously undermine the object and purpose of the treaty with respect to Article 17. Publication of a new General Comment will help ward off this growing threat and will help stabilize, on modern footing, the meaning of the right to privacy.

The foregoing analysis lays down the building blocks for a new General Comment. A new General Comment will have to develop an account of the values underlying privacy; provide an explanation of what the concepts of "home," "correspondence," and "family" mean today in light of new technologies; and provide a framework for what constitutes "interference" with privacy that is "unlawful" or "arbitrary." A new General Comment also needs to address current controversial and complex issues that have implications for privacy in the modern era, such as surveillance and other forms of data collection, retention, and use. These principles and the accompanying draft General Comment are offered in the main to spark debate and discussion. Any finalized General Comment arising out of the debate will, of course, be the sole responsibility of the HRC, as guided by its jurisprudence (as 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 developing world, and if the ICCPR is to retain its resonance as a leading instrument to ensure that protection, it is imperative that the HRC begins the process to review and replace General Comment 16 today.

Appendix 1: A Draft Revised General Comment

Article 17: The Right to Privacy

I. General remarks

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

2. The right to privacy is foundational for the healthy development of self and community. The right holds the balance between the public sphere in society, and other spheres.

3. Paragraph 1 of Article 17 protects both the right to privacy and the right not to have one's honour and reputation attacked. The reference to "privacy, home, family, or correspondence" aims to cover the ground of privacy protection, rather than to provide for individuated rights. The right to housing is protected by the International Covenant on Economic, Social, and Cultural Rights.[1] The right to family is separately protected elsewhere in the International Covenant on Civil and Political Rights.[2] Paragraph 2 of Article 17 underscores that everyone is entitled to the protection of the law in relation to both rights.

4. Both paragraphs of Article 17 have a wide reach. Paragraph 1 states that "no one" shall have their right to privacy arbitrarily or unlawfully interfered with, or their right to honour and reputation attacked. Paragraph 2 maintains that "everyone" has the right to protection of the law in this context. No individual is to be excluded from the domain of Article 17's protection.

"Privacy"

5. Privacy serves a constellation of values. The right to privacy ensures a sphere is reserved for self-expression of identity.[3] 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[4] and dignity.[5] As well, it extends to the right to be different and live accordingly,[6]

---

[1] See Article 11.
[2] See Article 23.
[3] Coeriel et al. v. The Netherlands, U.N. HUMAN RIGHTS COMM., Communication No. 453/1991at ¶ 10.2, U.N. Doc. CCPR/C/52/D/453/1991 (1994); See, e.g., Ituango Massacres v. Colombia, Judgment, ¶¶ 193-194, Inter-Am. Ct. of H.R. (July 1, 2006); Article 11 of the ACHR contains a similar, but not identical, protection of privacy to Article 17 of the ICCPR.
[4] Toonen v. Australia, U.N. HUMAN RIGHTS COMM., Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (1994).
[5] 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, Inter-Am. Ct. H.R., Judgment, ¶ 143 (Nov. 28, 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 the right to autonomy. The right to privacy has evolved to encompass informational privacy – the right to access and control one's personal information.[7] These subcomponents of privacy are not exhaustive but provide a rudder for the future protection of interests in privacy.

6. No artificial distinctions ought to be drawn when defining privacy. In particular, both the metadata of communications and their contents deserve equal protection. In an age when modern information technologies allow for cost-effective mass collection, storage and synthesis of personal data, and monitoring of individuals wherever they are located (including their on-line activities), metadata and content are equally important to an individual's maintenance of a sphere of private life.[8]

"Family", "home", and "correspondence"

7. 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 digital privacy.[9] 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 used to access them.[10] Additionally, the specific mention of "correspondence" highlights the importance of protection of privacy of a broad array of communications, and the need to curb controls or censorship of such communications.[11] The Human Rights Committee has equated telephone calls with "correspondence."[12] And "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.[13]

---

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.

[6] 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).

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

[8] 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).

[9] 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).

[10] 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).

[11] Miguel Angel Estrella v. Uruguay, U.N. HUMAN RIGHTS COMM., Communication No. 74/1980, U.N. Doc. Supp. No. 40 (A/38/40) at 150 (1983).

[12] U.N. HUMAN RIGHTS COMM., *Consideration of Reports Submitted by States Parties Under Article 40 of the Covenant*, Concluding Observations, Bulgaria, U.N. Doc. CCPR/C/BGR/CO/3 at ¶ 22 (Aug. 19, 2011).

[13] Copland v. the United Kingdom, App. No. 62617/00, Judgment, Eur. Ct. H.R., ¶¶ 43-44 (Apr. 3, 2007).

8. The General Assembly has confirmed that "the same rights people have offline must also be protected online, including the right to privacy."[14] Accordingly, it is important that where concepts of "family," "home," and "correspondence" have digital or virtual equivalents, equal protection is afforded to online as well as offline manifestations of these concepts. Most obviously, this means that e-mail and electronic communication that constitute "correspondence" must receive the same protection as letters and other communications that have previously been the subject of Human Rights Committee jurisprudence.[15]

Implementing these rights

9. It must be reiterated that the rights guaranteed in Article 17 are to be protected from all interferences and attacks, whether these emanate from State parties or private actors. States must also adopt legislative and other measures to give effect to the prohibitions on these interferences and attacks.[16] Paragraph 2 of Article 17 underscores the need for protection of the law, and also serves as a reminder that discretionary power (for example, exercised by the executive branch of governments) ought to be regulated by law where privacy interests might be engaged. It also highlights the need for independent and effective judicial oversight of any conduct that may potentially implicate privacy interests.[17]

10. It should be recalled that the Covenant applies extra-territorially. It is necessary to reinforce this point in the context of privacy, given the danger of cross-border violations of privacy. As noted in Article 2(1) of the Covenant, States must respect and ensure rights for all individuals subject to their territory or subject to their jurisdiction.[18] This means that a State Party must ensure protection of rights to everyone within its territory, and everyone within the power or effective control (including virtual power or effective virtual control) of that State Party outside of its territory.[19] Individuals subject to surveillance by a foreign State Party are within the power of that State Party. The Human Rights Committee has made clear that Article 2(1) "does not imply that the State party concerned cannot be held accountable for violations of rights under the Covenant which its agents commit upon the

[14] U.N. GAOR, 68th Sess., 3d comm. mtg., U.N. Doc. A/RES/68/167 (Dec. 18, 2013).
[15] Pinkney v. Canada, U.N. HUMAN RIGHTS COMM., Communication No. 27/1978, U.N. DocCCPR/C/OP/1 at 95, ¶ 34 (1985).
[16] See, e.g., General Comment 16, supra note 7.
[17] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, The Netherlands, U.N. Doc. CCPR/C/NLD/CO/4 (2009) [hereinafter U.N. Human Rights Comm., Concluding Observations on the Netherlands].
[18] See also, General Comment 31 at ¶ 10.
[19] *Id.*

territory of another State."[20] The view that the Covenant has no extraterritorial reach is contrary to the "consistent interpretation" of the Covenant.[21]

11. Article 2(1) of the Covenant makes clear, too, that rights must be respected and ensured consistent with the principle of non-discrimination. Distinctions based on national origin, for example, are prohibited. Non-nationals' privacy must rights must be given the same protection as nationals of a State.

12. States parties must also ensure effective remedies to victims where arbitrary or unlawful interferences with privacy occur, or where there are attacks on a person's honor or reputation.[22]

II. Limitations on the right to privacy

13. Privacy of person is not absolute under Article 17. Although the Covenant does not enumerate the permissible reasons for infringing 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. This reinforces the need for a culture of legality to pervade any governmental or private action that engages privacy interests and the duties of State parties to provide access to effective remedies.

15. The text of Article 17 does not contain any specific exceptions limiting the enjoyment of privacy, as in the case of Article 19, paragraph 3 of the ICCPR relating to freedom of expression or Article 8, paragraph 2 of the European Convention of Human Rights on the right to privacy. This absence of built-in restrictions indicates the need for robust protection of privacy under the ICCPR. A strict and narrow interpretation of the phrase "arbitrary or unlawful interference" is therefore warranted.[23]

16. Article 17 is a derogable right, per Article 4, paragraph 2 of the Covenant. Furthermore, Article 51 permits the State parties to amend the Covenant, if they so desire. These provisions fortify the view that a careful textual

[20] Lopez Burgos v. Uruguay, U.N. HUMAN RIGHTS COMM., Communication No. 52/1979, ¶ 12.3 U.N. Doc. CCPR/C/13/D/52/1979 (1981).
[21] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, United States at ¶ 284, U.N. Doc. CCPR/C/79/Add.50 (1995) [hereinafter U.N. HUMAN RIGHTS COMM., Concluding Observations on the United States of America].
[22] Bulgakov v Ukraine, U.N. HUMAN RIGHTS COMM., Communication No. 1803/2008, ¶9 U.N. Doc. CCPR/C/106/D/1803/2008 (1985).
[23] See generally, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* OHCHR, A/HRC/13/37 at ¶ ¶ 14-19 (Dec. 28, 2009) [hereinafter Special Rapporteur 2009 Report].

interpretation of Article 17's limitations on the right to privacy is necessary. Novel defences for those who interfere with privacy rights cannot be fashioned if not grounded in the text of Article 17. If States parties seek further defences, they can derogate from the right, or can propose an amendment to the right.

"Interference"

17. The interpretation of Article 17 has to be developed in light of recent advances in information technology, the now artificial distinction between metadata and content, the erosion of public and private spheres, and the modern day capacities of State parties to infringe persons' rights to privacy by tracking Internet activities, collecting, storing and synthesizing electronic data.

18. The term "interference" includes, among other things, the simple collection or storage of personal information or data, as well as any manual or automated searching, review, obstruction, or diversion of communications.[24]

19. "Interference" extends to indirect interference or the threat of interference if a person is able to show that the challenged action or legislative provision poses a threat to, or produces a chilling effect on, the enjoyment of their privacy.[25] This applies to cases where a person is able to show that they might be (or are in contact with someone who might be) the target of surveillance, even if, in fact, they (or their contact) turn out not to have been such a target. 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 data about communications, or metadata, also constitutes a prima facie interference with the right to privacy.[26]

"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 be consistent with the provisions, aims, and objectives of the Covenant.[27] Second, the interference must be pursuant to, and in accordance with, enacted

[24] General Comment No. 16 at ¶ 10; Copeland v. the United Kingdom, App. No. 62617/00, Judgment, Eur. Ct. H.R. (2007).
[25] Toonen v. Australia, U.N. HUMAN RIGHTS COMM., Communication No. 488/1992, U.N. Doc. CCPR/C/50/D/488/1992 (1994).
[26] 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).
[27] General Comment No. 16, at ¶ 3.

law (including international law).[28] Third, the domestic statutory framework must be accessible and ensure that any interference with privacy interests is reasonably foreseeable to the person concerned.[29] Fourth, domestic law must be "precise" and "clearly" defined.[30]

22. The second, third, and fourth requirements of lawfulness mirror 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."[31] This same test should guide the meaning of "unlawful" under the ICCPR.

23. The term 'unlawful' "means that no interference can take place except in cases envisaged by the law" (emphasis added).[32] It provides a measure of legal protection against the possibility of interference through executive acts and discretion. The term "unlawfulness" should also be interpreted in light of international laws and standards.[33]

24. Accessibility and foreseeability requires that laws and regulations governing privacy interests be made public and accessible. Foresight of the potential consequences of given conduct allows individuals to regulate their conduct in accordance with the law, thereby serving as a necessary protection against unlawful interference.[34]

25. The third requirement, specificity and precision, is a safeguard against abuse of power. It derives support from Human Rights Committee comments on wire-tapping[35] and from paragraph 8 of General Comment 16, which specifies

---

[28] 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.

[29] S.W. v. the United Kingdom, App. No. 20166/92, Judgment, Eur. Ct. H.R. ¶¶ 44-48, Series A no. 335-B (1995); K.-H.W. v. Germany [GC], App. No. 37201/97, Judgment, Eur. Ct. H.R. ¶¶ 72-76 (2001) (extracts).

[30] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Jamaica, U.N. Doc. CCPR/C/79/Add.83 at ¶ 20 (Nov. 19, 1997); U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Comments, Russian Federation, U.N. Doc. CCPR/C/79/Add.54 at ¶ 19 (July 26, 1995); General Comment 16, supra note 7, at ¶¶ 3, 8.

[31] Kafkaris v. Cyprus [GC], App. No. 21906/04, Judgment, Eur. Ct. H.R. ¶¶ 150-152 (2008).

[32] General Comment 16, supra note 7, at ¶ 3.

[33] 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).

[34] 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).

[35] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Jamaica, U.N. Doc. CCPR/C/79/Add.83 at ¶ 20 (Nov. 19, 1997); U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article

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."[36]

"Arbitrary"

26. The requirement for non-arbitrariness is distinct from the requirement that interference be lawful, and in accordance with the aims and objectives of the Covenant. States parties must ensure that the former is not conflated with the latter.

27. The term "arbitrary" within the meaning of Article 17, paragraph 1 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 suitable; namely it must be capable of achieving its stipulated aim. More specifically, there must be a rational connection between the interference and the aim. Third, the interference must be strictly necessary, and should be the least intrusive means of realizing its aim. Fourth, the interference must be fairly balanced in relation to the purpose sought to be achieved.[37]

28. A proportionality test is the correct method of interpreting "arbitrary" in relation to Article 17 because it incorporates a better framework, has been developed across jurisdictions,[38] and is consonant with the aims, objectives and purpose of the Covenant. It restricts the effects of the actions of States parties or private entities and provides safeguards to protect persons from the arbitrary infraction of their privacy rights.[39] The four prongs of the proportionality test are also consistent with General Comment 16's stipulation that only "information relating to an individual's private life, the knowledge of which is essential in the interests of society" can be called for by public authorities.

---

40 of the Covenant, Comments, Russian Federation, U.N. Doc. CCPR/C/79/Add.54 at ¶ 19 (July 26, 1995); General Comment 16, supra note 7, at ¶¶ 3, 8.

[36] *Id. at* ¶ 8.

[37] Toonen v. Australia, U.N. HUMAN RIGHTS COMM., Communication No. 488/1992, ¶14 U.N. Doc. CCPR/C/50/D/488/1992 (1994); R v Oakes, [1986] 1 S.C.R. 103, ¶ 70; 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., ¶¶ 42, 59, Series A no. 28 (6 September 1978). See also, Special Rapporteur 2009 Report, ¶¶ 14-18.

[38] See, e.g. R (Daly) v Home Secretary, [2001] 2 AC 532, ¶ 547; Bundesverfassungsgericht (BverfG - Federal Constitutional Court), 1 BvR 518/02 in Germany; STC 7/2004 and STC 261/2005 in Spain.

[39] See also, General Comment 16, supra note 7, at 7 (only "information relating to an individual's private life, the knowledge of which is essential in the interests of society" can be called for by public authorities.)

29. The proportionality test underpinning the non-arbitrary interference with the right to privacy applies even in cases where national security concerns are implicated. In this regard it is helpful to recall paragraph 1 of Article 5 of the Covenant, which prohibits States parties or any person from engaging in an activity which limits the right (to privacy) to "a greater extent than provided for in the present Covenant."

30. Mass surveillance of the contents of communications, including the interception, wire-tapping, searching or recording of communications, constitutes an arbitrary interference with the right to privacy, as it does not represent the least intrusive means of achieving particular aims. Mass collection of information about communications also constitutes such an arbitrary interference for the same reason.[40]

31. Other forms of information gathering and storage may also constitute arbitrary interferences with the right to privacy, if the actions lack an effective oversight mechanism or the requisite safeguards, required by the structured proportionality test. Independent oversight is required to prevent abuse,[41] prior judicial approval is required to ensure only pertinent evidence is being targeted,[42] and data must not be used for any purpose contrary to Article 17 or the Covenant.[43]

III. 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 the person, expressed in Article 9, rests on some of the same values as Article 17. In particular, interests in liberty and a protected sphere of action are respected by both Article 9 and Article 17. In addition, paragraph 1 of Article 9 emphasises the importance of legal procedures and protections, bearing some resemblance to paragraph 2 of Article 17.

---

[40] 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-203/12, C-594/12, Digital Rights Ireland Ltd v The Minister for Communications, Marine and Natural Resources [2013] C-203/12, C-594/12, ¶ 72 (H. Ct.) (Ir.) *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=683832.

[41] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Poland, U.N. Doc. CCPR/C/79/Add.110, ¶22 (1999) [hereinafter U.N. HUMAN RIGHTS COMM., Concluding Observations on Poland]; U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, Sweden, U.N. Doc. CCPR/C/SWE/CO/6, ¶ 18 (2009) [hereinafter U.N. HUMAN RIGHTS COMM., Concluding Observations on Sweden].

[42] U.N. HUMAN RIGHTS COMM., Consideration of Reports Submitted by States Parties under Article 40 of the Covenant, Concluding Observations, The Netherlands, U.N. Doc. CCPR/C/NLD/CO/4, ¶ 14 (2009) [hereinafter U.N. Human Rights Comm., Concluding Observations on the Netherlands].

[43] U.N. HUMAN RIGHTS COMM., Concluding Observations on Sweden, supra note 41, ¶ 18.

33. Violations of Article 17 threaten other rights in the Covenant. The Special Rapporteur on the protection and promotion of the right to freedom of expression and opinion has observed that insufficient privacy protections may have a chilling effect on other rights, such as the right to freedom of expression under Article 19 of the Covenant. Individuals may be chilled into silence in their online communications, for example, if they cannot be assured that their communications are private.[44] In addition, inroads into privacy rights may 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 privacy of online activity may deter an individual from engaging at all online, thereby limiting that individual's rights to free speech, freedom of thought, freedom of association, and political participation.

34. Protection of privacy is essential to securing a panoply of other related rights in the Covenant.

[44] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression,* OHCHR, A/HRC/23/40 at ¶ ¶ 24-27 (Apr. 17, 2013).