The Right Whose Time Has Come (Again)

Privacy in the Age of Surveillance

By Dinah PoKempner

Technology has invaded the sacred precincts of private life, and unwarranted exposure has imperiled our security, dignity, and most basic values. The law must rise to the occasion and protect our rights.

Does this sound familiar?

So argued Samuel Warren and Louis Brandeis in their 1890 *Harvard Law Review* article announcing "The Right to Privacy."[I] We are again at such a juncture. The technological developments they saw as menacing—photography and the rise of the mass circulation press—appear rather quaint to us now. But the harms to emotional, psychological, and even physical security from unwanted exposure seem just as vivid in our digital age.

Our renewed sense of vulnerability comes as almost all aspects of daily social life migrate online. At the same time, corporations and governments have acquired frightening abilities to amass and search these endless digital records, giving them the power to "know" us in extraordinary detail.

In a world where we share our lives on social media and trade immense amounts of personal information for the ease and convenience of online living, some have questioned whether privacy is a relevant concept.[II] It is not just relevant, but crucial.

Indeed, privacy is a gateway right that affects our ability to exercise almost every other right, not least our freedom to speak and associate with those we choose, make political choices, practice our religious beliefs, seek medical help, access education, figure out whom we love, and create our family life. It is nothing less than the shelter in which we work out what we think and who we are; a fulcrum of our autonomy as individuals.

The importance of privacy, a right we often take for granted, was thrown into sharp relief in 2013 by the steady stream of revelations from United States government files released by former National Security Agency (NSA) contractor Edward Snowden, and published in the *Guardian* and other major newspapers around the world. These revelations, supported by highly classified documents, showed the US, the UK, and other governments engaged in global indiscriminate data interception, largely unchecked by any meaningful legal constraint or oversight, without regard for the rights of millions of people who were not suspected of wrongdoing.

The promise of the digital age is the effortless, borderless ability to share information. That is its threat as well. As the world's information moves into cyberspace, surveillance capabilities have grown commensurately. The US now leads in ability for global data capture, but other nations and actors are likely to catch up, and some already insist that more data be kept within their reach. In the end, there will be no safe haven if privacy is seen as a strictly domestic issue, subject to many carve-outs and lax or non-existent oversight.

Human Rights Watch weighed in repeatedly throughout 2013 on the human rights implications of Snowden's revelations of mass surveillance, and the need to protect whistleblowers. This essay looks at how the law of privacy developed, and where it needs to reach today so that privacy is globally respected by all governments, for all people. Global mass surveillance poses a threat to human rights and democracy, and once again, the law must rise to the challenge.

A Concept Develops: The "Right to be Let Alone"

Many countries have long recognized the values that underlie the legal right to privacy—honor, reputation, and the sanctity of home and family life. But it was in the United States that private rights of action to defend privacy crystallized in the wake of Warren and Brandeis' call.

Judge Cooley in 1882 described privacy as "the right to be let alone."[III] Tort law over the next century allowed people—many of them celebrities or people trying to avoid celebrity—to obtain remedies against unwanted public disclosure or non-consensual exploitation of private information.[IV] The developing legal doctrine, aimed at shielding reputation and

honor, quickly conflicted with press freedom and the public's right to information—most notably when newspapers sought to cover issues of general public interest that might include embarrassing information about public figures.

The law as it developed in the US was deferential to freedom of speech concerns, in practice allowing the media wide latitude; in Europe, there was greater emphasis on protecting reputational rights and shielding personal information.[V]

Privacy as a limit on government intrusion gained ground in the wake of World War II and the rise of modern surveillance states. The Third Reich had relied heavily on census data to persecute, while many Communist states developed elaborate surveillance and data collection systems to monitor their populations and suppress dissent—restrictions that continue today in China, Vietnam, North Korea, Turkmenistan, and Cuba.

After World War II, the right to privacy made its way into many international human rights instruments and national constitutions, often phrased as freedom from interference with "privacy, family, home or correspondence," and the more traditional freedom from attacks on "honour and reputation."[VI]

Privacy has never been considered an absolute right. In international law it can be derogated, or limited, when a grave public emergency threatens the nation's life. Even then, the emergency must be officially proclaimed, and limitations not greater than the threat requires, nondiscriminatory, and consistent with international law, including respect for human rights.[VII]

If there is no such emergency, intrusions on privacy, family, home, and correspondence may not be arbitrary and must be embodied in laws that create clear expectations as to how and when they will likely be applied. These laws must aim to protect a legitimate interest in a democratic society, such as public safety or national security, be necessary and proportionate to that end, and subject to judicial safeguards and remedies.[VIII] These basic principles are common to most modern judicial consideration of various aspects of privacy.

Mind the Gap: New Technology and "Reasonable" Expectations

An important aspect of the law of privacy developed from the regulation of government search and seizure, generally in the context of criminal investigation. As the law developed,

judicially authorized warrants for official searches became a common requirement, and some legal systems treated unauthorized searches as a crime. The notion of privacy of "correspondence" broadened to include new technologies, such as telephones, with laws regulating when authorities could use wiretaps.

Yet protections have often lagged behind technological change. In the 1928 *Olmstead* case, the Supreme Court held that an unauthorized wiretap introduced as evidence in a criminal trial did not violate the constitutional right of the people "to be secure in their persons, houses, papers and effects."[IX] In 1967, the court reversed course, determining a person has "reasonable expectation of privacy" when talking in a public phone booth.[X] This bit of common sense developed into a doctrine for when to limit government power to conduct warrantless searches. While the home has generally remained inviolable in US law, what is outside the home or in public view (trash at the curb, a car backseat) is not.

But even judicial doctrine as to when expectation of privacy is "reasonable" has often not kept pace with rapid technological shifts or even popular expectations.[XI] Brandeis, later a Supreme Court justice, foresaw this problem in his famous *Olmstead* dissent when he predicted: "Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." He added: "Can it be that the Constitution affords no protection against such invasions of individual security?"[XII]

Brandeis' concern is fully justified in our age of mass data interception. Wiretaps eventually needed warrants, but surveillance metastasized in the 21st century under new laws that set lax standards for many types of digital information.

Privacy: Secrecy or Self-Determination?

The "reasonable expectation" doctrine led US law to conclude that many types of business records were not protected from search without warrant, based on the rationale that an individual shared the information willingly with a third party and could not object if it became known.[XIII]

But the objection has often been raised that sharing some personal information with a corporation does not mean there is an expectation it will be divulged to the government;

on the contrary, we usually expect some discretion and confidentiality in our business transactions.[XIV] Nor is it entirely accurate to say that sharing personal information via business records is entirely "voluntary," given how many necessary transactions of modern life require considerable disclosure.

US law has grown to equate "privacy" of communications with "secrecy," an approach "ill-suited to the digital age," in the recent words of Justice Sonia Sotomayor.[XV] The law in Europe took a different path. Germany, which recognizes a constitutional right of "personality," or the protection of one's integrity and capacity for self-development,[XVI] led the way. In 1983, its Constitutional Court annulled the national census law, announcing "informational self-determination" as a fundamental democratic right.[XVII]

Key to the European approach was the belief that individuals have a right to access and correct their data held by various institutions, and ultimately have a right to determine its use and disposal. An interlocking system of regional guidelines and standards emerged, albeit subject to national variation in legislation and application.[XVIII] In contrast, US data privacy law is a welter of difficult-to-navigate state laws or laws governing particular industry sectors that are often focused on data breach and fraud rather than on informational self-determination.

Still, the European approach is not beyond criticism: it has required businesses to retain data for significant periods beyond their own needs so the government may have access,[XIX] and makes oversight of government access subject to varying national standards.[XX] As data accumulation has moved from centralized storage to global "cloud" computing that involves more jurisdictions, actors, and laws, maintaining control over one's personal data has become more complicated as well.

Anonymity as the Ultimate Data Protection

One of the surest ways to control personal data—withholding one's real identity when communicating—found acceptance more readily in the US than elsewhere, not least because many of the nation's founders published revolutionary manifestos under pseudonyms.

While anonymity has never been considered an absolute or stand-alone right, the US Supreme Court has long recognized it to be part of speech that is entitled to a high level of

protection,[XXI] in part, as Justice Stevens wrote in 1995, because it can encourage speech. "Anonymity," he asserted, "…provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent."[XXII]

Anonymity is increasingly precious—and imperilled—amid the growing quantity of information online and advances in aggregating and searching databases, and is critical for people to be able to share ideas publicly without fear of retaliation or persecution.[XXIII]

In April 2013, the UN special rapporteur on the promotion and protection of the right to freedom of opinion, Frank LaRue, wrote of the "chilling effect" that restrictions on anonymity had on the free expression of information and ideas. He pointed out that when corporate actors exploit real name registration requirements to amass and mine personal data, they assume a serious responsibility to protect the privacy and security of such information.[XXIV]

Physical Privacy: Autonomy, Security, and Identity

As the law of search and seizure shows, understanding privacy in the physical world can influence its application to the virtual world. The strand of law protecting a person's intimate bodily attributes and decisions—including whether to choose marriage, abortion, start a family, or accept medical treatment—describes privacy as a way to assert one's physical autonomy and preferred identity, not as isolation or secrecy. [XXV] As such, it holds relevance for protecting autonomy and identity in cyberspace as well.

A key decision related to physical privacy is the 1994 case of *Nicholas Toonen v. Australia*. The Human Rights Committee, the treaty body that interprets the International Covenant on Civil and Political Rights (ICCPR), repudiated Tasmania's criminal law of sodomy declaring "it is undisputed that adult consensual sexual activity in private is covered by the concept of 'privacy.'" *Toonen* rejected the rationale that the law was to prevent the spread of HIV/AIDS, and argued it was not a reasonable or proportionate means to that end, and more likely to drive a vulnerable population underground.[XXVI]

In *Goodwin v. U.K.*, the European Court of Human Rights in 2002 similarly emphasized the many adversities post-operative transsexuals suffer when they cannot change the sex on their birth certificate, including denying their right to marry, employment discrimination,

and the denial of social benefits. The court focused on privacy in the sense of "the right to establish details of their identity as individual human beings" and concluded that transsexuals were entitled to "personal development and physical and moral security in the full sense enjoyed by others in society."[xxvii]

The logic of *Toonen* and *Goodwin* informs two recent foci of Human Rights Watch's privacy-related work: our call for decriminalizing simple drug use and possession (see the essay *The Human Rights Case for Drug Reform* in this volume),[xxviii] and our push for decriminalizing voluntary sex work by adults.[xxix]

Both drug use and even voluntary sex work can pose serious risks to health and safety (including heightened risk for HIV/AIDS), but driving participants into the shadows is usually highly counterproductive to efforts to treat, mitigate, or prevent harm. Criminalization in both cases can cause or exacerbate a host of ancillary human rights violations, including exposure to violence from private actors, police abuse, discriminatory law enforcement, and vulnerability to blackmail, control, and abuse by criminals. These severe and common consequences, and the strong personal interest that people have in making decisions about their own bodies, mean it is unreasonable and disproportionate for the state to use criminal punishment to discourage either practice.[xxx]

These approaches to physical self-determination are directly relevant to online privacy too. The physical and the virtual world are of course connected; our offline choices about friends, work, sexual identity, and religious or political beliefs are reflected in our online data and communications. Unwanted exposure of our private information can undermine the physical and moral security that the *Goodwin* decision emphasized is a key aim of privacy, and prevents us from developing a personal identity sheltered from coercion—considerations that underlie the creation of data privacy laws in the first place.

Surveillance's "Golden Age"

Two important developments have transformed the debate on privacy and ushered in what some have termed a "golden age of surveillance."[xxxi] The first was the shift of almost every aspect of social, economic, and political relations online, so that disruption to, or surveillance of, online activity can potentially harm or be used to harm almost every human right—whether civil, political, economic, social, or cultural.

The second development is the enormous advance in our ability to store, search, collate and analyze data with minimal effort and cost. This has serious implications for collecting and retaining data, providing enormous incentive to amass information at a time when much of our lives is exposed through online data. Moreover, states, including the US, have devoted considerable resources to ensuring our data is always accessible, including seeking backdoors into technology and collection points, and cracking strong encryption.[xxxii]

Concerns about the privacy of online communications and digital information were strong even before Edward Snowden began disclosing in June 2013 the massive and global extent of surveillance by the US National Security Agency. But since then, intense debate has raged as to whether mass surveillance is ever justified, and whether privacy can actually be effectively protected against governments and corporations bent on espionage.

Once again, we find that law and the courts have not kept pace.

Legal Loopholes for Surveillance

Though a crime in most legal systems, espionage is not banned in international law, and most governments practice it to some degree. But as the birthplace of the Internet, home to major related industries, and with most global online communications running through its territory or facilities, the US is uniquely placed to conduct global surveillance. Consequently, it is worth examining the loopholes it has knit into its legal doctrines that give it a relatively free hand in capturing bulk data.

The first big loophole is that the US does not extend Constitutional rights to foreigners abroad, whether protection from "unreasonable" search, privacy, or freedom of speech (including anonymous speech). Nor does the US recognize extraterritorial application of its obligations under the International Covenant on Civil and Political Rights. Instead, US law authorizes warrantless surveillance of foreign intelligence so long as the secret Foreign Intelligence Surveillance Court (FISC) approves measures to "target" collection of "foreign intelligence" information and "minimize" the incidental collection of the communications of US citizens or residents.[xxxiii] While foreigners have no protection against data collection, there are many exceptions for US persons that allow the government to retain their data as well—including encrypted communications and attorney-client communications. [xxxiv]

Another big loophole is that the US considers "metadata," or the information about each message—such as date, time, location, sender, recipient—to be business records that are disclosed to third parties, and so entitled to a far lower standard of protection than substantive conversation, under both constitutional doctrine and section 215 of the PATRIOT Act. This type of data can provide an incredibly detailed portrait of anyone's movements, interlocutors, transactions, and concerns over time.

These two exceptions give enormous scope for bulk surveillance, but the government has also applied elastic interpretations to the law's already generous terms. Orders for "targeting" foreign intelligence do not need to specify particular investigations or persons, just general objectives; and such "targeted" surveillance means having just "51% confidence"—a hair better than a coin toss—that the people whose data is collected are foreigners abroad. The FISC determined that *all* metadata records from major US telephone companies such as Verizon could be "relevant" to intelligence or espionage investigations, an interpretation that begs the meaning of "relevant."

Another major loophole to both international and domestic legal obligations is intelligence sharing arrangements that let states circumvent particular legal strictures on their own data collection activities. This appears to have been the case with US cooperation with the UK.[xxxv]

The present-day data collection practices of European states, including those collaborating with the NSA, have yet to be tested under the European Convention on Human Rights, but the case of *Klass v. Germany* suggests more demanding scrutiny could eventuate. There, the European Court of Human Rights emphasized that for surveillance to respect the right to privacy, there must be "adequate and effective guarantees against abuse" and that in view of the danger secret surveillance poses to democracy, states may not, "in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate."[xxxvi]

The US Congress is percolating with legislative proposals to reform the legal structure that enables mass surveillance, though none so far would protect the privacy rights of foreign persons located outside US territory. But a world of globalized communications and surveillance needs universal standards that are not too readily evaded or bent. Unless the

development of privacy as a legal right catches up to fill these gaps, the right may well become obsolete.

Global Communications, Global Obligations

What should be done?

Some argue we must simply live with the reality of pervasive online surveillance, and that public expectation of privacy has eroded. But this is neither accurate nor dispositive. Our understanding of privacy has in fact grown far beyond "a right to be left alone" into a right of personal self-determination, embracing the right to choose whom we share our personal details with and what identity we project to various communities. When applied to the digital world, privacy gives us some boundaries against unwanted monitors, and with it the essential freedom for personal development and independent thought.

While global surveillance will require a complex and global response, the US bears a particular burden, as a leader in both cyber-technology and mass surveillance, to rein in the serious overreach Edward Snowden brought to light. Among the steps Human Rights Watch has emphasized are requiring judicial warrant protection for metadata, recognizing that privacy is breached when data is collected (and not just when viewed or used), revamping the FISA court to make it a more adversarial and transparent body to check the NSA, and protecting whistleblowers who reveal rights-violating national security practices.

We must also recognize that the duty to protect rights in a world of globalized communication cannot stop at territorial borders. International law of the twentieth century assumed that a state's primary obligation is to ensure rights to all people in its territory or under its jurisdiction or effective control.[xxxvii] This makes sense, as generally one state cannot secure rights for people abroad without violating another country's sovereignty. But there are circumstances when a government must carry its human rights obligations beyond its national borders—such as when its police or military abroad capture an individual. What about when it captures the communications of millions of people at home and abroad?

Arguably, collecting and banking mass personal data over time confers such power to track, analyze, and expose people's lives that it should be thought of as a form of "effective

control." Some of us may not care about who sees our Facebook postings, but the security and human dignity of many people all over the world depends on the ability to limit who knows about their political preferences, sexual orientation, religious affiliation, and more.

Intentionally damaging acts, such as blackmailing, drone targeting, and coercion depend on discovering personal details; even when information is carelessly handled or misconstrued, terrible harms may result. A state that, without reasonable cause, appropriates in bulk the communications data of another state's inhabitants is damaging their security, autonomy, and exercise of their rights. At minimum, governments should apply the same legal protections to all persons whose privacy they breach as they do to their own citizens.

In the US, a federal court and an independent review panel appointed by the president joined the chorus of lawmakers in criticizing bulk data collection.[XXXVIII] President Obama was expected to announce his recommendations for surveillance policy reform on January 17, though it was unclear whether he would adopt his own review group's recommendations. European governments, quick to condemn NSA excesses, have failed so far to carry out effective reviews of their own policies of mass surveillance at home or abroad, including the extent to which they have collaborated in, or benefitted from, US data collection.[XXXIX]

It will take time to move the debate towards recognizing a global duty for states with extraterritorial surveillance capability to respect the privacy of all within their reach, but several encouraging signs suggest this will happen. In 2009, for example, Special Rapporteur on Human Rights and Counter-Terrorism Martin Scheinin called for developing soft law on data privacy and surveillance. In 2013, Special Rapporteur LaRue endorsed the need for the Human Rights Committee to update its General Comment on the right to privacy.[XL]

Two sets of principles that civil society expert groups recently issued may provide a basis for increasing consensus around standards: the Global Principles on National Security and the Right to Information ("The Tshwane Principles"),[XLI] endorsed by the Parliamentary Assembly of the Council of Europe;[XLII] and the International Principles on the Application of Human Rights to Communications Surveillance.[XLIII] These largely collect and restate general principles related to the right to privacy, transparency, and regulating surveillance in international law.

Most recently, Brazil and Germany in November 2013 introduced a UN General Assembly resolution that aims to create consensus against privacy abuses in digital surveillance both at home and abroad.[XLIV] The resolution calls for continuing reporting on mass surveillance and the right to privacy, including the implications of extraterritorial surveillance. Mirroring these efforts to articulate new standards are demands from civil society actors to reform government surveillance practices, ranging from a statement from major internet companies[XLV] to a petition addressed to world leaders by 562 well-known authors in 80 countries.[XLVI] These developments can strengthen international legal consensus and tip the balance of power back to individuals.

The year 2013 may well come to be viewed as a watershed when people around the world stood up to reassert their right to privacy. But this can only happen if these debates produce global standards and enforceable domestic laws with teeth. We cannot wait for individuals like Edward Snowden to blow the whistle, but must demand thorough investigation into the full extent of government and corporate data collection and analysis. States should commit to transparent and public review of their practices and laws in order to maximize—not trade off—privacy, security, and technical innovation that can enhance and further our lives and rights as human beings.

The right to privacy is not just about leaving people alone; it is about empowering them to connect, speak, think, and live on their own terms, without arbitrary state interference. The technological revolution is upon us, and we must do our best to help the law catch up—again.

Dinah PoKempner is general counsel at Human Rights Watch.

[I] Samuel D. Warren, Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review*, vol. 4, no. 5 (1890).

[II] See, e.g. Bobbie Johnson, "Privacy no longer a social norm, says Facebook founder," The Guardian, January 10, 2010 http://www.theguardian.com/technology/2010/jan/11/facebook-privacy (accessed December 9, 2013). Google also has argued that no gmail users have a reasonable expectation of privacy in their correspondence; see Google's motion to dismiss in In re Google Inc. Gmail Litigation, United States District Court, Northern District of California, Case No. 5:13-md-02430-LHK September 5, 2013 http://www.consumerwatchdog.org/resources/googlemotion061313.pdf (accessed December 9, 2013).

[III] Thomas McIntyre Cooley, A Treatise on the Law of Torts: Or the Wrongs which Arise Independent of Contract, 2nd ed. (Chicago: Callaghan and Company, 1888), p. 29.

[IV] See William L. Prosser, "Privacy," *California Law Review*, vol. 48, no. 3 (1960).

[v] James Q. Whitman, "The Two Western Cultures of Privacy: Dignity versus Liberty," *Yale Law Journal*, vol. 113: 1153 (2004): (accessed November 22, 2013), http://www.yalelawjournal.org/images/pdfs/246.pdf

[vi] See, e.g., Universal Declaration of Human Rights, adopted December 10, 1948, art. 12; International Covenant on Civil and Political Rights, art. 17(1); InterAmerican Convention on Human Rights, art. 11(2); European Convention on Human Rights, art. 8(1); cf. the recent post-communist Constitution of the Republic of Croatia, last revised in 2010, which includes not only the standard post-WWII privacy rights arts. 34 (homes inviolable), 35 (personal and family life, dignity and honor), 36 (freedom of correspondence and all other forms of communication), but also explicit protection for the "safety and secrecy of personal data" (art. 37). http://www.sabor.hr/Default.aspx?art=2408&sec=729 (accessed December 9, 2013).

[vii] See International Covenant on Civil and Political Rights, December 16, 1966, art. 4.1.

[viii] This is a general description of the standards common to most international instruments on privacy, with the most developed jurisprudence under the European Convention on Human Rights and the International Covenant on Civil and Political Rights. See Ian Brown and Douwe Korff, "Digital Freedoms in International Law," *Global Network Initiative*, June 14th, 2012, and sources cited at notes 17 and 18: (accessed November 22, 2013), https://globalnetworkinitiative.org/sites/default/files/Digital%20Freedoms%20in%20International%20Law.pdf

[ix] Olmstead v. United States, 277 US 438 (1928).

[x] *Katz v. United States,* 389 US 347 (1967).

[xi] For example, thermal scanning to detect marijuana cultivation has been used since the 1980s, but was only held to require a warrant in 2001. *Kyllo v. United States*, 533 US 27 (2001). Sometimes judicial findings that a particular technological surveillance technique engages no "reasonable expectation of privacy" appear quite counter-intuitive, as when aerial photography of manufacturing premises was compared to ordinary visual observation from the air or of an open field in Dow Chemical Co. v. US 477 US 227 (1986) or when a court analogized abandoned biological matter (susceptible to DNA analysis) to one's curbside trash in California v. Greenwood, 486 US 35 (1988); see also Elizabeth E. Joh, "Reclaiming 'Abandoned' DNA: The Fourth Amendment and Genetic Privacy, 100 NW. U. L. Rev. 857 (2006). There is also an argument that what may have seemed less reasonable when technological methods of surveillance first appear over time becomes more normal as people become acclimated to the invasion of privacy. These varying problems point to the underlying instability and subjectivity of the "reasonable expectations" test and the degree to which legal doctrines relating to new technology tend to be influenced by familiar physical analogies, appropriate or not.

[xii] *Olmstead v. United States*, 277 US 438 (1928) paras. 472-474 (Brandeis, dissenting).

[xiii] Two cases established this doctrine, *United States v. Miller*, 425 US 435 (1976) (bank records) and *Smith v. Maryland*, 442 US 735 (1979) (pen register of telephone calls).

[xiv] See exchange between Orin Kerr and Greg Nojeim, "The Data Question: Should the Third-Party Records Doctrine Be Revisited?" *ABA Journal Magazine,* August 2012, (accessed November 22, 2013), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/ . The European Court of Human Rights has also observed that privacy rights can apply to "activities of a professional or business nature," (*Niemietz v. Germany,* 16 EHRR 97 (1993), para. 29.

[xv] *United States v. Jones*, 565 US _, 132 S.Ct. 945 (2012) Docket no. 10-1259 (Sotomayor, J., concurring).

[xvi] See Edward J. Eberle, "The German Idea of Freedom," Oregon Review of Int'l Law Vol. 10 at p. 4 (2008) (discussing Basic Law art. 2.1) http://law.uoregon.edu/org/oril/docs/10-1/Eberle.pdf (accessed December 9, 2013).

[xvii] See Gerrit Hornung and Christoph Schnabel, "Data protection in Germany I: The population census decision and the right to informational self-determination," *Computer Law & Security Report*, vol. 25, issue 1 (2009), p. 84-88: (accessed November 22, 2013), http://dx.doi.org/10.1016/j.clsr.2008.11.002.

[xviii] Key developments include the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Privacy is also protected under EU law, including the EU Charter of Fundamental Rights and the 1995 Directive on the Protection of Personal Data.

[xix] The 2006 EU Data Retention Directive requires member states to require communications providers to retain communications data for a period of between 6 months and 2 years. The European Commission is engaged in an effort to revise the directive that would strengthen the privacy protections within it. For an excellent discussion of the abuses and human rights implications of mandatory data retention laws, see Erica Newland, "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development," *Center for Democracy and Technology*, October 2011, (accessed November 22, 2013) https://cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf

[xx] For a summary of the controversies surrounding the legality of the EU Data Retention Directive, see Electronic Frontier Foundation page on EU, (accessed November 22, 2013), https://www.eff.org/issues/mandatory-data-retention/eu

[xxi] McIntyre v. Ohio Elections Commission, 514 US 334 (1995).

[xxii] Ibid., 342.

[xxiii] For various examples, see Sam Gregory, "Human Rights Video, Privacy and Visual Anonymity in the Facebook Age," post to "Witness" (blog), February 16, 2011, http://blog.witness.org/2011/02/human-rights-video-privacy-and-visual-anonymity-in-the-facebook-age/ (accessed November 22, 2013).

[xxiv] Frank La Rue, "Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression," A/HRC/23/40 (2013), para. 49.

[xxv] See, e.g., *Griswold v. Connecticut*, 381 USUSUSUSUSUSUS 479 (1965) and *Eisenstadt v. Baird*, 405 USUSUSUSUSUSUS 438 (1972) (birth control); *Roe v. Wade*, 410 USUSUSUSUSUSUS 113 (1973) (abortion); *Lawrence v. Texas*, 539 USUSUSUSUSUSUS 558 (2003) (private consensual homosexual sex); *O'Connor v. Donaldson*, 422 USUSUSUSUSUSUS 563 (1975) (involuntary confinement for mental illness).

[xxvi] Human Rights Committee, Communication No. 488/1992: Australia. 04/04/1994 CCPR/C/50/D/488/1992 at paras. 8.4-8.6, accessed November 22, 2013, http://www.unhchr.ch/tbs/doc.nsf/0/d22a00bcd1320c9c80256724005e60d5.

[xxvii] *Goodwin v. United Kingdom*, 35 Eur. Ct. H.R. 18, para. 90 (2002).

[xxviii] Human Rights Watch, *Americas– Decriminalize Personal Use of Drugs*, June 4, 2013, http://www.hrw.org/news/2013/06/04/americas-decriminalize-personal-use-drugs

[xxix] See, e.g. Human Rights Watch, "Treat Us Like Human Beings: Discrimination against Sex Workers, Sexual and Gender Minorities, and People Who Use Drugs in Tanzania," June 2013, http://www.hrw.org/sites/default/files/reports/tanzania0613webwcover_0_0.pdf.

[xxx] These policies do not imply that states are prohibited from punishing drug or sex work activities that pose greater harm to others, such as trafficking, or that the state may not seek to discourage the sex or drug trade.

[xxxi] Peter Swire and Kenesa Ahmad, "'Going Dark' or a 'Golden Age for Surveillance,'" *Center for Democracy and Technology*, November 28, 2011 (accessed November 22, 2013), https://www.cdt.org/blogs/2811going-dark-versus-golden-age-surveillance.

[xxxii] Jeff Larson, Nicole Perlroth, and Scott Shane, "Revealed: the NSA's secret campaign to Crack, Undermine Internet Security" *ProPublica,* September 6, 2013, (accessed November 22, 2013), http://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[xxxiii] See section 702 of the FISA Amendments Act, as amended October 3, 2011, (accessed November 22, 2013) http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls

[xxxiv] Glenn Greenwald and James Ball, "The top secret rules that allow NSA to use US data without a warrant," *Guardian*, June 20, 2013, (accessed November 22, 2013), http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant (including link to one such order).

[xxxv] *The Guardian*, "NSA pays £100m in secret funding for GCHQ," August 1, 2013, http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden . See also, Human Rights Watch, "UK: Provide Clear Answers on Data Surveillance," June 28, 2013, http://www.hrw.org/news/2013/06/28/uk-provide-clear-answers-data-surveillance

[xxxvi] *Klass v. Germany*, 2 EHRR 214, paras. 50, 49 (1978)

[xxxvii] See International Covenant on Civil and Political Rights, art. 2.1. Although the text specifies "within its territory and subject to its jurisdiction," this has been interpreted disjunctively by the Committee as two separate conditions. See Manfred Nowak, *UN Covenant on Civil and Political Rights* (Kehl am Rhein: Engel, 2005), 2:4 p. 41-42 (para. 28: "When States Parties, however, take actions on foreign territory that violate the rights of persons subject to their sovereign authority, it would be contrary to the purpose of the Covenant if they could not be held responsible. It is irrelevant whether these actions are permissible under general international law … or constitute illegal interference"). See also UN Human Rights Committee, General Comment 31, Nature of the General Legal Obligation Imposed on States Parties to the Covenant, (Eightieth session, 2004), U.N. Doc. CCPR/C/21/Rev.1/Add.13 (2004) para. 10.

[xxxviii] Klayman v. Obama, Civ. Actions 13-0851, 13-0881 (RLJ) December 16, 2013 available at http://scholar.google.com/scholar_case?case=12334619679029296316&hl=en&as_sdt=6&as_vis=1&oi=scholarr and Liberty and Security in a Changing World, Report and Recommendations of the President's Review Group on Intelligence and

Communications Technologies, December 12, 2013, available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[xxxix] However, the European Parliament Committee on Civil Liberties, Justice and Home Affairs is carrying out an "Inquiry on Electronic Mass Surveillance of EU Citizens." http://www.europarl.europa.eu/committees/en/libe/subject-files.html?id=20130923CDT71796

[xl] Frank La Rue, A/HRC/23/40 (2013), para. 98. Many human rights nongovernmental organizations have also called for an update.

[xli] "The Global Principles on National Security and the Right to Information (Tshwane Principles)" (New York: Open Society Foundations, June 12, 2013), http://www.opensocietyfoundations.org/sites/default/files/global-principles-national-security-10232013.pdf (accessed November 22, 2013).

[xlii] Parliamentary Assembly of the Council of Europe, "Recommendation 2024 (2013): National security and access to information" (October 2, 2013).

[xliii] "International Principles on the Application of Human Rights to Communications Surveillance", July 10, 2013, https://en.necessaryandproportionate.org/text (accessed November 22, 2013) (HRW has endorsed these principles, along with nearly 300 other organizations).

[xliv]Ewen McAskill and James Ball, "UN surveillance resolution goes ahead despite attempts to dilute language," *The Guardian*, November 221, 2013 http://www.theguardian.com/world/2013/nov/21/un-surveillance-resolution-us-uk-dilute-language (accessed December 9, 2013).

[xlv] Aol, Facebook, Google, LinkedIn, Microsoft, Yahoo!, *Reform Government Surveillance* http://reformgovernmentsurveillance.com/ (accessed December 10, 2013).

[xlvi] Writers Against Government Surveillance, "A Stand for Democracy in the Digital Age," http://www.change.org/petitions/a-stand-for-democracy-in-the-digital-age-3 (released and accessed December 10, 2013).