



KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

PROTECTING HUMAN RIGHTS IN THE AGE OF SURVEILLANCE **ROUNDTABLE DISCUSSION**

Report For Public Distribution

April 8, 2014

I. Introduction

The Center for Democracy & Technology and the American University Washington College of Law Center for Human Rights and Humanitarian Law held a daylong convening on January 29, 2014, to discuss how to protect privacy and free expression rights in an era of massive trans-border surveillance. The discussion drew 45 participants from the United States, Europe, and Latin America and included academics, advocates, former jurists, and human rights experts.

The roundtable had several immediate outputs, including identification of key opportunities for civil society engagement for the short, medium, and long term. The group discovered key points of agreement between participants and areas to explore further. We also uncovered gaps in law, theory and practice that would benefit from new research and analysis. It became clear as the discussion progressed that there should be ongoing work to increase the alignment of strategies adopted by NGO, corporate, and academic actors. Engagement with the private sector, in particular, will be essential to the surveillance reform agenda.

II. Summary

The roundtable focused on specific areas of inquiry. First, the group discussed laws, norms, and principles applicable to mass surveillance in the international context. Second, participants identified legal, theoretical and practical gaps that need to be addressed. Third, the group evaluated key advocacy and scholarship opportunities that speak to these gaps, taking into account political and institutional realities that may help or hinder advocacy efforts.

A. Laws, Norms, and Frameworks

The following highlights a few of the many topic areas discussed during the conversation of laws, norms, and frameworks.

International Right to Privacy

There was general agreement among participants that it is important to consider whether current human rights instruments are sufficient to protect privacy in an era of systematic and cross-border surveillance. Participants had several different opinions about specifically how and where the right to privacy is implicated. For example, some participants held that the right to privacy is universal and states must therefore respect privacy rights of all people around the world. For others, this ideal is divorced from the reality of surveillance practices conducted by many nations and there is no international consensus that contemporary surveillance techniques are inappropriate. The group agreed that it is useful to break down questions about the right to privacy into smaller component questions, for example: 1. Does the right to privacy apply to a given situation, such as a particular surveillance activity? 2. If it does apply, does that activity violate this right? 3. When multiple sets of actors are involved (for example, two countries sharing the results of their respective surveillance activities or a government obtaining the assistance of a corporation in carrying out surveillance), how do the different components interact?

Extraterritorial Application of Human Rights Treaties

There was general agreement that the nature of global digital communications raises challenging issues around concepts of territory and jurisdiction. The group discussed both scholarly perspectives on extraterritorial application of human rights treaties, as well as the current state of interpretation from different human rights bodies. Over the course of the discussion participants emphasized that the United States is an outlier in its strictly territorial interpretation of its obligations under the International Covenant on Civil and Political Rights (ICCPR). While many scholars, jurists, and states support a broader interpretation, applicable jurisprudence is scant and sometimes conflicting. It is important for human rights bodies to address the issue of cross-border surveillance more explicitly in a range of venues to build a body of law.

Participants identified a range of communications surveillance scenarios that may implicate different bases for jurisdiction. They also examined specific cases that take a more expansive view of jurisdiction¹ and discussed the strategic implications of these cases for future advocacy. For example, in the opinion of one expert the best way to build accountability around surveillance is through international fora, where a complaint might target not only the nation conducting the surveillance but also complicit states sharing the results of the surveillance.²

Complicity and Positive Obligations

The group discussed the issue of whether states have a positive obligation to actively protect against human rights violations of other states and also whether a state's complicity in the mass surveillance activities of other states constitutes a human rights violation. There was significant energy around this topic, and a range of views was presented. Participants discussed how

¹ See for example *Munaf v. Romania*, Human Rights Comm., U.N. Doc. CCPR/C/96/D/1539/2006, ¶ 14.2 (2009).

² A case pending before the European Court of Human Rights poses exactly this question: *Big Brother Watch v. UK* challenges both the activities of the British government and the UK's receipt of information collected by the United States. CDT and others have applied for permission to intervene in the case. See application, https://www.cdt.org/files/pdfs/Application-to-Intervene_4.2.14_FINAL.pdf, and case study, <https://www.cdt.org/files/pdfs/BBW-et-al-v-UK-summary.pdf>.

models of complicity and positive obligations differ among international bodies, and noted how the European Court of Human Rights has produced some progressive jurisprudence on the topic.³ Some discussants warned that positive obligations must be approached cautiously. If countries act on positive obligations to protect their own citizens, for example by imposing data localization mandates, the result of such policies may be harmful to the open Internet. There was also concern that it is difficult to assess the positive obligations of states without more detailed information about the realities of state surveillance laws and practices.

Bulk Collection

Participants discussed whether bulk collection of individuals' data under surveillance regimes can be consistent with human rights. From one perspective, the indiscriminate collection of data, including about persons suspected of no wrongdoing, is necessarily a human rights violation. Several participants pointed out, however, that if bulk surveillance is never consistent with international human rights, then many countries have been persistent international human rights violators, as they have been conducting these practices over older technologies for decades. Participants also raised the concern that the line between collection and use is becoming increasingly blurred. Opinions on whether and how this line remains meaningful are evolving with participants' growing understanding of various surveillance capabilities and practices, such as the increasing ability to analyze information in near-real time as it is being collected.⁴

United States

The group discussed the legal frameworks for surveillance conducted by the United States, including Section 215 of the USA Patriot Act (covering bulk collection of metadata), Section 702 of the FISA Amendments Act (covering surveillance of people outside the US), and Executive Order 12333 (providing broad authority to conduct surveillance on people outside the US). Participants discussed the implications of Presidential Policy Directive 28 (which places limitations on the use of non-publicly available data collected in bulk and addresses the safeguarding of personal information collected through signals intelligence) and raised questions about how the directive will be applied.

Europe

Participants discussed relevant projects and processes in the Council of Europe, including the principles for surveillance programs developed by COE based on the European Convention on Human Rights.⁵ In addition, participants identified two areas to watch for new developments. First, it is anticipated that the Parliamentary Assembly will consider a resolution inviting the Secretary General to exercise his Convention powers and request information from member states regarding their surveillance practices and programs.⁶ Second, the Council of Europe may

³ See for example the case of *El-Masri v. the Former Yugoslav Republic of Macedonia*, available at <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-115621>.

⁴ A pilot project called Indect is one example of nearly real-time data analysis conducted for surveillance purposes: <http://www.indect-project.eu/>

⁵ See Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies, available at <https://wcd.coe.int/ViewDoc.jsp?id=2074317&Site=CM>.

⁶ See "Improving user protection and security in cyberspace" available at <http://www.assembly.coe.int/nw/xml/XRef/X2H-Xref-ViewPDF.asp?FileID=20560&lang=en>.

develop guidelines for member states regarding the rights to private life in the context of surveillance.

B. Gap Identification

In the second segment of the roundtable, the group discussed legal, theoretical, academic, and logistical gaps that make it difficult to understand the current landscape and chart a path forward. The following are among the gaps identified:

- There is a disconnect between the data protection community and the human rights community, as well as a disconnect between government officials who work in data protection and human rights and those who work in law enforcement and national security/intelligence.
- The law in a number of areas is not well developed. There needs to be more exploration of how the right to privacy applies in the context of surveillance. It was noted that the then-upcoming ICCPR review of the US by the Human Rights Committee⁷ offered an important opportunity, as did litigation in regional and international human rights courts.⁸
- There need to be more robust accountability mechanisms for the private sector, building on the Ruggie Principles and GNI Principles as a starting point.⁹
- The Human Rights Council has not yet squarely addressed the issue of cross-border surveillance.
- Transparency is crucial: It is difficult to determine what activities the law authorizes when the law or its interpretation is not public.
- It is important to learn more about the technical realities of surveillance programs and practices, including the role and capabilities of Internet and telecommunication companies.
- There needs to be more legal analysis and case law addressing whether surveillance is an exercise of authority or control for the purpose of jurisdiction.

⁷ A number of roundtable participants submitted comments in connection with the ICCPR review. In its concluding observations on the review, the Human Rights Committee was critical of both the US position on the jurisdictional scope of the ICCPR and the surveillance practices of the US. The civil society submissions and the concluding observations of the Human Rights Committee are available at http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=625&Lang=en.

⁸ For example, the Big Brother Watch case in the ECtHR offers an opportunity to establish the principle that a state can violate its human rights obligations not only directly but also by its complicity in the acts of other states.

⁹ The Ruggie Principles are available at http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. The Global Network Initiative Principles are at <http://www.globalnetworkinitiative.org/principles/index.php> and implementation guidelines are at <https://globalnetworkinitiative.org/implementationguidelines/index.php>.

C. Filling the Gaps and Identifying Opportunities

The group identified a significant number of short, medium, and long term opportunities for advocacy and thought leadership. This document highlights just a few of the opportunities discussed by the group.

Engaging Business

Throughout the roundtable, participants raised the importance of thinking further about the role of the private sector. They addressed both obligations of companies and also the importance of the private sector in government reform. Participants emphasized that business is deeply implicated in state surveillance practices, noting that there needs to be more work around the application of international treaty-based human rights standards to business and around self-regulatory frameworks for companies.

Leveraging United Nations Mechanisms

Participants agreed that it is important to take advantage of UN human rights bodies and processes in 2014 and beyond. Discussants raised the importance of the Human Rights Committee review of United States compliance with the ICCPR. They also talked about strategic contributions to the anticipated report from the High Commissioner for Human Rights on the right to privacy in the digital age, and the possibility of pushing the Human Rights Committee for a General Comment on privacy. In addition, discussants addressed the possibility of creating a UN Special Rapporteur on Privacy, and considered processes in Human Rights Council, including the upcoming Universal Periodic Review of the United States.¹⁰

Strategic Litigation

Participants agreed that strategic litigation is important for the further development of practice around human rights and surveillance, because it builds precedent upon which further actions can be based. Advocates and academics should support existing open cases and look for new litigation opportunities in the future. Several participants expressed interest writing an amicus brief for the case of Big Brother Watch and Others against the United Kingdom in the European Court of Human Rights.

Country-Specific Strategies

The group discussed unique circumstances and priorities in three countries: the United States, the UK, and Germany. In the United States, participants agreed that it will be challenging to persuade citizens and elected officials to advocate for the rights of people outside the United States and discussed strategies for linking domestic and international advocacy. Participants noted that in the UK, the government is examining the interplay between two human rights priorities: Internet freedom and the application of human rights standards to business. The discussion will serve as a “laboratory” for some of the issues raised globally around privacy and

¹⁰ The United Nations Human Rights Council is an inter-governmental body made up of 47 UN Member States that promotes and protects human rights and addresses human rights violations. The Human Rights Committee reviews the human rights records of Member States through the Universal Periodic Review process: <http://www.ohchr.org/EN/HRBodies/UPR/Pages/UPRmain.aspx>.

surveillance. Participants noted that Germany has the constitutional, economic, legal, and political infrastructure to be a test case for law on the right to confidentiality and integrity of IT systems, which could encompass surveillance practices. Some noted the importance of “leader” countries that can develop model laws for other countries to follow.

Thought Leadership & Analysis

In the course of discussion, participants mentioned several topic areas where it would be beneficial to have new analysis and thought leadership. First, it would be helpful to have better documentation of the legal and technical realities of surveillance in different countries, so that these programs may be compared to principles and best practices.¹¹ (CDT is developing a paper on the technical realities of surveillance in the US). Second, there is a need for scholarship and other thought leadership on the issue of privacy in the digital age that spans traditional academic disciplines, including human rights, traditional international law, and data protection. Finally, it is important to continue identifying and taking advantage of opportunities to build jurisprudence in human rights bodies around the right to privacy in the digital age.

To encourage continued discussion and collaboration on issues raised in the roundtable, CDT started a mailing list where participants can share ideas and coordinate advocacy efforts. CDT is also continuing to maintain and update a resources webpage¹² where participants can share their own work and other materials. Smaller discussions have continued offline between individuals with similar interests and groups with common advocacy goals.

For further information, contact CDT Policy Analyst Emily Barabas, ebarabas@cdt.org.

¹¹ Some research has already been published. See CDT’s paper Systematic Government Access to Personal Data: A Comparative Analysis, available at <https://www.cdt.org/systematic-access>. Charts comparing data from different countries are available at <http://govaccess.cdt.info/index.php>.

¹² The site is currently accessible only to roundtable participants and is available at <https://cdt.org/human-rights-roundtable>.