Supplementary Materials for Webinar #3

# Key Priority Issue: Privacy

## Global Guiding Principles and Frameworks

### 

### [GNI Global Principles on Freedom of Expression and Privacy](https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf)

The Global Principles on Freedom of Expression and Privacy have been developed by companies, investors, civil society organizations and academics who aim to protect and advance freedom of expression and privacy in the Information and Communications Technology (ICT) industry globally. The Principles are based on internationally recognized laws and standards for human rights and their application is informed by the UN Guiding Principles on Business and Human Rights. The Principles also include a set of [Implementation Guidelines](https://globalnetworkinitiative.org/implementation-guidelines/), aimed to provide further details on how participating companies will put the Principles into practice.

### [International Covenant on Civil and Political Rights](https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx)

The International Covenant on Civil and Political Rights (ICCPR) is a multilateral treaty adopted by the United Nations General Assembly. It commits it parties to respect the civil and political rights of individuals such as freedom of speech. Article 17 of the ICCPR emphasizes the right to privacy.

### 

### [UN Guiding Principles on Business and Human Rights](https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf)

The UN Guiding Principles on Business and Human Rights (UNGPs) is a framework that affirms that just as governments have a duty to protect human rights, companies also have a responsibility to respect human rights. The principles are grounded in the acknowledgement that the actions of transnational corporations and other business enterprises can significantly impact human rights. The UNGPs articulate the responsibilities of government and business actors with regards to business and human rights, and lays out operational principles for governments and businesses to meet these obligations.

### [Universal Declaration of Human Rights](http://www.un.org/en/universal-declaration-human-rights/)

The Universal Declaration of Human Rights (UDHR) outlines a set of human rights which are to be universally protected. The UDHR was proclaimed by the United Nations General Assembly in December 1948. Article 12 of the UDHR emphasizes the right to privacy.

## Regionally Specific Guiding Principles and Frameworks

### [American Convention on Human Rights](https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm)

The American Convention on Human Rights, also known as the Pact of San José, is an international human rights instrument that covers the Americas. Compliance with the Convention is overseen by the Inter-American Commission on Human Rights and the Inter-American Court of Human Rights, both of which stem from the Organization of American States (OAS). Article 11 of the Convention highlights the right to privacy.

### 

### [European Convention on Human Rights](https://www.echr.coe.int/Documents/Convention_ENG.pdf)

### 

The European Convention on Human Rights (ECHR) is an international treaty that aims to protect human rights and political freedoms in Europe. Compliance with the Convention is overseen by by the European Court of Human Rights. Article 8 of the Convention highlights privacy.

## Guides, Reports, and Toolkits

### [Applying the Guiding Principles on Business and Human Rights to the ICT Industry Briefing Paper, BSR](https://www.bsr.org/reports/BSR_Guiding_Principles_and_ICT_2.0.pdf)

### 

In June 2011, the United Nations Human Rights Council approved new Guiding Principles on Business and Human Rights. This decision represented a significant milestone in the history of business and human rights: More clarity exists today than ever before on government's’ duty to protect human rights and the business responsibility to respect human rights. In response, BSR published a report that highlights how companies, particularly those in the ICT industry, should apply the Guiding Principles to their business strategy and operations. In addition, this version of the briefing paper includes 10 lessons BSR learned while working to apply their strategies in practice.

### 

### [Corporate Accountability Index, Ranking Digital Rights](https://rankingdigitalrights.org/)

Ranking Digital Rights produces an annual [Corporate Accountability Index](https://rankingdigitalrights.org/index2018/) that evaluates 24 of the world’s most powerful internet, mobile, and telecommunications companies on their disclosed commitments and policies affecting freedom of expression and privacy. The Index provides concrete and measurable steps that internet, mobile, and telecommunications companies—as well as other companies throughout the sector—can take to improve how and what they disclose about policies and practices that impact digital rights, instead of having to come up with the answers on their own. The [Privacy category of the Index Methodology](https://rankingdigitalrights.org/2019-indicators/) seeks evidence that the company demonstrates concrete ways in which it respects the right to privacy of users. The company’s disclosed policies and practices should demonstrate how it works to avoid contributing to actions that may interfere with users’ privacy, except where such actions are lawful, proportionate and for a justifiable purpose. The company should also demonstrate a strong commitment to protect and defend users’ digital security, and clearly explain how they handle user information.

[Findings from the 2018 Corporate Accountability Index](https://rankingdigitalrights.org/index2018/report/privacy-failures/) show that companies don’t disclose enough about how they handle user information, which makes it difficult to assess the privacy, security, and human rights risks of using their services. In addition, the [2017 Investor Note](https://rankingdigitalrights.org/wp-content/uploads/2017/09/RDR_2017InvestorNote.pdf) and [2018 Investor Update](https://rankingdigitalrights.org/wp-content/uploads/2018/10/RDR_2018InvestorUpdate.pdf) both highlight the material risks in the ICT sector when companies fail to adequately assess the freedom of expression and privacy risks associated with their business practices.

### 

### [Getting Internet Companies To Do the Right Thing, New America’s Open Technology Institute](https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/)

For advocates seeking to protect privacy and security online, one of the most powerful levers for change is the internet industry itself. Getting internet companies to do the right thing when it comes to protecting their users can have a positive impact on millions or even billions of people. OTI explores how to push companies’ to do the right thing by developing case studies on three privacy and security practices:

* [Using Transit Encryption by Default](https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-1-using-transit-encryption-default/)
* [Offering Two-Factor Authentication](https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-2-offering-two-factor-authentication/)
* [Transparency Reporting](https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/)

### 

### [Privacy and Free Speech: It’s Good for Business Guide, ACLU of California](https://www.itsgoodfor.biz/)

Over the past few years, scandal after scandal has put tech companies under a microscope. Users, policymakers, and investors are demanding to know how companies are protecting privacy and free speech, and companies that fail to do so are being held accountable, by the government, by their users, and by their employees. This guide offers advice for companies wrestling with today’s most pressing challenges and includes sections on respecting user data, being transparent, partnering with users, and speaking up for free speech.

### 

### [The Digital Standard](https://www.thedigitalstandard.org/)

### 

The Digital Standard is a set of individual tests that taken together form a methodology for evaluating the privacy and security impacts of a given piece of software or hardware. It was created to define and reflect important consumer values that must be addressed in the development of software and hardware products. The Standard is underpinned by a set of guiding principles: electronics and software-based products should be secure, consumer information should be kept private, ownership rights of consumers should be maintained, and products should be designed to combat harassment and help protect freedom of expression. The Standard’s methodology is composed of 35 different “tests” that can be used to measure products to see how their design and policies meet best practices for digital privacy and security.

### 

### [Transparency Reporting Toolkit, New America’s Open Technology Institute](https://www.newamerica.org/oti/policy-papers/transparency-reporting-toolkit-reporting-guide-and-template/)

### 

The Transparency Reporting Toolkit focused on requests for user data to technology and telecommunications companies is a joint project by New America’s Open Technology Institute and Harvard University’s Berkman Klein Center for Internet & Society. The purpose of the Toolkit is to make it easier for companies to create better transparency reports about government requests for user data. Similarly, by providing a template and best practices, the Toolkit aims to make it easier for new companies to begin transparency reporting. By following the recommendations in this guide, which are grounded in existing best practices, transparency reports can become more consistent, easier to understand, and more effective.   
  
This edition of the Transparency Reporting Toolkit, published in 2016 includes the following:

* [Survey and Best Practices Memo:](https://static.newamerica.org/attachments/12935-the-transparency-reporting-toolkit/Transparency_Memo_Web.d0ecdb0e8c1a4dae9993e12ae61e5ef1.pdf) A survey of 43 transparency reports, identifying best practices across eight different areas.
* [Reporting Guide and Template for Reporting on U.S. Government Requests for User Information:](https://na-production.s3.amazonaws.com/documents/Transparency_Reporting_Guide_and_Template-Final.pdf) This guide provides a practical starting point for companies that want to create or improve their transparency reports, including a model transparency reporting template for companies designing their first report.

### 

### [Who Has Your Back, The Electronic Frontier Foundation](https://www.eff.org/who-has-your-back-2018)

EFF’s Who Has Your Back report aims to provide objective measurements for analyzing the policies and advocacy positions of major technology companies when it comes to handling data to the government. It focuses on a handful of specific, measurable criteria that can act as a vital stopgap against unfettered government access to user data. The latest EFF Who Has Your Back Report on government requests for user data assesses companies on the following criteria:

* Follows Industry-Wide Best Practices
* Tells Users About Government Data Requests
* Promises Not to Sell Out Users
* Stands Up to NSL Gag Orders
* Pro-User Public Policy: Reform 702

Six other organizations have used some version of EFF’s WHYB (government requests version) metrics to evaluate the practices of companies in their own countries, adapting the categories to local laws.

* Argentina - [Asociación por los Derechos Civiles](https://adcdigital.org.ar/qdtd/)
* Brazil - [Internet Lab](http://www.internetlab.org.br/en/projetos/quem-defende-seus-dados-who-has-your-back/)
* Chile - [Derechos Digitales](https://www.derechosdigitales.org/wp-content/uploads/qdtd-2017.pdf)
* Colombia - [Karisma Foundation](http://dondeestanmisdatos.info/2016/)
* Paraguay - [TEDIC](https://qdtd.tedic.org/)
* Spain and Latin America - [ETICAS Foundation](https://eticasfoundation.org/qdtd)

## Corporate Resources

Here are examples of Corporate Transparency Reports Related to Government Requests for User Data

### [Google](https://transparencyreport.google.com/user-data/overview?hl=en)

### [Facebook](https://transparency.facebook.com/government-data-requests)

### [Twitter](https://transparency.twitter.com/en/information-requests.html)

### [Apple](https://www.apple.com/legal/privacy/transparency/requests-2017-H2-en.pdf)

### [Microsoft](https://www.microsoft.com/en-us/corporate-responsibility/lerr)