MEMORANDUM

DIGITAL RIGHTS AND BUSINESS

A Primer on Risks and Solutions for the ICT Sector

PETER MICEK | SENIOR POLICY COUNSEL

JULY 2015

ACKNOWLEDGEMENT

The author would like to acknowledge the extensive support provided by Max Anderson, Anqi Li, Louise Rouse, and Matt Solomon in producing this paper.

Introduction

Google's Chief Legal Officer David Drummond has said, "Our business depends on the trust of our users." Drummond was directly responding to users threatened by the allegations of NSA spying on Google servers. But across the information and communications technology (ICT) sector, a lack of clarity around government access to user data has caused uncertainty and raised suspicions among investors, potential customers, and business partners.

The impacts are already being felt. Media and policy attention on dragnet government spying programs are causing legal, financial, and reputational harms to internet and telecom firms. For example, shareholders have sued IBM and Cisco for perceived complicity in government surveillance. The largest internet firms filed a lawsuit demanding the U.S. government allow more transparency on the extent of data actually being surveilled by intelligence agencies. The Information Technology & Innovation Foundation (ITIF) predicted in 2013 $21.5B to $35B losses for the cloud computing industry stemming from NSA surveillance revelations. ITIF published a follow-up report last month finding the cost to "far exceed" $35B, as the entire U.S. tech sector has underperformed due to U.S. surveillance. Furthermore, AT&T's attempt to expand in Europe was thwarted over EU policymakers' concerns, while Verizon lost a German government contract in 2014. Indeed, "American companies have reported declining sales overseas and lost business opportunities, especially as foreign companies turn claims of products that can protect users from NSA spying into a competitive advantage" according to a policy paper on Surveillance Costs by the Open Technology Institute (OTI) published last year.

While fighting to keep their surveillance infrastructure in place, many governments also increasingly seek to control how users express themselves online, and restrict how companies connect to customers across borders and networks. Governments require telecom operators to sign restrictive licenses and take actions that could adversely impact the human rights of users. Companies, and those that invest in them, need guidance to navigate licensing processes and law enforcement requests in order to avoid the civil and criminal liability, shareholder lawsuits, and falling stock prices that result when they are accused of contributing to rights violations.

Of course, not all privacy violations originate with government demands, as the 2013 extensive breach of Target's systems reveals. Network security is a shared responsibility of every company dealing with user data, and an area of renewed focus for regulators, privacy advocates, and shareholders.

ABOUT THIS MEMO

The mission of Access is to defend and extend the digital rights of users at risk around the world. As shown by our 2015 RightsCon Southeast Asia event, which drew more than 660 people, including 90 companies, tech firms from Asia-based startups to the Googles and Twitters of the world see the synergy between our mission to protect user interests, and their opportunities to grow and innovate.

This brief outlines the main challenges information and communications technology (ICT) providers face on freedom of expression and privacy issues. While certain companies are more exposed than others to risk, Access believes the challenges must be approached sector-wide. From better encryption, to engagement with outside stakeholders, the solutions we identify will prevent harm while delivering policies and services that users desire.

To be sure, internet and telecom firms must regain the trust of the public and technology users, who expect their private lives to remain so despite the increasing reach of internet services. We hope that, using the insights and solutions in this brief, financial professionals can help companies rebuild the trust and security that companies require to thrive, benefiting users and investors alike.

Sections I and II of this brief study free expression, access to information, and privacy, and note the companies most exposed to risks on these fronts. Section III presents sector- and company-specific responses and solutions.

1 Freedom of Expression, Access to Information, and Tech Investors

As protected by international law and nearly all national constitutions, the freedom of expression includes the right to seek, receive, and impart all types of information, in any form, subject only to narrow restrictions. While the rapid expansion of the ICT sector offers new opportunities for free expression and access to information, governments and complicit companies may impact users' exercise of these rights in new, often unforeseen ways.

ICT providers have contributed to violations through:
- Arbitrary restrictions on certain types of expression
- Blocking or filtering content
- System disruption or shutdown

Legal, reputational, and financial liabilities result when companies are perceived to actively participate in, or passively enable such violations – even when acting at the behest of governments. On a more basic level, these disruptions and blocking simply prevent customers from reaching the content and services they want. Unstable and insecure services do not deliver strong and sustainable financial returns.

Some companies exposed to these risks are:
- Tencent Holdings Limited and LinkedIn: Navigating China's internet rules
  - *Associated Press*: Chinese messaging service shuts politics accounts, reporting that the Chinese government forced WeChat, a service of TenCent Holdings, to shut down 40 accounts for political purposes.
  - See also *NY Times*: LinkedIn Goes to China, noting that LinkedIn will enforce some censorship through its new Chinese service.
- Telenor and Oredoo: Expanding into Myanmar's telecom greenfields
  - These two telcos won licenses to operate in Myanmar, a country whose government has previously shut down internet access nationwide.
  - OpenNet Initiative: Pulling the Plug: A Technical Review of the Internet Shutdown in Burma, analysis of the 2007 internet shutdown, where government sought to inhibit social mobilization during protests.
- Zain, Canar, MTN, and Sudatel: Vulnerable to Sudanese politics
  - Access: Mass internet shutdown in Sudan follows days of protest, blog post summarizing the September 2013 internet shutdown in Sudan.
- TeliaSonera, Vimpelcom, and Megafon: Unstable operations and deals in the CIS
  - *Chicago Tribune*: U.S. authorities probe TeliaSonera's Uzbek licence deal. The SEC is investigating TeliaSonera's corrupt deal for Uzbek 3G contract.
  - Renesys: Syria, Venezuela, Ukraine: Internet Under Fire, finding Armenia, Turkmenistan, and other nations vulnerable to internet disruptions because they lack robust connections to global internet.

"NET NEUTRALITY" AND FREE EXPRESSION

In the absence of regulation, those telecoms and internet service providers (ISPs) that own networks and internet infrastructure often charge competitors to access end users. This "pay-to-play" model discriminates against new market entrants, small and medium-sized enterprises, and those content providers trying to reach different markets.

To ensure that the internet remains a platform for free expression and disruptive market innovations, governments and ICT companies should respect the principle of "Net Neutrality." The guiding principle of the open and universal internet, Net Neutrality means that all traffic is treated on an equal basis, without discrimination, restriction, or interference regardless of its sender, recipient, type, or content. In addition to preserving the conditions that made the internet what it is today, Net Neutrality increases competition, and discourages price discrimination.

If Net Neutrality is enshrined in regulation, something that the European Parliament has previously voted for, the U.S. Federal Communications Commission (FCC) accomplished, and 16 countries globally have implemented, it would benefit certain sectors and companies including:
- **Skype**
  - *NY Times*: E.U. Lawmakers Approve Tough 'Net Neutrality' Rules, on the European Parliament's adoption of a Net Neutrality regulation.
- **Netflix**
  - *Christian Science Monitor*: Net neutrality: Is the Internet about to change? noting that Netflix recently had to cut a deal with Comcast when its streaming rates dipped 27%.
- **Startups**
  - Before the FCC ruling in the United States, venture capital firms warned they would stay away from media-heavy startups as these would in particular suffer the discrimination of a pay-to play model internet.

POLICY GUIDANCE

Through discussion with all stakeholders, including companies, investors, technologists, and activists, Access and our partners have produced guidance for companies to address their freedom of expression impacts.

This guidance includes:

- Access: Telco Action Plan – Respecting Human Rights: Ten Steps and Implementation Objectives for Telecommunications Companies, a guide for telcos to mitigate risk and avoid complicity in human rights violations.
- BSR: Protecting Human Rights in the Digital Age, identifying human rights risks along the ICT supply chain, including reference to specific companies.
- Access: Forgotten Pillar: The Telco Remedy Plan, providing guidance for telcos on how to redress human rights harms they've contributed to

Policy guidance only goes so far as its implementation, however. All stakeholders can play a role in promoting and measuring corporate progress toward more stable and dependable operations. See Section III below for some ways to get involved.

II The Right to Privacy, Government Surveillance, and Data Breaches

As enshrined in the International Covenant on Civil and Political Rights, every person has the right to freedom from arbitrary or unlawful interference with their privacy. At every juncture along the ICT service chain, there is the risk of unlawful and dangerous surveillance and sharing of communications content, records, and user-identifying data.

Some privacy risks that companies face include:

- Government surveillance of user activity and content
- Government access to user-identifying information
- Reputational, legal, and economic fallout from companies' over-collection of user data, poor data protection practices, and unlawful sharing of data
- Data breach from attacks on points-of-sale, stored data, and data in transit
- Unclear legal standards costs staff time and energy spent parsing requests, asking for clarification, and even weighing political considerations on whether to push back and possibly face retaliation for non-compliance

Most internet companies and telcos build their business models around user trust in the networks and entities that transmit and process their personal data. Unauthorized access or use of information by governments, as well as by private actors, fundamentally threatens this trust relationship.

Some companies exposed to privacy risks:

- **Microsoft**
  - *NY Times:* Revelations of N.S.A. Spying Cost U.S. Tech Companies, highlighting new expenses and deals lost by U.S. firms operating abroad.
  - See also *CNN*: How the NSA scandal hurts the economy, exploring how NSA revelations negatively impacted users' trust in U.S. internet firms in Europe.
- **IBM**
  - *Reuters*: Lawsuit accuses IBM of hiding China risks amid NSA spy scandal, describing how a large shareholder sued IBM for losses in China sales.
- **AT&T**
  - *Wall Street Journal*: NSA Fallout Thwarts AT&T, showing ramifications of U.S. government surveillance on proposed AT&T acquisition in Europe.
  - *Ars Technica*: AT&T's Cricket buy raises competition, pricing, and privacy questions. It compares AT&T privacy policies with Cricket's standards.
- **Cisco**
  - *Time*: Why Companies are Thinking Twice about Buying American, explaining why Cisco and other U.S. companies are suffering in international markets following revelations of government surveillance.
- **Target**
  - *NY Times*: For Target, the Breach Numbers Grow, reporting large data breach that affected up to 110 million consumers and impacted sales.
- **Facebook**
  - *The Times of India*: Privacy worries cloud Facebook's WhatsApp Deal, citing possible U.S. Federal Trade Commission (FTC) inquiry into Facebook's acquisition of WhatsApp.

The world's largest internet firms have banded together with a set of Global Reform Government Surveillance "Principles," which Access welcomed. Beyond reforming government policies, internet firms also have many options to better protect the personal data that is transmitted on their networks and stored on their servers. Access created "Data Protection – Why Care?", a factsheet on the need to protect personal data online, and recently enlisted companies in a new campaign to improve data security practices.

More initiatives and opportunities for companies to address their privacy challenges are outlined below.

III Industry Responses: Maximizing Transparency, Engagement, and User Trust

In many different sectors, from the extractives industry to internet governance, stakeholders from the private sector, government, and civil society join to craft frameworks and build international norms on business and human rights.

Often, these inclusive or "multi-stakeholder" bodies bring multinational corporations, industry groups, and human rights non-governmental organizations (NGOs) together to identify government and company best practices, offer country and sector-specific technological and policy support, and monitor compliance.

Access recommends technology companies join a **multi-stakeholder organization** like the Global Network Initiative (GNI) that carries out independent, expert human rights assessments. The ongoing engagement of these initiatives provides pragmatic guidance to companies on implementing rights protection frameworks. See Global Network Initiative: Implementation Guidelines for the Principles on Freedom of Expression and Privacy

In addition, ICT companies can take several steps to prevent risk and mitigate harms, including:

- **Encrypting** data and taking other steps in the Access Digital Security Action Plan. In particular, implementing strict encryption measures on all network traffic and executing verifiable practices to effectively secure user data stored at rest.
- Following best practice guidelines for **human rights due diligence** and responding to government requests in the Telco Action Plan.
- Issuing regular **transparency reports** about requests from governments for user data and content removal. These reports outline the scope and scale of government requests for user information, and how the requests were resolved. See Google Transparency Report; Twitter Transparency Report; AT&T Transparency Report; Verizon Transparency Report; Vodafone Law Enforcement Disclosure Report
- Assessing and publicly **reporting** on the human rights criteria being developed by the Ranking Digital Rights project.

In their human rights policies, mission statements, and ethics guidelines, companies should consult and refer to these frameworks on business and human rights, including:

- UN Guiding Principles on Business and Human Rights: the foremost framework for discussing the protection of human rights in business, establishing that companies have the duty to respect human rights and jointly remedy abuses.
- European Commission ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights: framework for the application of the UN Guiding Principles to the ICT sector.
- UN Global Compact Guidance on Responsible Business in Conflict-Affected and High-Risk Areas: A Resource for Companies and Investors: UN guidance for companies investing in situations where users are particularly at risk for human rights abuses.
- Telecommunications Industry Dialogue on Freedom of Expression and Privacy, "Guiding Principles": Commitments by the world's largest telcos to comply with international law related to freedom of expression and privacy.

Some companies have taken extraordinary steps to address their impacts on privacy and freedom of expression:

- Vodafone released a highly detailed transparency report, beginning in 2014, that examines surveillance law and policies in 29 countries in which it operates, as well as statistics for government requests it receives
- The Telecommunications Industry Dialogue has followed up with a legal annex of surveillance and interference laws in 44 countries.
- Google, Microsoft, and Yahoo recently completed their full assessments by the GNI.
  - See: Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo, finding that Google, Microsoft, and Yahoo are in compliance with the GNI Principles.
  - See also: Access analysis of Google, Microsoft, and Yahoo assessments.

Access is an international organization that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

FOR MORE INFORMATION

Please visit www.accessnow.org and contact:

Peter Micek | Senior Policy Counsel
peter@accessnow.org
+1-888-414-0100 x709