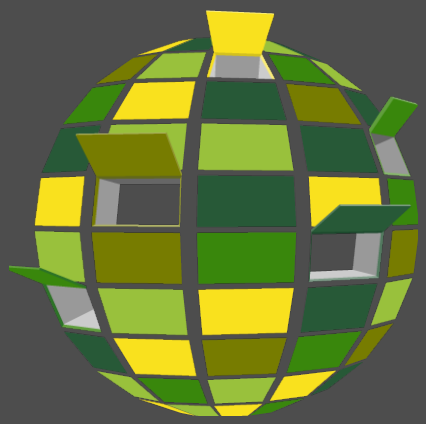


FREEDOM ONLINE COALITION

NOVEMBER 2015

WORKING GROUP 3

Privacy and Transparency Online

REPORT

WORKING GROUP 3
Privacy and Transparency Online

freedomonlinecoalition.com

Working Group 3 “Privacy and Transparency Online”

The Freedom Online Coalition is a group of governments who have committed to work together to support Internet freedom and protect fundamental human rights – free expression, association, assembly, and privacy online – worldwide.

The Freedom Online Coalition Working Groups were established to explore in more detail important policy issues facing online freedom and to inform the work of the Coalition and its members. Working Group 3 focuses on the relationship between governments and information & communications technology (ICT) companies, with a particular emphasis on respecting human rights online, including freedom of expression and privacy.

Co-chairs of Working Group 3

Katharine Kendrick, NYU Stern Center for Business and Human Rights
Stephen Lowe, UK Government

Selected Members of Working Group 3 2014-15

Alexandrine Pirlot de Corbion, Angela Daly, Ben Blink, Bouziane Zaid, David Sullivan, Eduardo Bertoni, Emma Llanso, Kevin Bankston, Lucy Purdon, Meg Roggensack, Monroe Price, Poncelet Ileleji, Rebecca MacKinnon and Stefan Heumann.

Country Members of Working Group 3

Germany, Sweden, United Kingdom and United States of America

We would also like to thank Gianna Lohnn, Simon Harari, Leanne O’Donnell and Liz Woolery for their contributions to this report.

This paper is the product of our multi-stakeholder working group, and not an official document of the Freedom Online Coalition. The report does not reflect the official views of FOC member governments (including those represented in this group).

Freedom Online Coalition Support Unit

Global Partners Digital
Development House
56–64 Leonard Street
London
EC2A 4LT
+44 (0)207549 0337
info@freedomonlinecoalition.com

TABLE OF CONTENTS

01

EXECUTIVE SUMMARY

This report reflects the work of the Freedom Online Coalition's Working Group 3 "Privacy and Transparency Online", carried out between August 2014 and May 2015. The Freedom Online Coalition (FOC) is a partnership of 28 governments, working to advance Internet freedom – free expression, association, assembly, and privacy online – worldwide.

The Privacy and Transparency Working Group focuses on protecting and respecting human rights in the relationship between governments and information & communications technology (ICT) companies.

The Working Group is comprised of experts from governments, ICT companies, civil society and academia from across five continents. The Group was established as a multi-stakeholder forum under the auspices of the FOC and aims to support member governments' implementation of the 2014 Tallinn Agenda for Freedom Online, which emphasizes the importance of enhancing transparency and protecting privacy as part of a commitment to Internet freedom. We aim not only to provide operational guidance to FOC government members and stakeholders, but also to contribute to the global discussion on transparency and accountability with respect to the relationship between governments and ICT companies.

This report is the product of the first year of the Working Group's work. It focuses on transparency about government requests to ICT companies to disclose user information or restrict user content accessed through company platforms. We specifically address how governments and companies manage requests related to law enforcement and national security, and what each party does or does not disclose to the public about these interactions.

The Tallinn Agenda for Freedom Online included the following recommendations, by which the FOC member governments:

> Dedicate [themselves] to respect … human rights obligations as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency, and call upon others to do the same;
>
> Call upon governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance, use of content take-down notices, limitations or restrictions on online content or user access and other similar measures, while committing ourselves to do the same.

The Group's work builds on these recommendations. We also build on the growing recognition of the role of the private sector in respecting and realizing human

rights. The Tallinn Agenda emphasizes "the importance and responsibilities of the private sector as a stakeholder in respecting human rights and fundamental freedoms online in the age of data-driven economies." We draw on the UN Guiding Principles on Business and Human Rights, as well as principles and operational guidance specific to ICT companies established by the Global Network Initiative (GNI), a multi-stakeholder organization committed to protecting and advancing free expression and privacy in the ICT sector.

Every day governments make requests to companies for user information or content restriction as a legitimate part of criminal investigations or intelligence operations. However, because this process involves a company providing a person's information to the government, or restricting the availability of information at the government's behest, these requests can also pose risks for human rights.

Transparency enables governments and companies to demonstrate that they are protecting and respecting human rights in the processing of government requests. It empowers other stakeholders to hold each party accountable to commitments like the Tallinn Agenda and ensure their behavior is in line with international human rights norms. Transparency reinforces privacy by fostering public debate on whether government requests are being made within frameworks that reasonably consider individual privacy together with national security and law enforcement interests. It also enables freedom of expression, providing access to information and mitigating the chilling effect that can accompany concerns about government surveillance.

It is for this reason that the Group focused this initial study on transparency about government requests to companies. At the same time, the Group recognizes there are legitimate reasons to withhold information from the public for law enforcement and intelligence purposes. Part of our motivation was to understand and articulate how to maximize accountability and transparency while enabling governments to carry out legitimate national security and law enforcement functions, which are also essential to the protection of human rights.

This paper is the product of our multi-stakeholder working group, and not an official document of the Freedom Online Coalition. The report does not reflect the official views of FOC member governments (including those represented in the group).

OUR APPROACH

The Working Group developed a series of discussion prompts to consult with representatives of governments and companies regarding their privacy and transparency practices connected to government requests to companies in national security and law enforcement contexts. The consultations were conducted in accordance with the Chatham House Rule, where the identity of those responding is not revealed in the report, beyond whether the respondent was from a government or company.

Our consultation framework consisted of two parts: the first on government access to user information, and the second on content restriction. In each section, we posed a series of questions inquiring into the current state of affairs, challenges to transparency, and opportunities for improvement. Our aim was to provide insights not only into the current state of transparency by governments and companies, but also into the considerations that both parties take into account when developing transparency policies and practices.

The governments and companies we interviewed varied both in type and in scope of transparency-related activities. We focused on FOC member governments and ICT companies with transnational reach. We consulted 7 governments and 8 companies, with multiple representatives from each:

- *Governments:* Australia, Estonia, Mongolia, the Netherlands, Sweden, United Kingdom, United States
- *Companies:* Cloudflare, Facebook, Google, LinkedIn, Mozilla, Orange, TeliaSonera, Vodafone

Working Group members raised the following topics with governments and companies:

- General understanding of the overall context as well as the specific laws, policies and processes that govern the relationship between ICT companies and governments;
- How governments make requests to companies for user information or for the restriction of content;
- How companies receive, process, and respond to government requests for user information or content restriction;
- The implications of these practices for individuals' privacy and freedom of expression, as well as broader considerations related to law enforcement and national security;
- Opportunities for, and challenges to, greater transparency, including law enforcement, national security, and other considerations.

INTERVIEW FINDINGS

A number of overarching themes emerged from our consultations:

- *Growing public expectations of government and corporate transparency* – Governments and companies are pioneering new measures to be transparent about matters that affect Internet users' rights, and acknowledge pressure to do more.
- *Moving beyond numbers* – Governments and companies can complement quantitative transparency (the disclosure of statistics on requests made or received) by better explaining the qualitative context for these requests. This might include explanations of internal processes, explanations of the legal and policy context, and illustrative examples of requests.
- *Providing the full picture* – Meaningful transparency requires greater reporting by governments, as well as consistency among companies and governments on how they report on numbers, policies and practices.
- *The effect of ambiguity* – Transparency suffers in the absence of clear laws, policies, and processes as companies and governments err on the side of non-disclosure.

We outline some key findings here, under the headings of state of play, challenges and opportunities.

STATE OF PLAY

Government and company representatives cited common motivations for being transparent about government requests, and use a range of methods to provide this transparency.

Motivations

Transparency is Part of the Institution's Philosophy

Both government and company representatives identified transparency as a normative value for their institution. Some government officials emphasized that transparency as a tool for government accountability was a core value in their country, reflected either in its legal foundations or by current leadership. Some

company representatives also viewed being transparent as part of the company's philosophy or starting premise.

Transparency Builds Trust

Government officials noted that transparency is essential to ensuring public trust in law enforcement and national security activities. Company representatives said that disclosing the scale and scope of government requests helps build trust with their users, which is essential for business.

Transparency is Increasingly Expected

Both government and company representatives recognized increasing public demand for transparency. They acknowledged that the global focus on government surveillance in the last few years has raised public expectations, and that failures to be transparent were noticed.

Methods

Transparency reports – Companies and governments publish "transparency reports," commonly understood to refer to regular statistical reporting on the number of requests made or received in a given period.

Principles – Some governments and companies publish high-level principles articulating broad commitments that inform their decisions related to government requests.

Guidelines – Guidelines published by governments and companies provide insight into how requests are handled on an operational level, complementing the commitments outlined in principles.

Public education tools – Some governments and companies use dedicated websites and blogs to provide context on policies and practices for a broader audience, and to describe any policy changes.

Performance reviews and assessments – Some governments and companies publish reviews and assessments of their performance related to requests. These may be reviews of the suitability of specific government or company policies, or may evaluate how the government or company has implemented a policy in practice, including if and how they have veered from stated commitments.

CHALLENGES

Government and company representatives see various legal, policy, and operational challenges to providing greater transparency about government requests for user information and content restriction.

Legal Challenges

Prohibitions on publication – Government prohibitions against publication of certain information or classes of information was identified by company representatives as a main difficulty.

Legal ambiguity – Legal ambiguity has hindered transparency in practice, as companies and governments interpret opaque laws about what is allowed by erring on the side of non-disclosure.

Differing jurisdictions – Companies with transnational operations face challenges understanding and complying with different countries' local laws, particularly when it comes to content restriction.

Indirect, informal, and extra-legal cooperation – Government-company interactions beyond those clearly defined in law lack transparency. These include arrangements such as self-regulatory and co-regulatory schemes for content restriction, and governments' use of companies' Terms of Service enforcement mechanisms.

Policy Challenges

Compromising government operations – Government officials voiced concern that transparency would compromise law enforcement or intelligence operations, by revealing the government's capabilities in different ways.

Affecting government-company relations – Company officials were concerned that their disclosure of information about government requests could provoke negative reactions from governments, ranging from temporary discomfort to real risks to employees.

Divergent internal attitudes – Representatives from both companies and governments noted divergent attitudes towards transparency within their own institutions. They emphasized the importance of high-level support and commitment to overcome disagreements.

Remedies – Both government and company representatives encountered challenges when talking about mechanisms for remedy: what recourse, if any, is available to an individual when their information is inappropriately released or restricted.

Operational Challenges

Capacity limitations – Both governments and companies identified capacity limitations as a challenge, with limited resources being in some cases the primary reason they had not done more to be transparent.

Designing internal systems – Designing effective internal methods for tracking and reporting requests was challenging, particularly as the number and scope of requests expands.

Communicating effectively – As interest in transparency grows, both government and company representatives reported challenges identifying and communicating well with an increasingly diverse audience.

OPPORTUNITIES

Government and company representatives identified opportunities – legal, policy, and operational – to increase transparency. While some opportunities were specific to individual consultees, both parties frequently raised the value of cooperation among governments or companies, as well as with other stakeholders. Representatives also explained how being transparent would further larger goals for their institutions, including improving internal coordination and building trust between one another and with external stakeholders.

Legal Opportunities

Legal reform – Multiple governments whose officials we consulted were in the process of reviewing policies and laws relevant to transparency and government requests to companies.

Encouraging change from the outside – Company representatives identified opportunities to encourage legal change, such as challenging government requests

in court and pushing for the ability to disclose more information on requests received.

Clarifying legal frameworks – Company representatives mentioned working with governments to clarify the application of a law, and to narrow a request so as to address the government's need while limiting a request's effect on users.

Policy Opportunities

Enhancing government transparency reporting – Both stakeholders identified opportunities for governments to disclose more information on the requests they make to companies.

Working together – All consultees identified room for improvement in their individual practices and pointed to the value of collaboration, both within their stakeholder groups as well as among governments and companies.

Public education – Government and companies saw opportunities for broader education of the public, noting that being transparent requires not just disclosure of information, but also equipping the audience with the framework to understand it.

Operational Opportunities

Internal education – Company and government representatives acknowledged that the process of compiling a transparency report or related materials helps educate people internally about what different parts of their institutions are doing and the broader implications of their actions.

Consistency – Government and company representatives identified opportunities for greater consistency around the processing and reporting of government requests, both internally and across their stakeholder groups.

RECOMMENDATIONS

The following recommendations are based on our consultations and informed by the collective expertise of the Working Group. They complement existing and emerging principles and best practices in the field, as outlined in the full report. The recommendations are specific to law enforcement and intelligence contexts, the focus of our research.

For governments

Establish clear policies and processes for making requests to companies and reporting on them to the public

Consistent with the Tallinn Agenda, government requests to companies for user information and content restriction must respect human rights obligations and be consistent with the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency.

Work together, and with all other stakeholders, to develop best practices for government transparency about requests made to companies

As governments try new approaches to transparency, they should work together and with all other stakeholders including civil society, the technical community, investors and academic experts on standards and best practices for public disclosure of requests made to companies for law enforcement and intelligence purposes.

Expand the scope of government reporting on requests to companies

No government has produced a comprehensive report on requests made to companies for user information and content restriction over a specific time period. Comprehensive reports would give citizens a more complete picture of how their governments are using their authority to access personal information or to restrict content. FOC governments are in a good position to consider what such a report would entail, including the kinds of internal coordination mechanisms that would be necessary to compile reports and how best to present them to the public.

Strengthen qualitative transparency about laws, policies, and processes

To complement increased quantitative reporting, governments should provide information to the public about laws, policies, or legal authorities that are employed to make requests. It is also important to disclose which parts of government are involved, and which have clear legal authority to request user information and content restriction. Where governments are already taking steps to be transparent – as through statistical reports, or policy reviews -- they should pursue ways to make this information more accessible.

Make a high-level commitment to transparency, and commit resources accordingly

Governments should make a high-level, public commitment to increasing transparency about requests made to companies. They should reflect this commitment by dedicating employee time and allocating a sufficient budget for reporting processes and other measures to inform citizens. They should develop mechanisms for coordinated record-keeping across government agencies that make requests of companies for user information and content restriction, and for keeping this information updated within a reasonable time period.

For companies

Establish clear policies and procedures to receive, process, and report on government requests for user information and content restriction

Companies can learn from each other and other stakeholders to implement responsible systems around government requests.

Strengthen qualitative transparency about company policies and processes

While companies should publish to the extent legally possible the numbers of requests they receive and comply with, they should also regularly publish information that clarifies their policies and procedures for responding to government requests.

Work together, and with all other stakeholders, to standardize transparency reporting

Companies should work with each other and with civil society, academics, investors, and the technical community to develop industry-wide standards for reports and other measures to boost sector-wide transparency about government requests. Currently, reports differ so widely in their scope and approach that it is difficult to carry out the type of comparative analyses that would facilitate policy recommendations.

Expand the scope of current reporting

Companies have focused mostly on transparency about government requests for

access to user information. Recognizing the freedom of expression implications, companies should be more transparent about government requests for content restriction, disclosing both the nature and number of requests as well as how the company handles them.

Make an executive-level commitment and commit resources accordingly

Companies should make an executive-level commitment to transparency and educate all parts of the company on how and why to be transparent around government requests for user information or content restriction. Companies should reflect their commitment by dedicating employee time and allocating a sufficient budget for regular, timely reporting and other measures to inform users.

AREAS FOR FURTHER RESEARCH

Through our consultations we identified the following areas for future work on transparency for both the Working Group and other stakeholders.

- Processes for government transparency
- Qualitative transparency for companies and governments
- Transparency about content restriction
- Cooperation through indirect, informal, and extra-legal channels
- Developing remedy

FUTURE ACTIVITY FOR THE WORKING GROUP

At the FOC conference in Mongolia in May 2015, the Working Group's mandate was renewed by FOC member governments. Our new mandate extends to the next FOC conference in 2016. The Group has identified two areas of focus out of the topics above. Building on the work reflected in this report, the Group will focus on 1) models and best practices for government transparency reporting on requests made to companies, and 2) best practices for qualitative transparency – how governments and companies can provide transparency about laws, policies, and processes related to government requests to companies.

The public debate on transparency has focused mainly on the relationships and practices among U.S. and European companies and governments. In our future work, we are committed to including the range of perspectives from companies, civil society and governments around the world necessary to advance global best practices. Likewise, we are interested in exploring areas of government-company interaction beyond the national security and law enforcement context.

We welcome collaboration with any initiatives or individuals working in these areas. To contact the Group, please email info@freedomonlinecoalition.com

02
INTRODUCTION

This report represents the work of the Freedom Online Coalition's Working Group 3, "Privacy and Transparency Online," carried out between August 2014 and May 2015. The Freedom Online Coalition (FOC) is a partnership of 28 governments working to advance Internet freedom – free expression, association, assembly, and privacy online – worldwide.

The Privacy and Transparency Working Group focuses on protecting and respecting human rights in the relationship between governments and information & communications technology (ICT) companies.

The Working Group is comprised of experts from governments, ICT companies, civil society and academia from across five continents. The Group was established as a multi-stakeholder forum under the auspices of the FOC and aims to support member governments' implementation of the 2014 Tallinn Agenda for Freedom Online, which emphasizes the importance of enhancing transparency and protecting privacy as part of a commitment to Internet freedom. We aim not only to provide operational guidance to FOC members and stakeholders, but also to contribute to the global discussion on transparency and accountability with respect to the relationship between governments and ICT companies.

This report is the result of the first year of the Working Group's work. It focuses on transparency about government requests to ICT companies to disclose user information or restrict user content accessed through company platforms. We specifically focus on how governments and companies interact in situations related to law enforcement and national security.

The report is based on consultations with companies and governments regarding their privacy and transparency practices with regard to government requests. The Group looked at how governments make requests to ICT companies for law enforcement or intelligence purposes, and how they release information about these requests to the public. The Group also looked at how companies respond to those requests and how they publicly share information about the process, number, and nature of requests they receive.

Every day, governments around the world make requests to companies for user information or content restriction. A government official might request that a company share information on the identity of the user behind a given email account, if that individual under investigation is suspected to be involved in criminal or terrorist activity. An official might request that a company filter or remove illegal content that is accessible through that company's platform. These requests arise constantly in law enforcement and national security contexts, as governments seek information for use in criminal investigations or intelligence operations.

However, because these requests involve a company providing a person's information to the government, or restricting the availability of information at the government's behest, these requests can also pose risks for human rights. For example, government officials may request information about an individual user not because they are investigating a crime but because the person has criticized that government. Officials may also pursue content removal through a direct request to the company hosting that information, without complying with that government's adjudicatory processes. Due to this potential for direct government requests to companies to circumvent due process protections, it is essential that both governments and companies provide information to the public about these interactions. Without such transparency, it is difficult for members of the public to determine whether government requests are appropriate and in accordance with the law, or whether companies are respecting the human rights of their users when responding.

It is for this reason that the Group focused this initial study on transparency about government requests to companies. At the same time, we recognize there are legitimate reasons to withhold information from the public for law enforcement and intelligence purposes. Part of our motivation was to understand and articulate how to maximize accountability and transparency while enabling governments to carry out legitimate national security and law enforcement functions, which are also essential for the protection of human rights.

This paper is the product of our multi-stakeholder working group, and not an official document of the Freedom Online Coalition. The report does not reflect the official views of FOC member governments (including those represented in this group).

THE FOUNDATION FOR OUR WORK

Our work is grounded in the recommendations of the Tallinn Agenda for Freedom Online, adopted by FOC member states in April 2014. The preamble to the Tallinn Agenda "recognis[ed] transparency of government processes and open government data initiatives as important elements in protecting human rights and fundamental freedoms, and participation in a democratic society." The Tallinn Agenda included the following recommendations, by which the FOC member governments:

> Dedicate ourselves, in conducting our own activities, to respect our human rights obligations as well as the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency, and call upon others to do the same;
>
> Call upon governments worldwide to promote transparency and independent, effective domestic oversight related to electronic surveillance, use of content take-down notices, limitations or restrictions on online content or user access and other similar measures, while committing ourselves to do the same.

The Tallinn Agenda also called on other stakeholders – non-member governments, the private sector, international organizations and civil society worldwide – "to endorse these recommendations to guarantee a free and secure internet for all."

The Group's work also builds on growing recognition of the role of the private sector in respecting and realizing human rights. The Tallinn Agenda emphasizes "the importance and responsibilities of the private sector as a stakeholder in respecting human rights and fundamental freedoms online in the age of data-

driven economies." The UN Guiding Principles on Business and Human Rights adopted in 2011 set forth the "Protect, Respect, and Remedy Framework," which established that governments have a duty to protect human rights, that companies have a responsibility to respect human rights, and that rights and obligations should be matched to appropriate and effective remedies when breached. We also draw on principles and operational guidance specific to ICT companies established in 2008 by the Global Network Initiative (GNI), a multi-stakeholder organization committed to protecting and advancing free expression and privacy in the ICT sector.

For the purpose of this report, we understand transparency to mean public reporting by governments and companies on their policies, processes, and statistics vis-à-vis government requests to companies for user information or content restriction. Our understanding of privacy is grounded in Article 17 of the International Covenant on Civil and Political Rights, which establishes that individuals have the right to protection of the law against arbitrary or unlawful interference with their privacy. In the context of this report, we understand privacy to refer to the extent to which individuals' personal information is protected against the arbitrary or unlawful disclosure by companies to government entities, including law enforcement and intelligence agencies. We also address requests from governments for content restriction, as these efforts can suppress an individual's speech and limit others' access to information, and can thereby infringe upon individuals' freedom of expression.

We see a positive relationship between promoting transparency and protecting privacy. The Tallinn Agenda principles outlined above – such as the rule of law, collection for a legitimate purpose, non-arbitrariness, and effective oversight – are critical to protecting individuals' privacy. They are essential to ensuring that invasions of privacy only occur within frameworks that reasonably consider individual privacy together with national security and law enforcement interests. Transparency reinforces privacy by fostering public debate on whether this objective is attained, in policy and in practice. It also enables freedom of expression, providing access to information and mitigating the chilling effect that can accompany concerns about government surveillance.

Transparency is a cornerstone of democratic governance and corporate best practice on respecting human rights. It enables FOC member governments to demonstrate that they are upholding key principles from the Tallinn Agenda for Freedom Online. Similarly, transparency allows companies to demonstrate their commitment to respecting human rights in how they handle the personal information of their users.

With transparency, individuals can understand how communications surveillance and other laws are used in practice, and how companies consider the human rights of their users when responding to government requests. Transparency provides oversight, as knowledge of government and corporate practice empowers civil society, investors, and other stakeholders to hold each party accountable to the commitments they have made and ensure their behavior is in line with international human rights norms.

OUR APPROACH

The Working Group developed a series of discussion prompts (included in the Appendix) to consult with government and company representatives regarding their privacy and transparency practices connected to government requests in national security and law enforcement contexts. The consultations were conducted in accordance with the Chatham House Rule, where the identity of those responding is not revealed in this report, beyond whether the respondent was from a government or company. These terms enabled those we consulted to be as frank as possible about perceived challenges to greater transparency as well as opportunities for improvement – through legal, policy, and operational changes.

Our consultation framework consisted of two parts: the first on access to user information; and the second on content restriction. In each section, we posed a series of questions inquiring into the current state of affairs, challenges to transparency, and opportunities for improvement. Our aim was to provide insights not only into the current state of transparency by governments and companies, but also into the considerations that both parties take into account when developing transparency policies and practices.

We sought to provide clarity on the following issues regarding government requests to companies for user information and content removal/filtering:

- General understanding of the overall legal context as well as the specific laws, policies, and processes that govern the relationship between ICT companies and governments;
- How governments make requests to companies for user information or content restriction;
- How companies receive, process, and respond to government requests for user information or content restriction;
- The implications of these practices for the privacy and freedom of expression of individuals, as well as broader considerations related to law enforcement and national security;
- Opportunities for, and challenges to, greater transparency, including legitimate law enforcement, national security, and other considerations.

We defined the Group's scope in the following ways:

- *Government-company interactions* – The mandate of this Group is to examine the human rights implications that arise through the interaction between governments and ICT companies. Our consultations did not address corporate or government transparency in other areas (e.g., use of customer data for commercial purposes; e-government transparency initiatives).
- *Law enforcement and national security* – Our research covered policies and practices around government requests to companies relevant to law enforcement or intelligence operations. Specifically, we looked at government requests to ICT companies for information on a customer suspected to be part of a criminal activity, and/or filtering or removal of content that the government deems illegal.
- *Policies, processes, and statistics* – Our research covered multiple tactics to be transparent about numbers of requests (quantitative transparency) and the contexts in which they are made and received (qualitative transparency). These tactics include transparency reports (defined below), principles and guidelines, public education tools, and policy reviews and assessments.

We consulted representatives from 7 companies and 8 governments that varied in structure (business model, government system), in geography, and in levels of experience with transparency policies and practices. Our consultations often involved multiple representatives from a given institution. We provide a list of companies and governments consulted under the Methodology section of this report.

THE CONTEXT FOR OUR WORK

The Working Group is operating in the context of dynamic and ongoing efforts, including the development of principles, guidelines and related assessment of the international and domestic legal issues and implications of government and company practices. This Group wishes to recognize other organizations and

initiatives working on transparency in this area, including Access, the Internet and Jurisdiction Project, Ranking Digital Rights, New America Foundation's Open Technology Institute, and others. Among organizations cataloguing such efforts, see the website of the Business and Human Rights Resource Centre.

We see our group's work as complementary to those efforts: our thinking is shaped by their work, and we hope that our analysis will in turn help inform these initiatives. We have included our discussion prompts used in consultations in the appendix, should they be useful for others to structure conversations on transparency with governments and companies. Likewise, our report and recommendations draw on principles and practices developed or endorsed by other organizations.

Over the last few years, companies and governments have taken unprecedented steps to increase transparency about practices that can affect individual privacy and free expression. At the same time, both parties as well as civil society groups, investors, and academics have identified critical areas for improvement. In this paper, we provide some examples of current approaches, and include further analysis in the Appendix.

Much of the transparency debate in the ICT sector has focused on company practices, particularly the publication of "transparency reports." Company transparency reports detail on a regular basis the volume and type of requests issued to them by governments – most commonly, requests to disclose user information or block and/or remove content. Since Google first published its transparency report in 2010, 62 other companies have followed suit.

To date, the majority of these reports have covered government requests for user information but not for content restriction. Most of these transparency reports are also quantitative in focus, reporting primarily the numbers of requests received. More recently, companies have strengthened the qualitative context in their reports, describing not only numbers of requests but also the legal and policy framework in which the company operates. Vodafone's 2014 Law Enforcement Disclosure Report was considered by some to be pioneering for including an annex with information on relevant laws in 29 countries in which the company operates. In June 2015 the Telecommunications Industry Dialogue, a group of nine telecommunications companies, published an online resource of legal frameworks in 44 countries where authorities seek access to user's communications or to restrict content.

We provide an appendix with an analysis of the scope of company transparency reports published to date.

In the last few years, there has also been growing public interest in government transparency about requests to companies for user information or content restriction. To our knowledge the Tallinn Agenda on Freedom Online is the most specific commitment by a group of governments addressing transparency in this context. No state publishes an overarching transparency report akin to those that some companies provide. At a national level, some states have disclosed information on requests for years in the context of government oversight, such as mandated reporting by a law enforcement agency to the organ of state such as Parliament that authorizes their activities. More recently, some states have pioneered practices aimed at a general audience. In 2013, the U.S. government established IContheRecord, a website intended to be a clearing house for information related to foreign surveillance activities, such as statistical and policy reports, public remarks, and declassified court opinions. A section of the website is dedicated to transparency, including about government requests to companies.

We provide an appendix with examples of reporting by governments whose representatives we consulted. The Group intends to expand this analysis in the coming year.

Civil society groups have pushed for both increased company reporting and greater government transparency. In March 2015, 46 civil society groups issued a Joint Statement from Civil Society to Technology Companies for Expanded Transparency Reports, commending companies already issuing transparency reports and calling on others to do the same. The letter recommends that companies follow certain best practices, such as categorizing types of requests, citing the legal justification and requesting government authority, and standardizing the management of government requests across countries. Investors have also played an important role in pushing companies to be more transparent.

Some civil society initiatives have also emerged to fill government reporting gaps. In 2013, The Estonian Institute for Digital Rights launched Project 451, in which it collected data from government agencies about requests to companies for content restriction, and published the resulting numbers as well as a description of relevant laws. In Poland, the NGO Panoptykon issued an "internet transparency report" by surveying four Polish internet service providers and compiling the numbers of requests for user information they had received. In Sweden, the thinktank FORES has issued what it calls a "reverse transparency report" by requesting information from 339 Swedish authorities on requests made to companies, and publishing the numbers as well as which authorities did not reply. In East Asia, the Hong Kong Transparency Report and Korea Internet Transparency Report have shed light on their governments' requests to companies by compiling already available information and working with government officials to disclose more. A similar project has started in Taiwan.

While the global debate on transparency has largely focused on companies and governments from North America and Europe, groups in other regions are leading groundbreaking efforts to advocate greater transparency. In addition to the civil society initiatives in East Asia mentioned above, companies such as Daum Kakao, which owns the South Korean messaging application Kakao Talk, have also begun publishing transparency reports. This Group benefited from insights from the government of Mongolia, and we are keen to engage with more governments outside of the North America and Europe. Given the diverse jurisdictions in which companies and governments are interacting, advancing best practices in transparency must include a broader range of regional perspectives.

Transparency reports have been the leading method of ensuring more public knowledge about user information and content restriction requests, but they are not the only way for governments and companies to be more transparent. Our paper attempts to go beyond reports. We include measures such as guidelines, public education tools and policy assessments within the transparency sphere. These other methods may appeal to different audiences and together provide more of a holistic view of how companies and governments are operating.

THIS REPORT

This report showcases our consultation process with governments and companies. The methods we used to undertake this consultation process are detailed in the next section (Part 3). We then present the findings from our consultation process (Part 4), followed by recommendations for improvements in transparency by both governments and companies (Part 5). Then, we detail what we see as avenues for future work, by this Working Group and by others (Part 6). Finally, in the Appendices, we provide examples of current corporate and government transparency reporting, as well as the full list of discussion prompts we used to consult governments and companies for this report

03

METHODOLOGY

The Working Group's work comprised three phases:

- *Phase One:* Establishing the framework (October – December 2014)
- *Phase Two:* Consultations and initial findings (January 2015 – mid-March 2015)
- *Phase Three:* Development and submission of recommendations (Mid-March – May 2015)

Members of the Working Group developed a framework of questions and discussion prompts to facilitate consultations with governments and companies regarding their privacy and transparency practices. In particular, the framework sought to explore how governments issue, and companies handle, requests for user information and content restriction in law enforcement and intelligence contexts.

In early 2015, Working Group members conducted consultations with representatives from governments and companies from the departments and sections responsible for making and handling these requests.

Consultations were carried out in accordance with the Chatham House Rule, that the identity of those giving certain responses would not be revealed in this report, beyond the fact of whether the respondent was from a government or company. In some cases where a specific practice is publicly available, we have cited companies or governments by name.

The consultation framework for governments and companies differed to reflect their roles but covered the same substantive areas. Consultations consisted of two parts: the first part comprising questions related to the access to user information; and the second part comprising questions related to content restriction. In each part, questions were posed around the themes of transparency, oversight, and remedy. We inquired into the current state of affairs for each theme, challenges to transparency, and opportunities for improvement.

The governments and companies we interviewed varied in type and scope of transparency-related policies and practices. We focused on FOC member governments and ICT companies with transnational reach. We interviewed seven governments and eight companies, often with multiple representatives from each:

- *Governments:* Australia, Estonia, Mongolia, the Netherlands, Sweden, United Kingdom, United States
- *Companies:* Cloudflare, Facebook, Google, LinkedIn, Mozilla, Orange, TeliaSonera, Vodafone

Working Group members raised the following topics with governments and companies, with the scope ranging based on the consultation:

- the processes by which government agencies interact with ICT companies to request information about those companies' users or to request the restriction of content in law enforcement and national security contexts;
- the processes by which companies receive, manage, and reply to these requests;
- the extent to which these processes are formal or informal;
- the legal/policy frameworks in which these processes take place;
- the extent to which the general public is aware of these laws and processes;
- the extent to which individuals affected by such requests are notified of them;
- the factors governments take into consideration when deciding what information to disclose to the public about requests to companies, including the reasons if/when governments withhold this information;
- the factors companies take into consideration when deciding what information to disclose to the public about requests they receive, including the reasons if/when companies withhold this information;
- the existence of oversight mechanisms such as surveillance authorization; limits on information sharing among government agencies; internal company processes for handling government requests; potential for companies to challenge data requests; and ability of companies to disclose security vulnerabilities in their products and services;
- the existence of remedies provided by governments or companies in cases of unlawful disclosure of information, and unlawful content restriction;
- the prospect of changes to internal processes and to transparency to the public.

Since our focus is on the interaction between governments and companies, our consultations did not address how transparent companies are in other areas, including use of customer data for commercial purposes. Likewise, our questions to governments did not cover other areas of government transparency, such as open government initiatives.

The full list of discussion prompts used with both government and company representatives can be found in the Appendix of this report.

04

INTERVIEW FINDINGS

As mentioned in the previous section, these consultations were carried out in accordance with the Chatham House Rule. Thus, our findings include quotations and statements which are not attributed to any particular government or company representative. However, we have mentioned certain government and company practices by name when these practices are publicly known and discussed.

A number of overarching themes emerged from our consultations:

- *Growing public expectations of government and corporate transparency* – Governments and companies report growing interest from the public, civil society, investors and academics about practices that can affect internet users' rights. Both parties are pioneering new measures to be transparent and acknowledge pressure to do more.
- *Moving beyond numbers* – Governments and companies can better explain the policies and processes involved in government requests to companies. Existing quantitative reporting can be strengthened by providing greater qualitative context. This might include explanations of internal processes, explanations of the legal/policy context, illustrative examples of requests, and narrative content describing the statistics.
- *Aligning government and company reporting* – Meaningful transparency requires greater reporting by governments. It also requires consistency among companies and among governments on how they report on numbers, policies, and practices.
- *The negative effect of ambiguity* – Transparency suffers in the absence of clear laws, policies, and practices. Both governments and companies reported erring on the side of non-disclosure in situations where it is unclear whether something should or could be made public.

In our consultations, we found many similarities between the challenges and opportunities faced by governments and those faced by companies. We have organized this report thematically, with government and company findings combined, to illuminate some of those connections. We have also presented the findings under three broad headings: State of Play (in which current practices are outlined); Challenges (in which obstacles to improved transparency are identified); and Opportunities (in which paths for improvement are identified).

STATE OF PLAY

Government and company representatives cited common motivations for being transparent. They used a range of methods to disclose information to the public.

Motivations

Representatives from the public and private sectors expressed several core reasons to be transparent about government requests for user information and content restriction.

Transparency is Part of the Institution's Philosophy

Both governments and companies identified transparency as a normative value for their institution.

Among governments, some officials started from the premise that transparency was a core value in their country, reflected either in its legal foundations or in the current leadership. Transparency also had an important role in some countries' institutional arrangements, to advance other fundamental or constitutional principles such as the rule of law or separation of powers. This role is manifested in performing an oversight function within government -- e.g., an intelligence agency reporting on its activities to the branch of government that authorizes its activities. As one official explained, "Even if the public isn't deeply engaging, transparency reporting is very important for parliamentary process… People are entitled to expect their representatives to interrogate [government practices] – it is reasonable for individuals to expect this."

Some company representatives also viewed transparency as part of their companies' philosophy or mission. One representative described transparency as an inherent company value, which in turn made specific practices like transparency reporting easy. The company representative(s) explained, "It is assumed we will always be transparent -- there's no Plan B. There's never been a lot of debate, it's just a premise we start with." Another representative echoed this commitment, saying transparency was "core to our mission." One company representative explained that transparency was not a standalone practice but a means to the company's main motivation, which is "to protect the privacy of our customers." As another representative said simply, "It's the right thing to do."

Transparency Builds Trust

Both governments and companies view transparency as ensuring trust among citizens/users, explaining that trust is essential to achieving their core objectives.

Government officials noted that transparency is essential to ensuring public trust in government intelligence and national security activities. Officials described this objective in two ways. One was reactive: that a government needed to be transparent in order to defend its activities against public skepticism or concern. One official explained that the 2013 disclosures by Edward Snowden of government surveillance activities had a "big impact on public debate" around government surveillance in his country. "We have some work to do to regain public trust in the idea of government surveillance," he acknowledged. For another official, however, trust was the starting place for intelligence activities to be successful. In that official's words, "You need public trust in order to carry out your mission. It's hard for people to trust what they don't know about."

For most company representatives, ensuring trust among users was viewed as being good for their business, even giving them a competitive advantage over rivals. As one representative stated simply, "There is a strong commercial consideration in being transparent."

Similarly, a representative said, "It would be a competitive detriment to not have a robust transparency reporting system among social networking companies or Silicon Valley companies." Multiple representatives mentioned that transparency was an area in which they "benchmarked" their performance against competitors.

Some company representatives mentioned specifically how transparency reports play into customer perceptions about the company. As one said, "We are a trust company – our goal is to be very transparent. If our users lose trust, they will leave – they have options to go elsewhere."

However, transparency does not inevitably build trust: the same representative acknowledged that reporting can also generate unease among users who were not previously focused on the issue of government requests, particularly those outside the United States using U.S.-based company services.

Transparency is Increasingly Expected

Both company and government representatives recognized an increasing public demand for transparency.

Officials from multiple governments mentioned that the 2013 Snowden disclosures have raised public expectations of transparency about intelligence operations. "We are certainly the subject of a huge amount of public scrutiny," one official said. "So while our supply side is constrained from the resource perspective," he said, referring to capacity challenges, "the demand side [for transparency] is not."

Company representatives also saw being transparent as increasingly expected, suggesting that users would notice if they were not. One representative said, "The public wants to know: what type of scrutiny are they under?" Company representatives found that since the 2013 surveillance disclosures, users were increasingly aware of privacy issues and posed more questions of companies. As one representative said of the company's decision to be more transparent after the revelations, "The level of debate on this issue was huge – we wanted to add perspective and response." As another representative said, "The more we report, the more users want us to report."

Methods

Governments and companies used a variety of tools to be transparent about their activities. These include transparency reports, principles, guidelines, public education tools, and performance reviews and assessments.

Transparency Reports

To date, most of the attention and advocacy on company and government transparency has focused on "transparency reports," commonly understood to refer to regular statistical reporting on the number of requests made or received in a given period. The governments and companies interviewed were at different stages in their transparency reporting practices. Of those already issuing reports, the substance and the presentation of the information varied.

Company transparency reports detail the volume and type of requests that governments have issued to the company – most commonly, requests to disclose user information or block and/or remove content – sometimes broken down by which government has made the requests.

As mentioned in the Introduction, there has been significant growth in company transparency reporting in the last few years. Multiple company representatives described transparency reports as becoming an industry standard. According to one internet company representative, for companies over a certain size, issuing a transparency report "doesn't even feel like an option anymore – it's the norm."

In the Appendix, we provide a comparison of existing company reports, illustrating some of the trends described here.

To date company reports have generally provided more advanced data on government requests for user information, with less reporting on content restriction. As the Appendix shows, over 90 percent of company reports cover government requests for user information, while only around 30 percent cover government requests for content restriction.

Most company reports have been statistical in focus. However, more recently, some companies are transitioning to provide a more complete picture. As one representative explained, transparency reports serve a broader goal than simply given a sense of scope of requests: they allow the company to "provide clarity to users about our practices, as well as shifts in legal regimes that result in a different approach to user requests and content removal."

Accordingly, some representatives interviewed described how their companies were adding qualitative context to the numbers in their reports. One representative described how the company now complements numbers with a narrative discussing the context in which government requests were being made, such as the legal framework in each country. A representative explained how this approach can help when statistics do not tell the full story – for example, when a law requires the company to give a government continuous direct access to telecommunications information. Vodafone's 2014 Law Enforcement Disclosure Report attracted attention for its inclusion of a legal annex with information on the laws in 29 countries in which the company operates.

Another example of qualitative reporting is Teliasonera's periodic reports on "major events" – defined as "unconventional requests and demands with potentially serious impacts on freedom of expression in telecommunications." These reports explain how the company makes decisions in difficult markets in response to pressing issues, often during or just after the event. For example, Teliasonera reported on orders from the government of Tajikistan to restrict access to websites, or from Kazakhstan to limit communications services in certain districts.

To complete the picture further, some companies have begun to report "in the negative" – that is, to report what the company has not experienced. One company representative consulted came from a company that publishes what it calls "warrant canaries" – noting what types of requests the company has not received, if that type of request typically comes with a non-disclosure order. By reporting zero requests, if the company removes the canary, a careful reader could assume a change. As one representative put it, it is a "way to let people be on notice."

Government transparency reports disclose the number of such requests a government, or part of government, has made to ICT companies as a group. To our knowledge, no government produces a comprehensive report with an inventory of all requests made to companies for user information or content restriction. However, multiple countries issue reports that provide information on requests made by specific parts of government in certain law enforcement and intelligence contexts. The reporting may include quantitative information – specific or aggregate data on number of requests – and/or qualitative descriptions of the laws, policies, and procedures guiding intelligence and law enforcement activities.

These reports are often mandated under legislation in the context of government oversight, such as a law enforcement agency reporting to the entity that authorizes its activities. While in some countries these reports have been published regularly for decades, typically they have not been produced with a broad public audience in mind. Some officials we consulted indicated a shift to viewing the reports as serving more of a public education purpose, and in at least one case a government has designed new reporting to be more accessible to a general audience.

In the Appendix, we provide examples of reporting tactics from governments consulted for this report. We are not aware of any comprehensive comparison of existing government reporting on requests to companies. To contribute to this field of study, the Group has chosen government transparency reporting as an area for further work in 2015-16.

Of reporting to date, in some countries law enforcement or intelligence agencies, as parts of the executive, report directly to another branch of power (usually the legislature) which authorizes or oversees their activities. In Australia, the Attorney General's Department is required to report to Parliament annually on the use of telecommunications interception and surveillance devices by Australian law enforcement agencies under two laws. Other countries have committees independent of government and established by law that carry out reporting. In the United Kingdom, the Interception of Communications Commissioner's Office (IOCCO), an independent oversight body created under the Regulatory Investigatory Powers Act (RIPA), undertakes an audit of how intelligence agencies, police authorities and other public authorities are using interception and communications data acquisition powers against existing legislation. The report is submitted to Parliament and made publicly available.

In our consultations and research, the group found more reporting on requests from law enforcement activities than from intelligence agencies. However, in June 2014, the U.S. Director of National Intelligence and relevant agencies issued the first "Statistical Transparency Report Regarding Use of National Security Authorities," in response to a directive from President Barack Obama to increase transparency about surveillance activities. The report discloses how often the government issued requests under certain national security authorities during a calendar year. (Legislation passed in June 2015, the USA Freedom Act, has since codified additional public reporting requirements for national security activities.)

The existing reporting by governments represented in our consultations is largely focused on requests for access to user information rather than on content restriction – a trend we believe applies more broadly. However, civil society transparency initiatives in Hong Kong and South Korea show that those governments have made information on content restriction requests public. One official we consulted also mentioned that his government had commissioned an academic report that assessed transparency about a voluntary government-company cooperation program for restriction of content related to child pornography.

Principles

Some governments and companies publish principles that inform decisions related to government requests for user information or content restriction.

At the national level, the U.S. intelligence community issued the "Principles of Intelligence Transparency for the Intelligence Community," which outline overall commitments on how the intelligence community will strive to be transparent. According to the document, the principles are intended to "facilitate [intelligence community] decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security." Collectively, the Tallinn Agenda includes high-level commitments on transparency by FOC member governments.

Some individual companies have published principles that guide their practices around government requests. For example, Teliasonera publishes a Group Policy on Freedom of Expression in Telecommunications, which defines the company's "commitments in relation to requests or demands with potentially serious impacts on freedom of expression in telecommunications," such as mass surveillance, network shutdown, or content filtering. Vodafone also includes a list of Privacy and Law Enforcement Principles within its 2015 Law Enforcement Disclosure Report, giving high-level indications of what the company does and does not do when supplying law enforcement agencies with user information.

Companies have made collective commitments to principles relevant to government requests through multi-stakeholder or industry initiatives. Global Network Initiative participants adopt the GNI Principles, which include a high-level commitment to respect and protect the freedom of expression and privacy rights of their users when confronted with government demands, laws or regulations to suppress freedom of expression or that compromise privacy in a manner inconsistent with internationally recognized laws and standards. The principles note that GNI participants will be "held accountable through a system of (a) transparency with the public and (b) independent assessment and evaluation of the implementation of these Principles." The Telecommunications Industry Dialogue, a group of telecommunications companies jointly addressing freedom of expression and privacy rights, is also grounded in a set of guiding principles to which members subscribe. The principles include a commitment to transparency, saying members will: "Report externally on an annual basis, and whenever circumstances make it relevant, on their progress in implementing the principles, and as appropriate on major events occurring in this regard."

While not directly published by companies, civil society-led principles such as the International Principles on the Application of Human Rights to Communications Surveillance have also played a role driving government and company transparency.

Guidelines

While principles lay out the high-level framework for government or company decision-making, guidelines can provide detail on the implementation of relevant policies. Guidelines published by governments and companies provide insight into how they handle requests on an operational level, complementing the high-level commitments outlined in principles. While sometimes written or published with a specific audience in mind (e.g., law enforcement professionals), guidelines provide the public with important information about internal process.

In the case of governments, the process may be articulated in varying levels of detail in the laws and policies authorizing such requests. The most specific example of government guidelines that the Group found in its consultations was from the U.S. Department of Justice, which publishes a manual on the laws and procedures through which federal prosecutors can search and seize computers and obtain electronic evidence in criminal investigations. While intended as a tool for law enforcement professionals, the guide is publicly available on the Department's website and provides a detailed picture of law enforcement authorities and practices in requesting information from companies.

Some of the companies whose representatives we consulted publish law enforcement guidelines which describe the company's process when it receives a request from a government. For example, LinkedIn's Data Request Guidelines outline the types of government requests that are accepted by the company (e.g., subpoenas, search warrants, and requests made through Mutual Legal Assistance Treaties, which are bilateral and multilateral agreements among countries that regulate government-to-government user data requests for law enforcement purposes). The Guidelines explain the information that must be provided by the requesting government agent; the types of data the company might provide in response; and how the company notifies its members about requests that may affect them. Some company guidelines are written explicitly as educational tools for law enforcement professionals seeking to understand how to approach the company. However, company representatives also viewed the guidelines as a

way to provide the public with an understanding of how the company interacts with governments and share best practices with other companies. For example, Teliasonera has published its internal assessment and escalation procedures for how it handles what it calls "major events", as discussed above. These procedures include five assessments: the request's legality; the seriousness of the freedom of expression implications; room for narrower interpretation; business implications of rejection or execution; and risk to safety and liberty of company personnel.

Of the companies we interviewed, fewer published law enforcement guidelines compared to transparency reports. Representatives differed in their assessment of which practice was more important for transparency, and more sensitive. One representative said, "We are more ready to commit to a transparency report than we are to commit to a law enforcement guide," explaining that the company was concerned that publishing law enforcement guide would "invite" requests.

Collectively, GNI participants follow the GNI Implementation Guidelines, which articulate that participating companies will seek to operate in a transparent manner when required by a government to restrict content or provide user information. According to the Guidelines, among other steps, participating companies will – if not unlawful – disclose to users in clear language what generally applicable government laws and policies require from companies, and the company's policies and procedures for responding to government requests.

Public Education Tools

Some governments and companies use dedicated websites or blogs to provide context for policies and practices and describe any changes.

In 2013 the U.S. government launched the website IC on the Record, intended to be a clearinghouse for information related to foreign surveillance activities, with a section of the website dedicated to transparency, including about government requests to companies.

The Australian Attorney General's Department has a section of its website which attempts to demystify new data retention legislation for a more general audience. As well as a link to the legislation, it includes a Frequently Asked Questions page, illustrative case studies of how retained data has been used by law enforcement agencies, and a 'Myths and Facts' page in which the Attorney-General's Department attempts to dispel what it sees as myths about data retention peddled in the public discourse. This follows the Attorney-General's Department's pre-existing webpages aimed at explaining telecommunications interception and surveillance in Australia in accessible language for the general public.

Some companies use company blogs to educate the public about their human rights-related policies, the introduction of new policies, and the context of their transparency reports. Companies are developing new and creative tools to put government requests in context for a general audience. For example, as an accompaniment to its transparency report, Google published a short cartoon video called "Way of a Warrant" describing how the company responds to U.S. search warrants. In June 2015 the Telecommunications Industry Dialogue published an online resource of legal frameworks in 44 countries where authorities seek access to user's communications or to restrict content, to provide the public with more information on the context in which companies operate.

Performance Reviews and Assessments

Some governments and companies also publish, periodically or on an ad hoc basis, policy reviews and public assessments of their performance relevant to the requests covered in this paper. These reports may be reviews of the suitability of specific government or company policies, or may evaluate how the government or company has implemented a policy in practice, including if and how they have veered from stated commitments.

The UK Interception of Communications Commissioner's Office functions as an independent auditor, carrying out inspections on samples of both interception of content and communications data to ensure intelligence agencies, police forces and other public authorities are using interception communications data acquisition powers in accordance with existing legislation. The IOCCO carries out inspections on a sample of the total number of warrants the government issued for interception and, amongst others, reports errors by category such as "failure to cancel interception," "no lawful authority," "over-collection," and "incorrect dissemination." In 2015, the IOCCO moved from annual to twice-yearly reports to monitor changes in public authorities' behavior under new legislation (the Data Retention and Investigatory Powers Act 2014).

In Australia, over the past 20 years there have been five major independent reports on aspects of telecommunications interception.

Governments are also asked to evaluate their performance publicly on issues of privacy and transparency in the context of the multilateral institutions, through mechanisms such as UN Universal Periodic Reviews, and engagement with UN Special Rapporteurs on freedom of expression and on privacy.

We are not aware of any company that individually issues a public assessment of its performance against a certain policy akin to such government reporting. As one company representative said: "That's where the rubber hits the road in terms of transparency – can you be straightforward when you've done something wrong?"

One representative we consulted explained that the company periodically conducts internal reviews of how it is handling content restriction requests, checking the company's decisions against its stated policies. The representative explained: "The company conducts regular spot-checks for the removal decisions, in which staff re-reviews the demand, makes sure the staff processing the demand hits the mark, and that there's consistency. Based on those spot-checks, staff can update the guidelines for removers." However, this assessment is not public. As part of GNI participation, companies agree to independent assessments of their performance on human rights, including their compliance with government requests for user information or content restriction. The first of these assessments was published (in anonymized form) in January 2014.

CHALLENGES

Governments and companies see various legal, policy, and operational challenges to greater transparency around government requests for user information and content restriction.

Legal Challenges

The consultations revealed legal challenges for governments and companies, both in the design and implementation of laws.

Prohibitions on Publication

Representatives from multiple companies mentioned government prohibition on publication as a main difficulty, with one representative calling it one of the "biggest barriers to being more transparent." They mentioned different forms. One form was prohibition on aggregate reporting on a class of requests the government has made of the company, for example, under a specific legal authority. Another form was specific non-disclosure orders that prohibit companies from informing the individual subject of the government's request. The companies whose representatives we consulted varied significantly in their policies on user

notification. From a transparency perspective, one representative explained that while her company understood and respected the need for secrecy in individual cases, non-disclosure orders that were "indeterminate" were "especially problematic."

A company representative reported that a number of countries in which it had operations did not allow the publication of transparency reports under the license agreements between the company and the relevant government. This highlights that, along with generally applicable laws, terms negotiated specifically in license agreements may pose legal challenges for transparency.

Legal Ambiguity

Government and company representatives also demonstrated how legal ambiguity can hinder transparency in practice, as they interpret unclear laws by erring on the side of non-disclosure. When one government official was asked to clarify whether certain companies were allowed to publish the number of interception warrants they had received, he replied: "It is for the company to interpret the law as they see fit, but they have interpreted it as not disclosing." (The government does disclose in that case.) In another country, an official noted that the government had previously said companies were not allowed to report on requests, but a legal analysis commissioned by an external group had found this was not the case. Companies have since started reporting in that country, and the government has not attempted to prohibit publication.

From the company perspective, one representative noted that misinterpretation resulting from opaque laws could create real risks for employees. For companies with in-country staff, if the company publishes something that a government thought should have been kept private, the government could take punitive measures against employees on the ground. A representative noted, "There are situations where nothing can be reported at all, even anonymously, due to national laws, risks to safety and health of personnel."

Differing Jurisdictions

For company representatives managing requests from around the world, understanding and complying with different countries' local laws was a significant challenge – according to one representative, the "biggest legal challenge" the company faces. Companies operating transnationally interact with differing legal systems and standards around the world. "There are many different potential orders and laws in different countries, and there's always a challenge in parsing the law," one said. Company representatives expressed that it is particularly challenging to manage varying laws on content restriction: What does a global company do when the law in one jurisdiction requires restriction of content that is legal in many other parts of the world, or even legal under recognized international standards?

Indirect, Informal, and Extra-Legal Cooperation

In our conversations and research, we found a great lack of transparency when it comes to company-government interactions beyond those clearly defined in law – indirect, informal or extra-legal channels for cooperation. These include self-regulatory and co-regulatory schemes for content restriction, under which governments and companies voluntarily cooperate to identify and restrict illegal content such as child pornography. They also include government use of companies' general Terms of Service enforcement mechanisms. These mechanisms were highlighted as a way in which companies and governments are increasingly interacting; however, there is very little transparency in these processes. The Group's analysis of company transparency reports (see Appendix) illustrates that very few companies report on requests through these channels.

Policy Challenges

Policy challenges to transparency took a number of forms: concerns over the implications of transparency for law enforcement/national security capabilities, transparency's effect on government-company relations, divergent internal attitudes, and unclear policies and processes for remedy.

Compromising Government Operations

Government officials voiced concern that transparency would compromise government operations by revealing the government's capabilities in different ways. As an official explained, "The tension for us is around giving a certain amount of transparency while preserving our ability to investigate crimes and national security threats." As one official put it, the more information is released around a secret, the better adversaries will be able to construct what the government is trying to keep secret.

An official described simultaneous priorities: On one hand, there is "a broad understanding among [intelligence] professionals that we have to better explain why we exist, what are the rules, how we follow them… and that we're not perfect." On the other hand, there is a view that the agencies need to do better protecting "sources and methods" – the strategies and tools used in investigations. "It's really reconciling those two and making sure we're aligned," he said. "I don't see them as inconsistent."

Government officials cited national security risks of different forms. One cited the risk of giving adversaries an overall sense of the scope of that government's activities in a given area. Other officials cited risks in being transparent about specific practices. One official used the example of a remedy process in which individuals can bring claims that their information was unlawfully intercepted. In replying to these claims the government does not confirm the instance of interception if it is found not to be unlawful. This policy in place to "stop terrorists bringing spurious claims just to check if their communications have been intercepted."

When it comes to providing numbers, there was a difference of opinion or practice among governments – and even among agencies within a government – over how providing aggregated vs. specific numbers affected the risk calculation. While one official acknowledged that specific numbers could be helpful internally to show a spike in requests from a particular agency, he called it a "difficult balancing act" how specific to be about these numbers with the public.

In short, one official said: "'Transparency is part of what it means to be in the Intelligence Community, but we have to provide it responsibly because we are stewards of the public trust." Some company representatives acknowledged the risks governments cited, with one company representative advocating that a "balanced approach" be taken for user notification in particular. "It could be argued that people have a right to know, but on the other hand it could be irresponsible for operators to do this," the representative said.

Affecting Government-Company Relations

Company and government representatives acknowledged that transparency can affect their relationship.

One government official said that recent revelations about government surveillance had made relationships with Internet Service Providers more

challenging. "We are looking to rebuild those relationships if we can," he said. Multiple government officials acknowledged in particular the importance of strong government-company relationships for voluntary cooperation regimes, such as those to restrict content related to child pornography. One government had commissioned a study on how to increase transparency in such an arrangement.

Some company representatives were concerned that publicizing information on government requests could provoke a negative reaction from a government, ranging from discomfort to actual risks to the safety of company employees in that country, as noted above. They acknowledged that they incorporate this risk into decisions about what to publish.

Beyond relations with governments, company representatives differed in their interpretations of how and whether transparency reports shaped actual government behavior. Representatives from multiple companies expressed concern that governments would issue more requests as a result of transparency reporting, as they saw the scope of other governments' requests. Another company had not seen evidence for this concern, and in fact the representative professed that in the company's experience, the opposite had occurred. That representative shared an anecdote in which a high-level official expressed skepticism of the company's published number of requests from his government. When the company detailed the requests and their origins, the official was shocked. According to the representative, illustrating "the scale of requests by lower-level officials to their higher-ups [led] to a reduced number [of requests] from that country" in the future.

Multiple company representatives indicated that their company's risk calculation around transparency reporting had evolved, all in the direction of believing that the positive effects of transparency outweighed the risk of provoking more government requests. "We feel comfortable that the benefits to the members outweigh the risks," one said.

Divergent Internal Attitudes

Representatives from companies and governments noted divergent attitudes towards transparency even within their own institutions. They emphasized the importance of high-level commitment within their institutions to overcome disagreements.

Government officials pointed to the role of internal culture and consensus in fostering or hindering transparency efforts. As one official said, transparency is "anathema to many intel[ligence] professionals." Improving transparency took articulating basic principles, such as: "We shouldn't be classifying in order to protect from embarrassment, but in order to make sure it aligns with national security." An official pointed to the need to bring together diverse parts of the government, saying, "They have different perspectives and that's why they value them... A lot of this [effort] is working with agencies and looking at what's being requested to be public, and working together to achieve a common understanding."

Officials reported that high-level commitment to transparency was essential to breaking through disagreement or discomfort at lower levels of government. "What you need is leadership and direction that [transparency] is an important task we should focus on," one said. On prioritizing transparency, one official said: "It's a matter of getting everyone coordinating, moving together toward a common goal. It's complicated, but hopefully we're at a stage where we have a common understanding."

Company representatives also reported differing internal attitudes towards transparency, with the dynamics varying by company. One representative explained that engineers tended to be the champions of transparency and privacy in that company's process, from product development through publication. A representative reported a cultural difference between newer employees and those who had been with the company for a longer period of service, with the longer-term employees in that case tending to see more benefit to transparency. Multiple representatives highlighted the importance of executive-level commitment to institutionalize transparency within the company.

Remedies

Both governments and companies encountered challenges when talking to the Group about mechanisms for remedy: what recourse, if any, is available to a user when his or her information is inappropriately released or restricted. Remedy is the third pillar of the UN Guiding Principles on Business and Human Rights, which recognizes "the need for rights and obligations to be matched to appropriate and effective remedies when breached." However, in our consultations, discussions of remedy fell noticeably short: consultees reported fewer policies and processes in place to handle such cases, compared to other steps in the process of a issuing and responding to government request. Some organizations have conducted research in this area, and the Telecommunications Industry Dialogue includes as one of its principles a commitment by members to "examine, as a group, options for implementing relevant grievance mechanisms." We identify remedy as an area for future work at the end of this paper.

Operational Challenges

Companies and governments reporting operational challenges to greater transparency – in capacity, internal systems, and effective communications.

Capacity Limitations

Both governments and companies pointed to capacity limitations as a challenge. Government officials identified limited resources as a main challenge to being transparent, and one which was not well understood by the public. In one official's words: "I want to be more transparent about how much time and effort it takes to do this and how much your subject matter experts who are supposed to be doing the collection and analysis, you have to pull off that path to work on [how to be transparent]," since they best knew what could be published without compromising government operations. Indeed, one official stated that lack of capacity was that government's main reason for not being more proactive on transparency reporting. Another official whose government has invested in transparency measures acknowledged, "A lot of governments around the world – there's no way they could do it."

Company representatives also said limited resources affected their ability both to track requests and to report them to the public. One company representative explained, "Internally, resources are valuable, and actually generating these reports costs a lot – in terms of staff time – to make them accessible and user-friendly." The resource challenges of tracking requests and then reporting them to the public were considered to become more acute the more jurisdictions the company operated in, with some countries left out of reports simply because of limited capacity. A representative from a larger company acknowledged that capacity was even more strained for smaller companies, for whom "it's a matter of resources" whether they can produce a transparency report.

Designing Internal Systems

Governments and companies also expressed operational challenges in designing effective internal methods for tracking and reporting requests.

For governments, decentralization posed a significant challenge to tracking internally and reporting to the public in a comprehensive manner. For a given government, requests to companies come from multiple agencies, to multiple companies, to serve multiple law enforcement and intelligence purposes. One official interviewed identified nine different government agencies that are permitted under different authorities to make requests of companies, for reasons ranging from counter-terrorism to tax evasion. Indeed, this internal decentralization was a challenge in the Group's effort to arrange government consultations: getting an overview of one government's policies required coordination with and among representatives from multiple agencies, some of which did not usually interact on such matters. Some government officials reported that it was necessary to educate other colleagues on the value of transparency in order to secure their participation in the consultation process.

Company representatives suggested that governments were in a better place to provide a comprehensive picture of requests across operators. However, government officials pointed out that the decentralization of requests may be inherent to a government's structure. They made the case that while companies may be more nimbly structured to have a single point of entry for requests, for a government to have a single point of exit for requests could require significant operational or legal and policy changes. One provided the example that in a federal system, federal officials have less access to information about requests made by state and local governments (which have no general obligation to coordinate or report their investigative activity to the federal government) than the companies would (which receive and can compile requests from all levels).

Company representatives, too, spoke to the challenges of designing effective internal systems. Multiple representatives said their companies were in the process of updating their systems, particularly in response to growing numbers of requests from more and more jurisdictions. These changes included everything from who in the company was involved to the technical tracking: one representative explained that his company had just transitioned from an Excel sheet to a more sophisticated database to track requests.

Communicating Effectively

There is no one audience for the government and corporate transparency tactics outlined in this report. Some are aimed at reporting to elected representatives; others are aimed at the general public; some are for a country-specific audience while others are global. As interest in transparency grows, both government and company representatives reported challenges identifying and communicating well with an increasingly diverse audience.

With growing public interest in government policy, practices such as performance reviews and reports that were previously read mostly by other parts of government and specialists now attract a broader audience among the press and average citizens. New government approaches such as IC on the Record aim to present this information in a more comprehensive way that is accessible to a broader audience. At the most basic level, a government official noted that as surveillance became the topic of increasingly global debate, the fact that his government's reporting was not available in English was a limitation.

Greater transparency leads to more informed public discussion on government policies. An official described how a lack of transparency had led to a "vast misunderstanding among media and the public" during recent policy debates. "People didn't really understand what had been done in the past… Our legislation isn't the easiest thing to understand, nor is it widely publicized," he explained. "It's when the government seeks to make changes that people get their minds focused on this kind of stuff. When you are trying to change a law, you need to convince the public that this is a good thing."

One official noted the need to provide context on why the government could not always be transparent. "Generally we've been so worried about protecting sources and methods, generally our posture is that the less said about you the better – no news is good news," he said. "I'm not even sure certain segments of the public understand why we exist and why we have to keep secrets."

Company representatives likewise noted the challenges of identifying and serving different audiences. When designing a report for mass consumption, representatives voiced frustration at how the statistics could be misportrayed or oversimplified in the media. For example, one representative said, a report that the company complied with a significant number of content restriction requests may be portrayed as a high level of political censorship, when in fact many of the requests had to do with basic fraud or impersonation. Some company representatives instead said that the reports are not intended to appeal to a broad audience. Instead, they are produced for "those who need them" – NGOs, activists, investors, and legislators who may use the reports to analyze and advocate for certain government or company policies. "We want to give people as much information as possible, so that they can assess the scope and impact of laws in their countries," one said. Representatives said that part of their audience used the reports to evaluate company behavior. In the words of one representative, "NGOs hold us accountable." Another representative said "investors show a lot of interest" in that company's transparency reports.

Company representatives also cited language limitations when communicating with a global user base. While the practices companies explain affect a global constituency, most reporting to date has largely been in the English language. As one representative said, "We are very conscious that just because we are being transparent in English may not carry very much weight." She added, "At the end of the day it's about meaningful transparency," and in that company's case, providing information on policies in different languages was a key step toward that aim.

One of the primary concerns that company and government representatives shared in communicating effectively was overcoming the limitations of numbers. Transparency reports have so far focused on reporting the quantitative – number of requests received – without much information on the legal and policy context in which they are made. Company representatives expressed the limitations of this approach, with one saying, "Numbers are not a foundation for true public transparency." That representative said that for that company, "context was more important than numbers, as the context provides more information on the process." Numbers are limited not only because readers lack information on the context, but also because companies have divergent recording and reporting methods that make comparisons difficult. As the representative explained, "If everyone starts publishing numbers, it's inconsistent. Each company has different methods of recording demands. One demand could be five accounts."

OPPORTUNITIES

Government and company representatives identified a range of opportunities – legal, policy, and operational – to increase transparency about government requests to companies in law enforcement and intelligence contexts. While some were specific to individual consultees, both parties frequently raised the value of cooperation among governments or companies, as well as with other stakeholders.

Legal Opportunities

Representatives identified opportunities for legal improvements, instigated both from within governments and by external actors.

Legal Reform

Multiple governments whose officials we interviewed were in the process of reviewing policies relevant to transparency and government practices related to access to user information and/or content restriction. Officials from one government pointed to forthcoming legislation as a source for transparency improvements. Another official interviewed reported that his government was actively considering new reporting on intelligence requests. In addition, both domestic and regional courts are reviewing challenges to existing legislation that may affect transparency about government requests.

One example of legal reform is the USA Freedom Act, adopted in the United States in June, which includes new transparency provisions among other reforms. For example, the Act requires declassification (or, where that is not possible, declassified summaries) of opinions by the Foreign Intelligence Surveillance Court of Review (FISC) that involve significant or novel issues. It also increases the government's public reporting obligations regarding specific uses of FISA authorities, and allows recipients of FISA orders to make either annual or semiannual reports of the approximate aggregate number of FISA orders they have received.

Encouraging Change from the Outside

Company representatives saw opportunities to push for legal reform from the outside. One company representative emphasized the opportunity for companies to challenge government requests in court, and to push for the ability to disclose more information on requests received. Several companies whose representatives we consulted had taken legal action for the right to publish more information on national security-related requests, which had resulted in an agreement with the government permitting greater transparency.

Clarifying Legal Frameworks

Company representatives also mentioned opportunities to work with governments to clarify legal application. Representatives reported that they work with governments to narrow the scope of a request to provide what was necessary for law enforcement/intelligence purposes, while limiting the request's effect on users (for example, in terms of the number of accounts affected, or the impact on users over whom the government in question has no jurisdiction).

Policy Opportunities

Government and company representatives identified multiple policy opportunities to improve transparency – through government reporting, working together, and public education.

Enhancing Government Transparency Reporting

Both stakeholders identified opportunities for governments to disclose more information on the requests they make to companies.

Representatives from a number of countries interviewed reported that their governments were considering being more transparent about requests being made to companies as a matter of policy.

Since the Group began this project, there have been developments in a number of countries we consulted, in addition to the passage of the USA Freedom Act in the United States. In Sweden, the government publishes an annual report to Parliament with statistics on government applications by law enforcement agencies for interception of electronic communications. Last year's report commissioned a study to consider how to increase transparency about the use of surveillance by the Swedish Security Service responsible for intelligence gathering. In June, the investigator commissioned to look into this possibility recommended greater reporting on intelligence activities, a proposal which is now under consideration.

Overall, officials expressed varying likelihoods that their governments would become more transparent, depending on political dynamics in each country and the level of reform already undertaken or underway. One official reported that he "can't imagine a complete overhaul" of policies, but that his government "will keep pushing the boundaries" within the bounds of the law. An official reflected that after recent reforms, "We think we have the balance right with our reporting requirements, as far as our mandatory ones go."

Many company representatives emphasized the need for governments to directly provide more information to the public. As noted earlier, some company representatives suggested that governments were in a better place to provide a comprehensive picture of requests to the public because the government could report across operators. One representative suggested that governments should also "report on which requests have gag orders associated with them," which companies cannot disclose, and that these reports should be verified by third parties.

Generally, government officials saw discussions about the appropriate bounds of government transparency about requests to companies in the context of ongoing policy debates resulting from technological changes. "Technology has changed everything, because it means there's just so much more information available," one said. "This isn't a static phenomenon – it's very vibrant, and one where we'll have a continuing dialogue in our courts and executive branch, all driven by changes in technology."

Working Together

Overall, all consultees identified room for improvement in their individual practices and pointed to the value of collaboration, both within their stakeholder groups as well as among governments and companies.

Across the consultations, representatives from companies expressed eagerness to learn from other companies when adopting a new transparency policy or practice. Company representatives also identified opportunities to work together, including in standardizing the way in which they report on government requests (from how requests are counted to how they are categorized publicly) and in advocating for legal, regulatory, and procedural reforms by governments. "We have an opportunity to work together across government, civil society organizations, and companies on trying to improve methodologies so it becomes more like apples and apples," one company emphasized. Some representatives also mentioned collaboration with initiatives such as the Chilling Effects website, which collects reports of legal complaints and requests for content removal.

Some company representatives who are members of multi-stakeholder initiatives mentioned the importance of these groups in shaping their approach to transparency. One representative reported that participation in the GNI was very important for developing transparency policies and applying them in the countries in which it operates. In particular, the company's internal team dealing with law enforcement requests cites commitment to the GNI principles as reason and justification for pushing a government for more specificity in a request, for getting the request in writing, and for interpreting the request narrowly.

Government officials also noted the value of dialogue with each other, companies,

and other stakeholders on these issues. One official acknowledged, "There needs to be a continued dialogue and set of standards between companies and governments." Another official emphasized that the current debates about transparency were just one example of policy issues where the government and citizens will have to ask , "What do we want in society?" He emphasized, "Media and civil society are also part of the process to challenge and ask questions."

Public Education

Government and companies saw opportunities for broader education of the public. Being more transparent requires not just the disclosure of more information, but also equipping the audience with the framework to understand it.

For governments, effective transparency education starts with explaining the mission of law enforcement and intelligence agencies. "What I want us to be more transparent about is the value we have to national security and our partners, and the need we have to keep secret a lot of what we do," one official said. Another stated: "We could do a better job of communicating what is going on with the general public." He admitted "people may or may not be interested," but that when policy debates arise, basic education was critical for informed public debate.

Likewise, companies can educate users proactively that their information can be accessed by governments in some circumstances. "We inform our customers that there are exceptions when we cannot protect their privacy," one representative explained. Government and company representatives repeatedly highlighted that for better public understanding required more qualitative transparency about the policies and processes underpinning government requests to companies. One company representative said that the top of her "wishlist" for better transparency was finding a way to provide more explanation of what legal requests are, how they work and what they mean. The Google "Way of a Warrant" video describing the process of a U.S. warrant mentioned above is one way to provide this type of context.

A company representative explained that in her experience, being transparent not only educated the public, but also created opportunities to improve policies, as questions from users prompted the company to clarify and consider revisions.

Operational Opportunities

Government and company representatives identified opportunities to educate people across their institutions and to be more consistent internally.

Internal Education

Company and government representatives acknowledged that the process of compiling a transparency report or related materials helps educate people internally about what different parts of their institutions are doing and the broader implications of their actions. "Tracking and reporting is helpful for internal governance and processes," one company representative explained.

An official whose government had made recent transparency improvements highlighted the importance of making sure they took hold at all levels of the government, explaining, "We are institutionalizing these processes and changes so that they are part of the Intelligence Community going forward." Company representatives suggested that company reports showing the extent and range of government requests can also prompt better internal coordination among agencies of the same government by giving them an overall picture of requests made and prompting better coordination among agencies. In the words of one company representative, "[Company] transparency reports can help governments get their own houses in order." Companies also suggested that law enforcement guidelines help educate government officials on how to legally issue a request to a company for user information or content restriction.

Consistency

Government and company representatives identified opportunities for greater consistency around the processing and reporting of government requests, both internally and across their stakeholder groups.

An official from one government identified standardization of request processes and reporting across government agencies as an area for work. The official identified initial steps as standardizing and making public the procedures for gathering information, the level of aggregation, and how the data is aggregated.

Many company representatives saw room for improvement in establishing consistent sector-wide standards for transparency reporting – both in how companies count and categorize requests they receive, and how they present them to the public. There are currently a variety of approaches to collecting data and to counting and reporting requests, making it impossible to compare data from different companies. "If we are able to consistently have similar categories and approaches among our peers," one representative said, "there is a standard foundation for members to compare and contrast policies." For one representative, this would ensure that the data reported "becomes more meaningful."

05
RECOMMENDATIONS

Based on the Interview Findings, and informed by the collective expertise of Working Group members, we make the following recommendations for governments and companies wishing to be more transparent about government requests for user information and content restriction. These recommendations are specific to the law enforcement and intelligence contexts, which accords with the scope of the Group's activities.

These recommendations build on, and reinforce, a canon of principles and best practices in the Internet freedom field and fit into a broader conversation about transparency from companies and governments in areas that can affect human rights. We see multiple opportunities for advancing these recommendations, through the Working Group and through other avenues. Companies can work through established multi-stakeholder initiatives and otherwise with civil society and investors leading projects focused on aligning expectations on corporate transparency. Governments developing National Action Plans on Business and Human Rights (building on the UN Guiding Principles) can use that process as an opportunity for greater transparency and accountability on the issues raised in this report. We look forward to further collaboration with governments, companies, and all stakeholders working in this area.

FOR GOVERNMENTS

Establish clear policies and processes for making requests to companies and reporting on them to the public

Consistent with the Tallinn Agenda, government requests to companies for user information and content restriction must respect human rights obligations and be consistent with the principles of the rule of law, legitimate purpose, non-arbitrariness, effective oversight, and transparency. Important procedural safeguards include:

- Promoting transparency and independent, effective domestic oversight related to electronic surveillance, use of content take-down notices, limitations or restrictions on online content or user access and other similar measures;
- Submitting requests through formal channels via clear, legally binding processes that enable such accountability and oversight: requests in writing, signed by an authorized official of the requesting agency, stating the appropriate law under which the request was made;
- Disclosing to the public the legal authorities and processes through which requests to companies are made, and what information can be obtained/ restricted;
- Clarifying which government offices/officials have the authority to make requests of companies;
- Clarifying the permitted uses for information obtained through a request (e.g., disclosing in criminal trials how information was obtained);
- Ensuring access to appropriate and effective remedy for individuals whose privacy or freedom of expression have been violated.

Work together, and with all other stakeholders, to develop best practices for government transparency about requests made to companies

Governments should work together and with all other stakeholders including civil society, the technical community, investors and academic experts, on standards and best practices for public disclosure about requests made to companies in law enforcement and intelligence contexts. The Working Group welcomes FOC governments who were not represented in our consultations to engage with us in the next year. Group members can serve as resources to governments developing or revisiting transparency practices. We also encourage governments to work with other civil society-led initiatives focused on government reporting.

Expand the scope of government reporting on requests made to companies

As governments try new approaches to transparency, they should explore ways to coordinate across relevant government agencies with the power to make requests. No government has produced a comprehensive report on requests made to companies for user information and content restriction over a specific time period. Comprehensive reports would give citizens a more complete picture of how their governments are using their authority to access personal information or to restrict content. FOC governments are in a good position to consider what such a report would entail, including the kinds of internal coordination mechanisms that would be necessary to compile reports and how best to present them to the public.

Strengthen qualitative transparency about laws, policies, and processes

To complement increased quantitative reporting, governments should disclose to the public the laws, policies, and authorities that are employed to make requests to companies. It is also important to disclose which parts of government are involved, and which have clear legal authority to request user information and content restriction. Where governments are already taking steps to be transparent – as through statistical reports, or policy reviews -- they should pursue ways to make this information more accessible. This may involve centralizing reporting on a common website, and contextualizing it for a general audience.

Make a high-level commitment to transparency, and commit resources accordingly

Governments should make a high-level, public commitment to increasing transparency about requests made to companies. They should reflect this commitment by dedicating employee time and allocating a sufficient budget for reporting processes and other measures to inform citizens. They should develop mechanisms for coordinated record-keeping across government agencies that make requests of companies for user information and content restriction, and for keeping this information updated within a reasonable time period.

FOR COMPANIES

Establish clear policies and processes to receive, process, and report on government requests for user information and content restriction

Companies can learn from each other and other stakeholders to implement responsible systems around government requests. These include:

- Limiting company entry points for government requests, and which employees have access/authority to respond;
- Establishing practices for challenging overbroad requests, or those that are outside the scope or authority of the law;
- Having clear mechanisms for escalation and oversight within the company for requests that raise significant policy and human rights questions;
- Tracking and responding to requests in a consistent way globally;
- Conducting periodic reviews of company policies and processes;
- Providing mechanisms for user notification and appeal.

Strengthen qualitative transparency about company policies and processes

While companies should publish to the extent legally possible the numbers of requests they receive and comply with, they should also regularly publish information that clarifies their policies and procedures for responding to government requests. This may include publishing law enforcement guidelines and/or providing information on the political and legal contexts in the countries where the company operates (including, where possible, what information a company is not permitted to report in a country, and/or areas of ambiguity in the law). This "qualitative transparency" provides essential context for quantitative reporting on government requests. Companies should explore ways to educate readers of transparency reports, such as a guide to the legal processes the company undergoes, explanations of what report terminology means, and narrative description of report content and how it compares to prior years.

Work together, and with all other stakeholders, to standardize company transparency reporting

Companies should work with each other and with civil society, academics, investors, and the technical community to develop industry-wide standards for reports and other measures to boost sector-wide transparency about government requests. Currently, reports differ so widely in their scope and approach that it is difficult to carry out the type of comparative analyses that would facilitate policy recommendations. Recognizing that companies have diverse business models and services, consistency in tracking and reporting would help citizens compare the scope and nature of government requests across services. A number of organizations are working on developing best practices and templates for reports and can be resources. Multi-stakeholder initiatives like the Global Network Initiative also play an important role in facilitating common approaches.

Expand the scope of current reporting

Companies have focused mostly on transparency about government requests for access to user information. Companies should expand their reporting on government requests for content restriction, disclosing the nature and number of requests as well as how the company handles them. To complement reporting on requests received in a past period, companies can be transparent with users proactively. This may include:

- Informing users of company policies before entering a new market;
- Informing and educating users when Terms of Service are revised, possibly including a "red line" version of the TOS that highlights changes;
- Setting clear policies for managing and reporting on requests the company has not yet received but expects to receive in the future.

Make an executive-level commitment and commit resources accordingly

Companies should make an executive-level commitment to transparency and educate all parts of the company on how and why to be transparent around government requests for user information or content restriction. Managing government requests and being transparent takes resources and coordination. Companies should reflect their commitment by dedicating employee time and allocating a sufficient budget for regular, timely reporting and other measures to inform users. Smaller companies with limited capacity can draw on the experiences of more established companies and on other efforts in the field to develop templates and best practices.

06

NEXT STEPS

Through our consultations we identified the following areas for future work on transparency for both the Working Group and other stakeholders.

Processes for Government Transparency
Current government reports are limited to certain parts of government or specific government activities. How can governments coordinate internal reporting processes to provide a more comprehensive picture of government requests? What are best practices for standardizing processes across different parts of government? What safeguards are necessary to ensure that individual privacy is protected in the process of compiling reports?

Qualitative Transparency for Companies and Governments
While reports focused on numbers remain a cornerstone of transparency reporting, governments and companies can explain their policies and practices to the public in an accurate and accessible way. What information helps citizens understand how their data is accessed or restricted, by whom and under what circumstances? What information on laws, policies, and processes should companies and governments disclose? Are there reasons why companies or governments might believe that disclosing this information could have negative consequences? What are best practices for providing qualitative transparency?

Transparency about Content Restriction
Most reporting by governments and companies has focused on requests for user information. To mitigate risks to freedom of expression, both parties can be more transparent about government requests to companies for content filtering or removal. What is the scope of these content restriction requests? What are the laws, policies, and processes involved? Are there best practices for conveying this information to the public in an understandable way, taking into account different laws and categorizations of content across jurisdictions?

Cooperation through Indirect, Informal, and Extra-legal Channels
Public debate has focused on transparency about direct government requests to companies, yet other mechanisms for government-company cooperation remain opaque. These include self-regulatory and co-regulatory schemes for requests for user information or content restriction, and governments' use of companies' Terms of Service enforcement mechanisms. Recognizing the potential human rights implications of these arrangements, how can governments and companies provide transparency in these cases?

Developing Remedy
Under the "Remedy" pillar of the UN Framework on Business & Human Rights, states must take appropriate steps to ensure that when business-related human rights abuses occur on their territory, those affected have access to effective remedy. Companies have a responsibility to respect human rights in the context of government requests, but the role of redress mechanisms for victims of abuses has never been fully defined. Company and government representatives reported fewer policies or processes in place to handle such situations and be transparent. Under what laws and authorities are citizens entitled to remedy from governments and/or companies, and what do these processes entail? How can these be communicated to the public?

FUTURE ACTIVITY FOR THE WORKING GROUP

At the FOC conference in Mongolia in May 2015, the Working Group's mandate was renewed by FOC member governments. Our new mandate extends to next FOC conference in 2016. The Group has identified two areas of focus out of the topics above. Building on the work reflected in this report, the Group will focus on 1) models and best practices for government transparency reporting on requests made to companies, and 2) best practices for qualitative transparency – how governments and companies can provide transparency about laws, policies, and processes related to government requests to companies.

The public debate on transparency so far has focused mainly on the relationships and practices among U.S. and European companies and governments. In our future work, we are committed to including the range of perspectives from companies, civil society and governments around the world necessary to advance global best practices. Likewise, we are interested in exploring areas of government-company interaction beyond the national security and law enforcement context.

We welcome collaboration with any initiatives or individuals working in these areas. To contact the Group, please email info@freedomonlinecoalition.com.

07

APPENDICES

CONSULTATION PROMPTS

The Working Group used the following prompts to structure conversations with governments and companies about requests for user information and content restriction. They were designed to foster open discussion under Chatham House Rule.

COMPANY CONSULTATION PROMPTS

The Members of the Working Group seek clarity and insight on the following set of core topics to further their understanding of the current state of play in terms of transparency, and opportunities/obstacles therein. The topics are divided into two main areas for discussion: Access to User Information, and Content Removal/Blocking. Each area has three sections: Transparency, Oversight, and Remedy.

We hope you and your colleagues will give these topics consideration in advance of the meeting. If a given topic is difficult to address in this setting, we are eager to understand that limitation.

Access to User Information

1. Transparency

Members of the Working Group seek to better understand the factors that companies consider when approaching transparency around government access to user data. These factors may be internal (e.g., company policies or practices) or external (e.g., legal environment). We would like to understand company decision-making processes regarding if and how information about these requests is shared publicly, and if and how individual users are notified.

Members of the Working Group also seek to better understand how companies view the potential value or risks associated with publicizing these requests. We also seek to understand motivations for providing public reports on government requests, and other actions taken to further company transparency.

2. Oversight

Members of the Working Group seek to better understand company practices and oversight mechanisms used for handling requests from governments for user data, and challenges or considerations faced in responding to these requests. Relevant practices include but are not limited to internal procedures for reviewing or objecting to requests (e.g., on legal grounds), determining whether requests were made legitimately and appropriately, and identifying data or content that may be produced. We are interested in mechanisms to review and process requests for user data ex ante, and/or to review the sufficiency of and compliance with related procedures ex post.

Similarly, we hope to learn more about how internal oversight mechanisms and policies are crafted, how those policies speak to the organization's goals with respect to transparency, and how, if at all, those policies respond to public opinion and changes in the legal climate.

3. Remedy

Members of the Working Group seek to better understand company practices and considerations with respect to the notification of users affected by government requests for user data. We are also interested in company practices and challenges in providing and implementing remedial procedures for customers when user information may have been unlawfully or inappropriately released.

Content Removal/Blocking

4. Transparency

Members of the Working Group seek to better understand the factors that companies consider when approaching transparency around government requests for content removal/blocking. These factors may be internal (e.g., company policies or practices) or external (e.g., legal environment). We would like to understand company decision-making processes regarding if and how information is shared publicly, and if and how individual users are notified.

Members of the Working Group also seek to better understand how companies view the potential value or risks associated with publicizing these requests for content removal/blocking. We also seek to understand motivations for providing public reports on such requests, and other actions taken to further company transparency.

5. Oversight

Members of the Working Group seek to better understand what internal oversight mechanisms are in place within companies to guide processing and responding to government requests for content removal/blocking ex ante and/or to review the sufficiency of and compliance with related procedures ex post regarding such requests.

6. Remedy

Members of the Working Group seek to better understand company practices and considerations with respect to the notification of users affected by government requests for content removal/blocking. We are also interested in company practices and challenges in providing and implementing remedial procedures for customers when user information may have been unlawfully or inappropriately released.

GOVERNMENT CONSULTATION PROMPTS

The Members of the Working Group seek clarity and insight on the following set of core topics to further their understanding of the current state of play in terms of transparency, and opportunities/obstacles therein. The topics are divided into two main areas for discussion: access to user information, and content removal/blocking. Each area has three sections: Transparency, Oversight, and Remedy.

We hope you and your colleagues will give these topics consideration in advance of the meeting. If a given topic is difficult to address in this setting, we are eager to understand that limitation.

Access to User Information

1. Transparency

Members of the Working Group seek to better understand the factors that governments take into consideration in authorizing, compelling or prohibiting requests for user data, including potential limitations and constraints in disclosing and discussing the sources of legal authority and relevant interpretations thereof that authorize, compel or prohibit government requests for user data for criminal investigation or intelligence purposes.

Members of the Working Group seek to better understand the types of concerns that impact a government's willingness to disclose or to allow companies to disclose information about specific and aggregate numbers of government requests for company user data.

2. Oversight

Members of the Working Group seek to better understand the perspectives of relevant government agencies of the benefits and drawbacks of different forms of oversight mechanisms that are or could be used to authorize requests for company user data ex ante and/or to review the sufficiency of and compliance with related procedures ex post.

3. Remedy

Members of the Working Group seek to better understand the challenges that relevant government agencies face regarding existing, or potential new efforts to establish, remedial procedures that are/could be used to identify when company user data may have been inappropriately accessed, used, or shared with/by governments, and to establish related remedies.

Content Removal/Blocking

4. Transparency

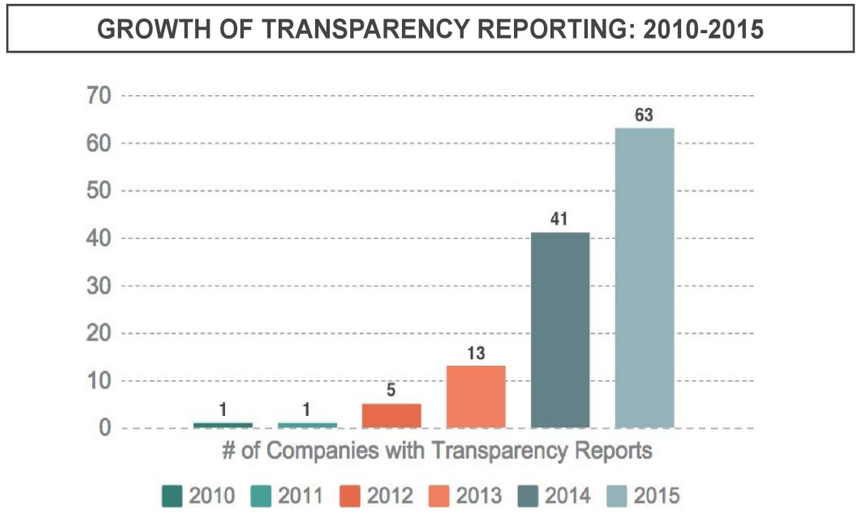
Members of the Working Group seek to better understand the laws and policies, including regulations upon which governments depend in order to identify and vet information that the government believes should be removed by companies from their platforms or through other means (such as filters or blocking) made inaccessible for users, whether for intellectual property, libel/reputation, or other purposes.

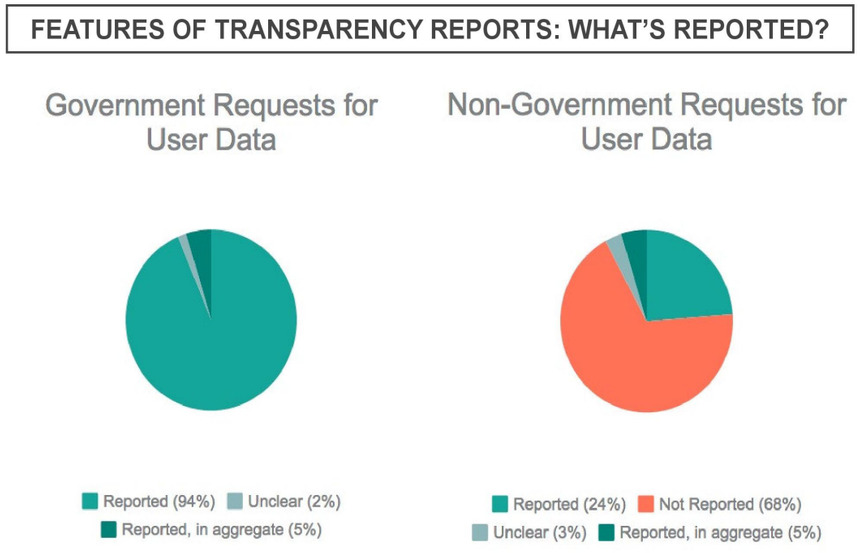
Members of the Working Group seek to better understand the views of relevant government agencies on the potential value or risks associated with making requests for content removal public.

5. Oversight

Members of the Working Group seek to better understand the perspectives of relevant government agencies on the benefits and drawbacks of different forms of oversight mechanisms that are or could be used to authorize requests for content removal ex ante and/or to review the sufficiency of and compliance with related procedures ex post regarding government takedowns.

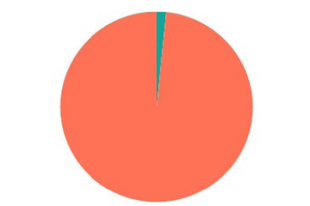
COMPANY TRANSPARENCY REPORTING PRACTICES





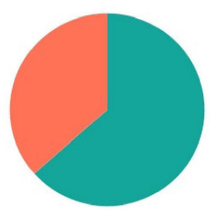
FEATURES OF TRANSPARENCY REPORTS: WHAT'S REPORTED?

Terms of Service and Policy Enforcement



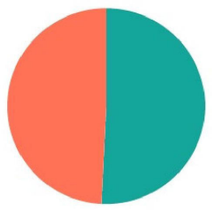
Reported (2%) Not Reported (98%)

Compliance with and/or Responses to Requests



Reported (63%) Not Reported (37%)

Also Publishes a Law Enforcement Guide



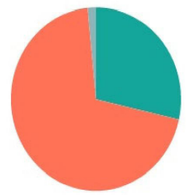
Yes (51%) No (49%)

Reports Having Never Received a Request for User Data

Yes (No Requests Received) (10%)
No (Requests Received) (90%)

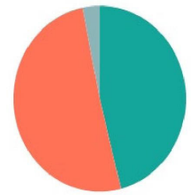
FEATURES OF TRANSPARENCY REPORTS: WHAT'S REPORTED?

Government Requests for Content Removal



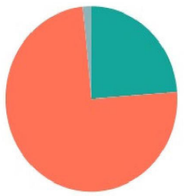
Reported (29%) Not Reported (70%)
Unclear (2%)

Non-Government Requests for Content Removal



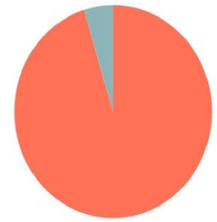
Reported (46%) Not Reported (51%)
Unclear (3%)

Intellectual Property Takedowns



Reported (24%) Not Reported (75%)
Unclear (2%)

Requests from Self- and Co-Regulatory Regimes



Not Reported (95%) Unclear (5%)

GOVERNMENT TRANSPARENCY REPORTING PRACTICES

To the Group's knowledge, no one has done a comprehensive comparison of current government transparency reporting. While this Group could not undertake such a survey, our review of reports from governments represented in our consultations revealed a range of practices that enhance transparency. The following reports illustrate approaches that could be considered for incorporation into the reporting practices of FOC governments. They do not reflect the full extent of reporting activities by these governments.

Reporting on Interception Errors

United Kingdom

In the United Kingdom, the Interception of Communications Commissioner's Office (IOCCO), mandated by Section 57(1) of the Regulatory Investigatory Powers Act (RIPA), undertakes an annual audit of the use of interception against existing legislation as part of the government's oversight regime. The findings from that audit are reported to Parliament annually and made publicly available. As part of the audit, the IOCCO inspects a sample of interception warrants issued during the reporting period and identifies any errors committed in the implementation of the warrant. The March 2015 report identified 60 interception errors, broken down by category.

A breakdown of interception errors under RIPA can be found in the Interception of Communications Commissioner, Rt. Hon Anthony May, March 2015

Identifying Areas for Improvement

Sweden

The Swedish Government submits an annual national surveillance report to Parliament titled "Account of the Use of Certain Secret Surveillance Measures". The report describes the history and provisions of the Code of Procedure and the checks and balances that govern covert surveillance operations in the country. It also breaks down the statistics for surveillance, interception, and collection of electronic communications by criminal investigation type, with comparisons to the previous year's numbers. The report ends with an update of proactive government actions that have taken place during the year and planned improvements to further increase transparency.

Describing the Application of Government Authorities

United States

In addition to an annual statistical report, the National Security Agency Director of Civil Liberties and Privacy Office published two special reports in 2014 with specific information on the NSA's use of two national security authorities that have been the subject of public debate: Section 702 of the Foreign Intelligence Surveillance Act, and Executive Order 12333. The reports include descriptions of how the NSA uses those authorities in practice, including at the level of the individual analysts and supervisors responsible for implementation. It also describes the safeguards used by the NSA to protect privacy and civil liberties at each stage of implementation.

Disclosing How Data Was Used

Australia

In Australia, the Attorney-General issues annual reports that detail the interceptions, access to telecommunications information, and use of surveillance devices by government authorities. The reports include the number of prosecutions in which lawfully intercepted information was given in evidence and the categories of crimes prosecuted as a result of those interceptions, disaggregated by jurisdiction.

A breakdown of the number of prosecutions in which lawfully intercepted information was given in evidence can be found in the Telecommunications (Intercept and Access) Act 1979 – Annual Report 2013-14

Creating a Dedicated Public Resource

United States

Agencies in the United States Intelligence Community created a dedicated website, IC on the Record, for the purposes of ongoing transparency reporting to the public. IC on the Record serves as clearing house for information related to foreign surveillance activities of the U.S. Intelligence Community, including official statements, statistical transparency reports, testimonies, declassified materials and fact sheets.

The annual Signals Intelligence Reform Report published on IC on the Record includes an inventory of measures taken by the U.S. intelligence community to enhance transparency.

Freedom Online Coalition Support Unit

GLOBAL PARTNERS DIGITAL

Development House
56–64 Leonard Street
London EC2A 4LT

+44 (0)20 7549 0336

freedomonlinecoalition.com