



# FREEDOM ONLINE COALITION

MAY 2015

## **WORKING GROUP 3**

Privacy and Transparency Online



# WORKING GROUP 3

## Privacy and Transparency Online

### Working Group 3 “Privacy and Transparency Online”

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

#### Members of Working Group 3

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

Note: This document is a draft executive summary of the forthcoming report of the Working Group. It is a living document and will be updated in the final report.

#### Freedom Online Coalition Support Unit

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

[info@freedomonlinecoalition.com](mailto:info@freedomonlinecoalition.com)

---

## EXECUTIVE SUMMARY (DRAFT)

---

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 26 governments, working to advance Internet freedom – free expression, association, assembly, and privacy online – worldwide.

This Working Group is comprised of experts from governments, Information & Communications Technology (ICT) companies, civil society and academia from across five continents. The Group was established under the auspices of the FOC and aims to support the implementation by member governments of the 2014 Tallinn Agenda for Freedom Online, which emphasizes the importance of transparency and open government as part of member states' commitment to Internet freedom.

Specifically, FOC members “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.”

Our work also builds 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.” The UN Guiding Principles on Business and Human Rights adopted in 2011 established the “Protect, Respect, and Remedy Framework” under which governments have the duty to protect human rights, companies have the responsibility to respect human rights, and both have an obligation to provide mechanisms for remedy. We also draw on principles and operational guidance specific to ICT companies established in 2008 by the Global Network Initiative.

This report represents the first phase of the working group's work. It focuses on transparency about government requests to companies for user information or content restriction, specifically in law enforcement and national security contexts.

This working group aims 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.

Transparency in how governments make these requests to companies, and in how companies respond to them, is critical to protecting and respecting Internet users' rights. Transparency enables governments and companies to demonstrate whether they are upholding key principles from the Tallinn Agenda for Freedom Online - such as the rule of law, collection for a legitimate purpose, non-arbitrariness, and effective oversight - and for other stakeholders to hold governments and companies accountable to such principles.

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.

In analyzing government requests to companies in national security and law enforcement contexts, we sought to provide clarity to the following areas:

- General understanding of the general legal context as well as the specific laws, policies, and processes that govern the relationship between ICT companies and governments;
- How ICT 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.

## METHODOLOGY

The Working Group developed a series of questions to consult with representatives of governments and companies regarding their privacy and transparency practices connected to government requests on matters related to national security and law enforcement. The consultations were conducted in accordance with 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.

Our consultation framework consisted of two parts: the first on access to user information; and the second on content restriction. We looked at how governments and companies publicly disclose information about the process, number and nature of the requests. In each section, we posed a series of questions inquiring into the current state of affairs, challenges to transparency (including legitimate law enforcement and intelligence needs), as well as opportunities for improvement.

The governments and companies we interviewed varied both in type and in scope of transparency-related policies and practices. We focused on FOC member governments and ICT companies with transnational reach. We interviewed 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

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.

We find the qualitative insights gained from these interviews to be essential in informing a conversation about identifying and implementing best practices on transparency about government requests to companies. We see that conversation as the next stage of analysis by members of this Group and others in the field. To that end, we have put forward some preliminary recommendations and areas for future research.

## CONSULTATION FINDINGS

A number of overarching themes emerged from our consultations:

- *Growing public expectations of government and corporate transparency around matters that affect Internet users' rights:* Governments and companies are pioneering new measures to be transparent, and civil society groups are advocating for both to do more.
- *Moving beyond numbers:* Transparency reports published by companies and a few governments that have tended to focus on the numbers of requests can be strengthened by providing greater context. This might include explanations of the policies and processes governments and companies follow, illustrative examples of requests, and narrative content describing the data, including how it might differ from previous reports.
- *Providing the full picture:* Meaningful transparency requires greater government reporting, as well as consistency among companies and among governments.
- *The effect of ambiguity:* Transparency suffers in the absence of clear laws, policies, and processes.

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

### STATE OF PLAY

Governments and companies use a range of measures to provide transparency about government requests made to companies for access to user information or content restriction. These include transparency reports, guiding principles and other public education tools.

- *Transparency reports:* The governments and companies interviewed were at different stages in issuing transparency reports. Company transparency reports detail the volume and type of requests issued by them to governments – most commonly, requests to disclose user information or block and/or remove content. Government transparency reports disclose the number of such requests a government, or part of government, has made to companies.
- *Guidelines:* Some governments and companies rely on formalized guidelines or principles to inform decisions related to government requests. Some companies

publish these guidelines to explain how they respond when governments request user information or content restriction.

- *Public education tools:* Some governments and companies use dedicated websites or blogs to describe changes and provide context for reports or policies.

To date, transparency reports have been the dominant tool, especially among companies. While these are largely retrospective – reporting on number of requests in a prior period – we see a rise in proactive measures, such as a company explaining policies before entering a new market, or reporting which requests it has not received.

## MOTIVATIONS

Many companies and governments interviewed were already taking steps to be transparent, as in the issuance of a transparency report. Representatives from both the public and private sectors expressed some common motivations for being 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. Some government officials started from the premise that transparency as a tool for government accountability was a core value in their country, reflected either in its legal foundations or in the current leadership. Some companies also viewed transparency as part of their philosophy or mission, with their reporting practices being one part of a larger, overarching commitment to transparency.
- *Transparency as ensuring trust:* Government officials noted that transparency is essential to ensuring public trust in government 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 critical for business.
- *Transparency is a growing expectation:* Both government and company representatives recognized an increasing public demand for transparency. Some company representatives suggested that not being transparent would be a competitive detriment. Company representatives also identified specific audiences for their reports, including investors, the press, and NGOs and other advocates.

## CHALLENGES

Governments and companies see various kinds of challenges (legal, policy, operational) to greater transparency about government requests for user information and content restriction.

### *Legal challenges:*

- Prohibitions against publication of certain information or classes of information were identified as a shared legal challenge.
- 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.
- For some companies, the transnational nature of their operations makes it

necessary to interact with various legal systems with differing standards. This was particularly challenging with 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?

#### *Policy challenges:*

- Transparency's implications for national security and law enforcement were identified as a policy challenge, due to concerns that transparency would compromise government operations.
- Some company officials were concerned that their disclosure of information about government requests could undermine relations with some governments. Additionally, some companies believed that publicizing requests could provoke a law enforcement backlash and might even pose risks to the safety of employees in some countries.
- Representatives from companies and governments noted divergent attitudes towards transparency even within their own institutions. They emphasized the importance of high-level support and commitment to overcome disagreements.

#### *Operational challenges:*

- Both governments and companies identified capacity limitations as a challenge. Companies' limited resources made it difficult to track and report on requests. Government officials also cited capacity limitations as a main obstacle to being more transparent, particularly as decisions about publishing sensitive information requires input from subject matter experts.
- Designing effective internal methods for tracking and reporting requests was considered to be another operational barrier, particularly if there was not a centralized system for managing requests.
- Company representatives also found it challenging to identify and thus best serve the audience for transparency reports. Some representatives felt that the audience was primarily NGOs and civil society groups or others such as journalists and academic researchers. Users of ICT company services were also identified as readers of transparency reports, though some company representatives expressed concern whether the content of transparency reports can be accessible and easily understood by a general audience.

## OPPORTUNITIES

Transparency reporting creates a number of opportunities for companies and governments to improve internal communication and effectiveness, in addition to building trust between one another and with external stakeholders. The reporting process itself helps educate people within governments and companies about what different parts of their organizations are doing, and the broader implications of their actions. Company reports showing the extent and range of government requests can also prompt better internal coordination among agencies of the same government.

Company-government interaction around transparency reporting creates other opportunities. These include companies working with governments to narrow the scope of requests being made (for example, in terms of the number of accounts affected, or the request's impact on users over whom the government in question has no jurisdiction). Officials from a number of countries reported that their governments were considering increased levels of transparency about requests

being made to companies through upcoming legislation and policy reviews.

Various opportunities emerged for companies to work with each other, 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. Some company representatives who are members of multi-stakeholder initiatives mentioned the importance of these groups in shaping their approach to transparency. Government officials also noted the value of dialogue with each other, companies, and other stakeholders on these issues.

Government and companies saw opportunities for broader education of the public. Company representatives highlighted the value of explaining to users their policies and process around government requests. Government officials also noted the need to educate citizens about these requests, as well as on why the government could not be transparent about all activities.

## RECOMMENDATIONS

We make the following preliminary recommendations based on our consultations. They complement existing and emerging principles and best practices in the field, as outlined in our full report.

### FOR GOVERNMENTS

*Establish clear policies and processes to make, and report on, requests made to companies.*

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. Governments should provide context about which laws, policies, or legal authorities are used to justify 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.

*Expand the scope of government reporting on requests to companies.*

No government has produced a comprehensive report on the requests it 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 legal authority to access personal information stored by companies or to restrict content. FOC governments are in a good position to consider what such reporting would entail, including the kinds of internal coordination necessary to compile reports and how best to present them to the public.

*Devote adequate resources and capacity for coordination.*

Governments should demonstrate and support their commitment to transparency by dedicating employee time and budget for reporting processes and other measures to inform citizens.

## 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. Multi-stakeholder organizations such as the Global Network Initiative are particularly good at facilitating this collaboration.

*Strengthen transparency about qualitative policies and processes as well as quantitative statistics about government requests.*

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

*Standardize transparency reporting.*

Currently, transparency reports differ so widely in their formats, scope, and approach that it is difficult to carry out comparative analyses that would facilitate policy recommendations and other solutions that would enhance the protection and respect for online freedom of expression and privacy. Companies should work with each other and with outside experts to develop industry-wide standards for transparency reports and other measures to boost sector-wide transparency about government requests.

*Devote adequate internal resources and coordination.*

Companies should reflect their commitment to transparency by dedicating employee time and budget for reporting and other measures to inform users.

*Make an executive-level commitment to transparency.*

Companies should make a high-level commitment to transparency and educate all parts of the company on how to design and implement transparent processes around government requests for user information or content restriction.

## AREAS FOR FUTURE RESEARCH

To date, the public debate on transparency has focused on the relationships and practices among U.S. and European companies and governments. In our further 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.

Through our consultations we identified the following areas for further work:

### *Qualitative transparency for companies and governments:*

While quantitative reports focused on numbers remain a cornerstone of transparency reporting, we should develop best practices for how 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 disclose? What information should government disclose? Are there reasons why companies or governments might believe that disclosing this information could have negative consequences?

### *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. Under what laws and authorities are citizens entitled to remedy from governments and/or companies? What do remedial processes entail, and who from governments and companies is involved? How can these be communicated to the public?

### *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?

### *Cooperation through indirect, informal, and extra-legal channels:*

To date the public debate – and this Group’s work – has focused on direct government requests to companies. There remains a great lack of transparency in other realms of government-company cooperation, such as self-regulatory and co-regulatory schemes for requests for user information or content restriction, and governments’ use of companies’ Terms of Service enforcement mechanisms. How can we improve transparency from governments and companies in these cases?

**Freedom Online Coalition Support Unit**

**GLOBAL PARTNERS DIGITAL**

Development House  
56-64 Leonard Street  
London EC2A 4LT  
+44 (0)20 7549 0336

**[freedomonlinecoalition.com](https://freedomonlinecoalition.com)**

