



Freedom Online Coalition
Working Group 3
Privacy and Transparency Online

Submission to UN Special Rapporteur David Kaye:
Study on Freedom of Expression and the Private Sector in the Digital Age

About the FOC Working Group on Privacy and Transparency Online

The Freedom Online Coalition Working Group on Privacy and Transparency Online 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. The Working Group is comprised of experts from governments, ICT companies, civil society and academia from across six continents.

Our Group was established as a multi-stakeholder forum under the auspices of the Freedom Online Coalition (FOC), a group of governments who have committed to work together to support Internet freedom and protect fundamental human rights worldwide. The Group supports FOC 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.

In our first year, we conducted research on transparency about government requests to ICT companies for user information and content restriction. We conducted consultations with companies and governments, focusing specifically on how the parties interact on issues related to law enforcement and national security. We examined the role of transparency as a tool for government and corporate accountability, and as a fundamental part of empowering individuals to fully exercise their rights online, including freedom of opinion and expression. We published a report in November 2015 outlining our findings and proposing recommendations for companies and governments. The report is attached to this submission and available at <https://www.freedomonlinecoalition.com>.

This Submission

In this submission, we articulate why transparency from ICT companies and governments is critical to empowering individuals to exercise their freedom of opinion and of expression. Drawing on our research, we highlight core elements of what it takes to be transparent in a way that is meaningful to individual users. Finally, we identify areas for further work in this field and preview future activities of this Group.

We encourage the Special Rapporteur to include transparency as a core component of his study of the ICT sector, and we hope that this submission and our accompanying report serve as a resource. The focus of this Group's research has been transparency about government requests to companies for user information and content restriction. Companies receive similar requests from private entities and individuals, and these can also implicate human rights. While requests from private entities are outside of the scope of our Group's work to date, we note that they raise transparency considerations that also require attention.

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

The Importance of Transparency

Individuals rely on information and communications technologies (ICTs) to express themselves and engage in their everyday activities, both personal and professional. As part of using ICT services, they provide personal information to companies and communicate publicly and privately over their platforms. They often have little awareness of the policies and processes that companies use to collect and manage their information.

Meanwhile, governments around the world make requests to ICT companies to provide information on individuals or restrict access to user-generated content. These requests arise frequently in legitimate law enforcement and national security contexts. A government official might request that a company share information on the identity of the user behind a given email account, if that individual is suspected to be involved in criminal or terrorist activity. A government official might request that an ICT company filter or remove illegal content that is accessible through that company's platform. These requests can come in the form of legal orders or through informal, indirect, and extra-legal channels.

These interactions can result in companies providing private information to governments, or restricting expression and access to information. Government requests, and the subsequent responses by companies, can therefore threaten the human rights of ICT users in certain contexts. Government officials may request information on an individual, or the restriction of access to content he or she produced, not because they are investigating a crime but because that person has criticized that government or is seen to pose a threat due to their race, religion, sexual orientation, or political affiliation. Officials may also ask an ICT company to restrict access to or search of content without going through that government's formal legal processes.

Due to the potential for these requests to circumvent due process protections, it is essential that both governments and ICT companies provide information to the public about these interactions. Individuals have insufficient information to understand how governments are invoking laws to make requests of companies for user information or content restriction. Affected users rarely have the information needed to understand how companies interpret these laws, and under what circumstances governments could access their data or restrict content. In some cases, companies are legally prohibited from publishing certain information or classes of information related to these requests. The scale of these requests in specific jurisdictions is also unknown.

Transparency about government requests to companies and the underlying policies and procedures facilitates oversight. Knowledge of government and corporate practice empowers civil society, investors, and other stakeholders to hold each party accountable to the expectations of users, international human rights norms, and commitments like the Tallinn Agenda. Transparency enables public debate on whether requests are being

made within frameworks that reasonably consider individual rights together with national security and law enforcement interests.

Transparency empowers individuals to make informed choices about the ICT services they use, and understand how they can use them safely. Citizens cannot understand how authorities access and control their information and content without disclosures by ICT companies and governments. With transparency, individuals can understand how communications surveillance and other laws are used in practice, how specific companies consider the human rights of their users when responding to disclosure or content restriction requests, and whether these requests are ever refused for failing to ensure respect.

There are legitimate reasons for governments to withhold information from the public for law enforcement and intelligence purposes, which we addressed in our report last year. The challenge is 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. As many companies and governments have demonstrated through adapting transparency policies over time, there is room for improvement and experimentation to increase disclosure while carrying out these important functions.

Enabling freedom of opinion and expression

Much of the debate over transparency in the ICT sector has focused on government requests to companies for user information, and their potential implications for privacy. Yet, transparency about how ICT companies receive, interpret, and process requests is equally critical to enabling freedom of opinion and expression.

A lack of transparency can cause a chilling effect. When individuals are unclear about what communications and information governments can access or restrict, they are less likely to feel safe speaking freely over those platforms in the first place. Transparency facilitates and enables freedom of expression by providing citizens with an accurate understanding of how their communications and data could be provided to or restricted by government officials. Citizens may not be fully empowered to exercise their right of freedom of opinion and expression without this understanding.

Without transparency, ICT company and government actions that implicate users' expression can go unexamined by the public. Requests from governments to ICT companies for content restriction can suppress an individual's speech and limit others' access to information. The majority of company transparency reports published today disclose numbers of government requests for user information, but not for content or search restriction. Likewise, while some governments issue reports on requests they have made to companies for user information, few governments we identified in our research report on content or search restriction requests.

Individual users do not have a good sense of the scope and nature of requests for content or search restriction taking place. Without more information from companies and governments, we cannot have a fully informed public debate on the implications for freedom of opinion and expression in this process.

Making Transparency Meaningful

In our report, we analyze the state of play of government and corporate efforts to disclose information about requests for user information and content restriction. We discuss challenges both parties face in designing transparency-related policies and practices, and opportunities to improve disclosure to the public. We refer

you to our report for an in-depth study of these topics based on our research and consultations with governments and ICT companies.

As we advocate for more transparency in the ICT sector, we must remember that improving transparency is not only about encouraging individual companies and governments to disclose more statistics. Information must be disclosed in a way that is beneficial and useful to the individual users whose rights are at stake.

Making transparency meaningful to individuals requires the following:

- *Government and company reporting:* Governments and companies must both report in order for individuals to have a complete picture of how their information is accessed or content is restricted. The combination of government and company reporting helps the public understand potential implications for human rights and averts misunderstandings about surveillance and content restriction. Meaningful transparency requires greater disclosure by both parties, as well as consistency among companies and governments on how they report on numbers, policies and practices.
- *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. For individuals to understand how their information is treated, they need more information on what laws, policies, and processes governments use to justify and execute these demands. They also need more information on how companies interpret government laws and policies, what internal processes they use to respond to requests, and what safeguards they have in place to protect user rights.
- *Accessibility and availability to a general audience:* Governments and companies should disclose information in a manner and format that is accessible to the average user. It is not sufficient for a company to disclose data without context for users to interpret the numbers. Likewise, it is not sufficient for governments to have reporting by law enforcement and intelligence agencies to oversight committees if these bodies are not allowed to disclose anything to the public. Both parties can reach a general audience by making information easily accessible, explaining the framework in which requests take place, and providing illustrative examples.
- *Disclosure of all forms of government requests:* Public debate has focused on transparency about direct government requests to ICT 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. Recognizing the potential human rights implications in these informal and extra-legal interactions, governments and companies should disclose more information about the nature and scope of these arrangements.

Future Activities of the Working Group

We strive to encourage companies and governments to be transparent in a way that empowers individuals with the information necessary to exercise their rights freely and safely online. In the coming year, the Group is pursuing a number of activities toward this goal:

- *Defining transparency:* We are developing a multi-stakeholder definition of what corporate and government transparency means from the user perspective. This framework will encompass

company and government reporting, and statistical reporting as well as the disclosure of laws, policies, and processes. We will open the draft definition to public comment.

- *Analysis of emerging issues:* We are launching a blog series looking at emerging issues related to transparency in the ICT sector. An initial area of focus is the rise of informal and extra-legal requests to companies related to concerns over terrorist use of the internet.
- *Policy development:* We are pursuing longer-term projects to address major research gaps on transparency and partner with governments and companies developing relevant policies and practices. Our initial focus is on developing models for more robust government transparency reporting, which we found to be an underdeveloped area in our research.

We welcome further engagement with the Special Rapporteur and collaboration with any initiatives and individuals working in these areas. To contact the Group, please email info@freedomonlinecoalition.com.