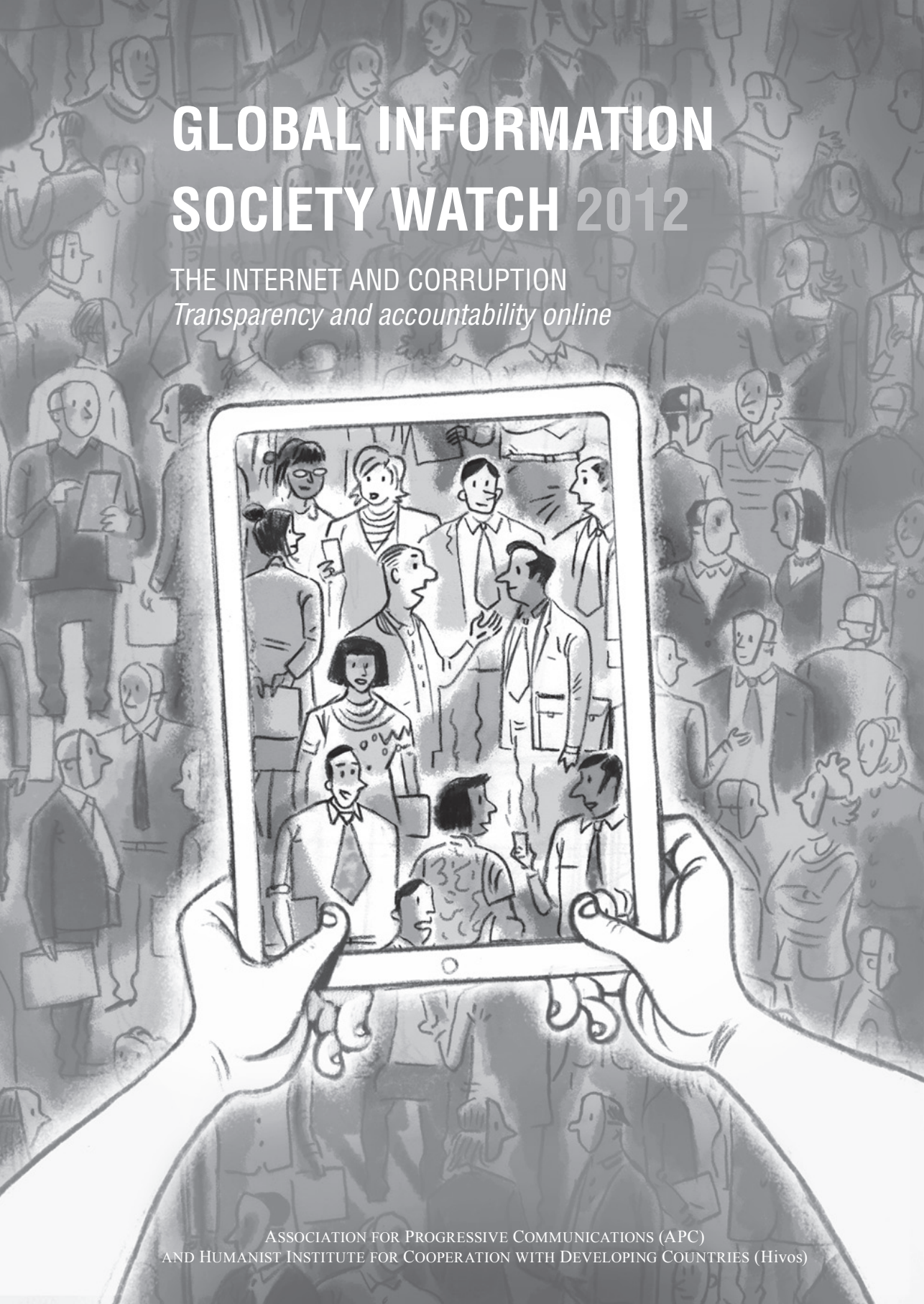
GLOBAL INFORMATION SOCIETY WATCH 2012

THE INTERNET AND CORRUPTION

Transparency and accountability online



ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)
AND HUMANIST INSTITUTE FOR COOPERATION WITH DEVELOPING COUNTRIES (Hivos)

Global Information Society Watch

2012

APC Hivos people unlimited

Steering committee
Anriette Esterhuysen (APC)
Loe Schout (Hivos)

Coordinating committee
Karen Banks (APC)
Monique Doppert (Hivos)
Valeria Betancourt (APC)

Project coordinator
Valeria Betancourt

Editor
Alan Finlay

Assistant editor
Lori Nordstrom

Publication production
Mallory Knodel

Proofreading
Valerie Dee
Lori Nordstrom

Graphic design
Monocromo
info@monocromo.com.uy
Phone: +598 2 400 1685

Cover illustration
Matías Bervejillo

Financial support provided by
Humanist Institute for Cooperation with Developing Countries (Hivos)
Swedish International Development Cooperation Agency (Sida)

Global Information Society Watch
Published by APC and Hivos
2012

ISSN: 2225-4625
ISBN: 978-92-95096-85-1
APC-201301-CIPP-R-EN-DIGITAL-176

Transparency reporting

James Losey and Grady Johnson
Open Technology Institute
www.opentechinstitute.org

Don't censor censorship: Why transparency is essential to democratic discourse

Introduction

As the internet has grown, so have the interpretations of how national laws should be applied and enforced. How governments and companies perceive their various roles in this debate has a direct impact on freedom of expression and privacy, and though their full extent remains unknown, today censorship of online content and the sharing of users' private data are established practices. It is how we approach this fact going forward that matters, and both governments and companies have a role to play in fostering an honest and informed conversation.

Every society must contend with questions around the sanctity of citizens' private information about what constitutes acceptable content. The goal of transparency is not to prescribe policy, but to create space for a democratic discussion of the trade-offs each society must ultimately make. As citizens and users, it is important to understand how and when our communications may be blocked or monitored, by whom and for what reasons.

Increasingly, those governments most eager to remove content and access users' private data are not "the usual suspects", but many Western democracies that concurrently support concepts of internet freedom. Ultimately, any policies with the potential to impact citizens' and users' rights to free expression and privacy must be subject to intense scrutiny. Transparency is essential to this process.

This report provides an overview of how some companies are already taking steps to be more transparent, and how these efforts can be expanded and improved upon. This includes a discussion about what types of companies should consider transparency reports, and the relevant data that should be reported. Finally, we discuss the role of governments and how they can support a democratic discussion of these issues.

Why transparency?

Internet companies operate in a complex legal environment and restrictions of content online can differ greatly between countries. For instance, the United States' (US) Digital Millennium Copyright Act requires the prompt and thorough removal of content deemed to infringe copyright – a process initiated not by the government but private actors. In India, the Information Technologies Rules require websites to block content that could be considered harmful, harassing, blasphemous, defamatory or libellous,[1] while Thailand's Computer Crimes Act is actively used to prosecute individuals and even website operators for content considered defamatory to the royal family.[2] How companies interpret local laws – and how and when they comply – can have profound implications for freedom of expression.

A company's terms of service can also impact heavily on users' rights. Beyond their legal requirements, companies act as *de facto* sovereigns of their piece of cyberspace – in her book, *Consent of the Networked*, Rebecca MacKinnon describes these online kingdoms by names like "Facebookistan" and "Googledom". The community guidelines for the popular blogging site Tumblr explicitly forbid users from posting content that is "harmful to minors" or "malicious bigotry".[3] Both Facebook[4] and Tumblr[5] have recently updated their policies to include content dedicated to self-harm and eating disorders. Despite their obvious impact on freedom of expression, there is little transparency around how companies craft these policies, or evaluate when and if violations have occurred.

1 www.mit.gov.in/sites/upload_files/dit/files/GSR314E_10511%281%29.pdf

2 See Tunsarawuth, S. and Mendel, T. (2010) Analysis of Computer Crime Act of Thailand, Centre for Law and Democracy, available at www.law-democracy.org/wp-content/uploads/2010/07/10.05.Thai_.Computer-Act-Analysis.pdf

3 www.tumblr.com/policy/en/community

4 www.facebook.com/communitystandards

5 www.bbc.co.uk/newsbeat/17195865

Companies are also under increasing pressure to release their users' data. These requests typically come from law enforcement agencies and can include a user's identity, their files or the contents of their communications. In 2011 alone, mobile phone providers in the US complied with 1.3 million requests for user data.[6] How companies make sense of these requests – and, crucially, when and if they comply – is a pivotal question.

The complex interplay between governments and companies in limiting freedom of expression and the right to privacy makes obvious the need for greater transparency. Law professor Derek Baumbauer argues that the "legitimacy of censorship is best judged by the process through which a state arrives at blocking decisions."[7] This question of how policies are developed and their impact in practice applies to the question of surveillance as well.

However, debates on how data is used or content is blocked should not take place in a vacuum. Indeed, as MacKinnon notes in her book, Google's intent on publishing their transparency report was to "start a conversation about censorship and surveillance."[8] While some might argue that there is no legitimate basis to surveil a conversation, others are willing to accept the practice under a certain bar of due process. The same can go for the blocking of content. In his report, Frank La Rue, the United Nations Special Rapporteur on the Right to Freedom of Opinion and Expression, outlined cases in which online content may be blocked, provided it meets specific criteria – including a sufficient measure of transparency.[9]

Transparency reporting mechanisms are a vital component for debating both the efficacy and validity of content censorship and lawful interception of communications in an open society. These reports can be published by both companies and governments.

Existing transparency reports

A handful of companies have already begun to publish transparency reports.[10] Google helped pioneer the practice, publishing their first semi-annual report in September 2010.[11] Since then, Sonic.net, SpiderOak, LinkedIn, Dropbox and now Twitter have all released statistics that can provide details on content removal and compliance with requests for user data.[12] While Google and Twitter (which operate internationally) have more expansive transparency reports, other companies' transparency reports contain innovative ideas worth noting.

Government removal of content

Twitter and Google both document government requests for the removal of content. These are typically divided between requests from law enforcement and court orders, and are further subdivided by country. Significantly, both companies also include their rate of compliance – that is, the percentage of times they complied with takedown notices versus those they refused. Google further breaks down the requests by product and reason.

Removal due to copyright claims

Both Twitter and Google document copyright-related takedown requests. Google's report cites the number of notices and the compliance rate, while Twitter also includes the number of users/accounts affected and the number of tweets removed. Neither specifies in which country the request originates.

Google first included content removed as a result of copyright claims in May 2012.[13] Its report reveals that Google receives thousands of copyright infringement notices on a weekly basis – between May-June 2012 alone, nearly two million URLS were requested to be removed from Google's search results. Significantly, Google does not include data on copyright removal requests for its other products like Blogger and YouTube. Twitter and Google both send copies of copyright takedown requests to the Chilling Effects Clearinghouse.[14]

Requests for user data

Several companies document government or court-ordered requests for user data, including Twitter, Google, Sonic.net, LinkedIn, SpiderOak and Dropbox. In its inaugural transparency report,

6 www.wired.com/threatlevel/2012/07/mobile-data-transparency/all

7 Bambauer lists four traits of "legitimate censorship": it is openly described, transparent about what it restricts, narrow in the material to which it applies, and accountable to the people it seeks to protect. Bambauer, D. E. (forthcoming) Orwell's Armchair, University of Chicago Law Review; Brooklyn Law School Research Paper No. 247, available at SSRN: ssrn.com/abstract=1926415

8 MacKinnon, R. (2012) *Consent of the Networked: The Worldwide Struggle for Internet Freedom*, p. 245.

9 www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

10 EFF discusses these in their report Who Has Your Back. Our intention is to provide more analysis and offer recommendations. www.eff.org/pages/who-has-your-back

11 mashable.com/2010/09/21/googles-transparency-report

12 To visit these transparency reports please visit:
Google: www.google.com/transparencyreport
Twitter: support.twitter.com/articles/20170002
Sonic.net: corp.sonic.net/ceo/2012/04/13/transparency-report
LinkedIn: help.linkedin.com/app/answers/detail/a_id/21733
SpiderOak: spideroak.com/blog/20120507010958-increasing-transparency-alongside-privacy
Dropbox: www.dropbox.com/transparency

13 googleblog.blogspot.com/2012/05/transparency-for-copyright-removals-in.html

14 www.chillingeffects.org/twitter, www.google.com/transparencyreport/removals/copyright/faq

Twitter documents requests for user data, total number of users impacted, and the percentage of requests complied with for 23 countries, while Sonic.net and SpiderOak publish data on requests within the US. LinkedIn publishes the number of requests received, member accounts impacted, and their compliance rate for five countries, including the US. Google also documents requests for user data, including the number of requests received per country (with some exceptions), the number of users/accounts associated with the requests, as well as the percentage that Google complied with. The data requests listed here refer only to criminal investigations.

Cloud services are particularly relevant with regards to user data requests. Dropbox documents how many times law enforcement requests data while Sonic.net subdivides these requests into civil subpoenas and law enforcement requests. Sonic.net also lists how much data was surrendered, including their rate of compliance. SpiderOak goes a step further and differentiates between federal law enforcement requests and state law enforcement requests. The company also lists how many court orders were issued, the number of times user data was surrendered, and the rate of compliance.

Additional transparency

Google includes real-time and historic traffic data in their transparency report, which can be used to document when services are not accessible in specific countries.[15] In one famous case, the data from Egypt in January 2011 was used to document the precipitous falls in traffic as the internet service providers were shut down, one at a time.

Often, companies are forbidden from informing their users that they have turned data over to law enforcement. In order to circumvent this, some companies have implemented a "warrant canary", an automated system telling users at regular intervals that their data has not been requested. If the canary falls silent, users should assume their data has been accessed.

Recommendations

Private industry

Copyright removal

Responding to copyright-related takedown notices is a unique challenge. This is by far the most common form of content removal, typically issued via private firms or individuals, and often involves interpreting complex questions of fair use and intellectual property rights. Further complicating the matter are the safe harbour provisions in laws like the Digital Millennium Copyright Act, which grants immunity to service providers provided they remove the offending content within 24 hours. The sheer volume of requests, coupled with such restrictive response times, is a recipe for overblocking. Indeed, it is a well-documented occurrence.[16]

Given this reality, our recommendations are three-fold. First, companies must formulate and publish their internal mechanisms for processing requests, including a clearly articulated appeals process for users who feel their content has been removed unfairly or by mistake. Second, a regular transparency report should document the number of takedown notifications, the amount of content included in each request, the rate of compliance, the number of users affected, and the number of removal requests published. Finally, reports should also cite from whom the request originated and under which law or laws the content has been challenged. Where possible, companies should include the URL or at least a brief description and categorisation of the content that has been removed.

Additionally, users should be notified (as far as is possible) that their content has been removed. "Users" in this case refers not just to the content owner, but all users – visitors should be presented with a visible notification when attempting to access the original content. One example is the suggested 451 error code, inspired by the book *Fahrenheit 451*.[17] Lastly, companies should publish the takedown requests through the Chilling Effects Clearinghouse or similar databases.

Faced with such an overwhelming number of takedown requests, companies are bound to make mistakes. The purpose of transparency is to give users the tools to detect them, and to provide an appropriate means of recourse when such accidents occur.

Government removal requests

Government removal requests take many forms, and any reporting should reflect this. Companies should first differentiate between requests that originate from government agencies and those from legal cases. Government agencies should be further subdivided into federal and local law enforcement – or any other state entities – and court-issued orders

15 www.google.com/transparencyreport/traffic/

16 www.openrightsgroup.org/blog/2012/new-reports-of-overblocking-on-mobile-networks

17 www.guardian.co.uk/books/2012/jun/22/ray-bradbury-internet-error-message-451

separated from informal requests (if such requests are to be honoured at all). Perhaps most importantly, reports should make clear the reason (citing any applicable laws) for the removal of content.

Without knowing the origin, justification and legal processes involved in a request, it is impossible to judge its validity. Speculating that Argentina blocks less content than say, Italy, invites only unfair comparisons. Equally important to the amount of content removed is the procedure through which requests are issued and processed.

As with copyright, whenever content is removed there must be ample notification. A "block page" or 451 error code is appropriate in this case and should include the relevant laws and agencies associated with the request.

Government requests for user data

Requests for user data are a complicated issue. Companies are obliged to cooperate with local governments, but they also have a responsibility to protect their users' privacy. Transparency in this case is not straightforward: several companies have made the case that publishing user data requests could threaten ongoing investigations.[18]

The solution here is first and foremost *procedural* transparency. Like governments, companies must have clearly articulated procedures for when and how they are allowed to access and share their users' private information. When this process has not been honoured, companies are obliged not to comply. Companies should further detail and publish what constitutes an unreasonable request, and make it policy to challenge such requests and any associated gag orders.

Companies should report on the number and type of requests, with at least a distinction between those with warrants and without. This data should then be divided by country and include the agency or agencies involved and any applicable laws. Included should be the compliance rate, as well as any legal challenges against unreasonable requests.

Unless specifically ordered otherwise, company policy should be to inform users that their data has been accessed. Some companies may also want to consider implementing a warrant canary system if they lack the legal resources to challenge unreasonable gag orders.

Governments

Governments can also play a crucial role in increasing transparency. By reporting on their own takedown and user data requests, governments have the opportunity to show their commitment to openness and also to corroborate reports from private industry.[19]

Governments should first create a public resource on the policies that allow the restriction of content online, or which government agencies are permitted to access the personal data or communications of citizens. Second, governments should track and publish statistics on all requests to block content or access user data. This is already partly in practice in many countries – in the US, courts release an annual document on all authorised wiretaps (with some exceptions). However, this report excludes other types of surveillance, like requests for user identities, communications history, messages and location tracking.[20] A complete report would document all such requests and classify them accordingly.

Finally, governments should contribute this information to a public database of all such requests. Currently, the Chilling Effects Clearinghouse serves as a repository for takedown requests, including copyright and parody,[21] and could be expanded to incorporate this new data.

Conclusion

Transparency is not a panacea for the abuse of human rights, nor do transparency reports alleviate companies and governments of fault when restricting freedom of expression. Governments and companies alike are well positioned to provide this debate with accurate and timely data supporting a democratic debate on policies that result in censorship and surveillance. Combined with scrutiny, transparency reports provide a necessary, but not sufficient, component of supporting internet freedom. ■

18 www.google.com/transparencyreport/userdatarequests/faq

19 One concept of this idea is outlined by Joakim Jardenberg in the Stockholm Principles. stockholmprinciples.org

20 www.uscourts.gov/Statistics/WiretapReports/WiretapReport2011.aspx, www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request

21 www.chillingeffects.org