Key Issues: Responding to State Attacks on Freedom of Expression

Many private sector intermediaries face the challenge of what to do when confronted by government demands which do not accord with international human rights standards. The responsibility to avoid complicity in human rights violations is a key part of the UN's Protect, Respect and Remedy framework:

> 73. The corporate responsibility to respect human rights includes avoiding complicity. The concept has legal and non-legal pedigrees, and the implications of both are important for companies. Complicity refers to indirect involvement by companies in human rights abuses – where the actual harm is committed by another party, including governments and non-State actors. Due diligence can help a company avoid complicity.
>
> 74. The legal meaning of complicity has been spelled out most clearly in the area of aiding and abetting international crimes, i.e. knowingly providing practical assistance or encouragement that has a substantial effect on the commission of a crime, as discussed in the 2007 report of the Special Representative. The number of domestic jurisdictions in which charges for international crimes can be brought against corporations is increasing, and companies may also incur non-criminal liability for complicity in human rights abuses. [references omitted][1]

How companies should respond to government demands which harm freedom of expression is the main issue the GNI focuses on. The GNI makes it clear that it does not expect companies to refuse to comply with domestic laws and instead focuses on engagement with governments to encourage them to adopt laws and policies which are in line with international freedom of expression standards. The GNI's Implementation Guidelines state that companies should require governments to follow established domestic legal processes when restricting freedom of expression and that companies should interpret any demands that such restrictions make on them in a manner which is minimally intrusive to freedom of expression. The GNI Implementation Guidelines also say that companies may legally challenge

[1] Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, 7 April 2008. Available at: www.reports-and-materials.org/sites/default/files/reports-and-materials/Ruggie-report-7-Apr-2008.pdf.

restrictions or demands which do not comport with human rights standards, but ultimately stresses that this decision lies at the discretion of the companies themselves:

> It is recognized that it is neither practical nor desirable for participating companies to challenge in all cases. Rather, participating companies may select cases based on a range of criteria such as the potential beneficial impact on freedom of expression, the likelihood of success, the severity of the case, cost, the representativeness of the case and whether the case is part of a larger trend.[2]

After the Snowden revelations, the Electronic Frontiers Foundation (EFF) withdrew from the GNI and developed its own, stronger and more specific set of standards regarding how companies operating in the United States should respond to government requests.[3] These standards hold that companies should only hand over user information when confronted by a legal warrant, should publish regular transparency reports on these requests and should publish guides which explain their internal procedures for responding to government requests. The EFF standards also ask companies to provide notice to users about a government request before it is responded to, when that is legally permitted. In cases where they are prohibited from informing the user right away, the EFF calls on companies to commit to notifying the user as soon as this is legally permitted.

Arabic Network for Human Rights Information

Egypt's Telecommunications Act does nothing to protect the privacy and personal data of Internet users, and instead is focused on guaranteeing that the authorities can access any information or data they desire. Article 64, for example, prohibits telecommunications service providers and users from using encryption systems in their conversations, and forces Internet service providers to provide the means necessary for national security bodies and the armed forces to obtain information about their users. Telecommunications companies in Egypt cannot get licenses without allowing the military and security services to access the personal data of their users, including to spy on political activists.

Vodafone, a company that provides telecommunications and Internet services in Egypt, publicly announced that Egyptian law allows the national security services and the military to conduct surveillance of communications, and disclosed that they were being forced to cooperate with the security services under Article 64 of the Telecommunications Act, as well as Article 95 of the Code of Criminal Procedure.

[2] Global Network Initiative, Implementation Guidelines for the Principles on Freedom of Expression and Privacy. Available at: globalnetworkinitiative.org/sites/default/files/GNI_-_Implementation_Guidelines_1_.pdf.

[3] These standards are available at: www.eff.org/who-has-your-back-government-data-requests-2015#best-practices. Although the standards focus primarily on data protection and privacy, they also deal with content removal requests.

The company also mentioned the existence of secret wires connected directly to its network and the networks of other mobile operators which allowed government agencies to eavesdrop and record conversations of users and, in some cases, track their whereabouts.

The Dynamic Coalition on Platform Responsibility (DCPR), in its *Recommendations on Terms of Service and Human Rights*, suggests that companies should only comply with requests which are grounded in a "legitimate" law or regulation, defined as follows:

> Laws and regulations are procedurally legitimate when they are enacted on the basis of a democratic process. In order to be regarded also as substantively legitimate, they must respond to a pressing social need and, having regard to their impact, they can be considered as proportional to the aim pursued.
> (a) It must be provided by law, which is clear and accessible to everyone (principles of predictability and transparency);
> (b) It must pursue a legitimate purpose (principle of legitimacy); and
> (c) It must be proven as necessary and the least restrictive means required to achieve the purported aim (principles of necessity and proportionality).
> If it is manifest that the measure would not pass this three-pronged test, the platform operator should deny the request and, to the extent possible, challenge it before the relevant court. [references omitted][4]

Christopher Parsons

In 2012, Google began warning a subset of its users that they might be the targets of State-sponsored attacks by inserting a warning notification at the top of their screens when they log into Google services. Google is well situated to analyse such attacks and provide the warnings because of the company's ability to analyse and investigate incoming malware and phishing attacks. Facebook also started issuing similar warnings as of October 2015. The notifications from these companies are important because few individuals are able to understand whether a particular phishing, spearphishing or malware attack originates from a commercial, State or other actor. Moreover, the warnings can help individuals to correlate other abnormal activities with a similar threat actor or set of actors. In effect, these companies' investigations and warnings can help individuals realise the threats facing them and subsequently try to adjust their behaviour to reduce their risks.

However, these notifications systems also highlight that the precise methodologies that are used to determine who is responsible for an attack are not well publicised. The heuristics or analysis or investigatory techniques that go into determining whether an attack is State sponsored thus cannot be directly analysed and validated

[4] "Recommendations on Terms of Service and Human Rights", Dynamic Coalition on Platform Responsibility. Available at: review.intgovforum.org/igf-2015/dynamic-coalitions/dynamic-coalition-on-platform-responsibility-dc-pr/.

(or refuted) by the broader security community. Further, the notices do not indicate which country is engaged in these sorts of sponsored attacks, or whether US-based companies would notify individuals of a US government-sponsored attack or just of attacks sponsored by foreign governments. Notably, the attacks that Google and Facebook alike notify users about are limited to 'hacking' attempts; subscribers whose data is requested using a lawful access tool do not receive notifications. The result is that even the 'best of breed' analysis and investigation systems that inform specifically affected subscribers have significant deficits.

Beyond notifying specific individuals that they have been targeted by a State actor using malware or other attack tools, companies can try and notify individuals whose data is requested by such agencies. Subscribers rarely learn of requests to access their data by government agencies, unless they are subsequently charged with an offence. As a result, their personal information can be captured by government agencies, and used or disseminated amongst such agencies, entirely without their consent or even knowledge. And, where a charge is not brought against the individual, they may never have an opportunity to contest the legitimacy of the government possessing - or having requested - the information in the first place. Only private sector intermediaries are in a position to know whether a subscriber's information has been requested. As a result, a powerful way for private sector intermediaries to facilitate transparency surrounding State-driven surveillance is to commit to informing subscribers about such requests.

Some of the most challenging cases of private sector complicity in human rights violations involve China, which has an abysmal freedom of expression record as well as a large and rapidly growing population of Internet users. The country has been particularly bold in taking action against companies that refuse to acquiesce to their demands, including by blocking them from the lucrative Chinese market.

In addition to complying with censorship demands associated with China's "Great Firewall", there have been allegations that major tech firms were directly complicit in assisting the Chinese State to prosecute journalists.[5] There have even been instances of private sector actors being utilised as weapons of cyber war. In March 2015, reports emerged of an enormous distributed denial of service (DDoS) attack being mounted against GitHub, a website which, among other projects, provides access to tools to subvert China's censors.[6] Analysis of the attack revealed that it originated from servers of the popular Baidu search engine, redirecting users of the

[5] Joseph Kahn, "Yahoo helped Chinese to prosecute journalist", The New York Times, 8 September 2005. Available at: www.nytimes.com/2005/09/07/business/worldbusiness/07iht-yahoo.html.
[6] Sebastian Anthony, "GitHub battles 'largest DDoS' in site's history, targeted at anti-censorship tools", Ars Technica, 30 March 2015. Available at: arstechnica.com/security/2015/03/github-battles-largest-ddos-in-sites-history-targeted-at-anti-censorship-tools/.

site to participate in the attack against GitHub, although Baidu strenuously denied complicity.[7]

Although China is the most high profile example, companies face similar dilemmas in other countries. Both Twitter and Facebook have faced substantial criticism for removing content in Pakistan,[8] while telecoms companies operating in Ethiopia have faced scrutiny for facilitating the country's invasive surveillance and censorship programmes.[9] Moreover, abusive government demands can also be made in free and open democracies. In 2010, Amazon, a major United States-based web hosting company, cut off the Wikileaks website from its platform after a United States Senator complained directly to them about Wikileaks' disclosures.[10] The United States-led mass surveillance programmes, which relied heavily on private sector intermediaries, are another example of an abusive practice taking place in a developed democracy. This also demonstrates the secrecy in which even pervasive systems can operate. It is safe to assume that for every well-publicised case of an intermediary acquiescing to State demands which violate the rights of their users there are many more which pass under the radar screen.

Ultimately, Google is not responsible for bringing democracy to China and Twitter is not responsible for promoting tolerant secularism in Pakistan. However, private sector intermediaries do have a duty to avoid complicity in abuses carried out by the governments of the countries where they operate. Ideally, these considerations should begin with a human rights impact assessment before a new market is entered, or a new product is launched. Private sector intermediaries should develop strategies to mitigate any risks identified, for example by disabling particular features which may be prone to misuse in a particular national context or by avoiding locating their employees or storing data in countries which have a poor record of respecting freedom of expression or the right to privacy.

No government, of course, has a perfect human rights record. What constitutes a legitimate restriction on freedom of expression is complex and different countries have different rules in areas such as privacy, obscenity, defamation, hate speech and so on. As a result, by and large, it is reasonable to expect private sector

---

[7] Bill Marczak and Nicholas Weaver, "China's Great Cannon", Munk School of Global Affairs, 10 April 2015. Available at: citizenlab.org/2015/04/chinas-great-cannon/.

[8] Robert Mackey, "Twitter Agrees to Block 'Blasphemous' Tweets in Pakistan", The New York Times, 22 May 2014, available at: www.nytimes.com/2014/05/22/world/asia/twitter-agrees-to-block-blasphemous-tweets-in-pakistan.html?_r=2; and Declan Walsh and Salman Masood, "Facebook Under Fire for Temporarily Blocking Pages in Pakistan", The New York Times, 6 June 2014, available at: www.nytimes.com/2014/06/07/world/asia/pakistan-facebook-blocked-users-from-political-pages-and-outspoken-rock-band-laal-against-taliban-.html?_r=1.

[9] Arvind Ganesan, "They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia", Human Rights Watch, 25 March 2014. Available at: www.hrw.org/report/2014/03/25/they-know-everything-we-do/telecom-and-internet-surveillance-ethiopia.

[10] Ewen MacAskill, "WikiLeaks website pulled by Amazon after US political pressure", The Guardian, 2 December 2010. Available at: www.theguardian.com/media/2010/dec/01/wikileaks-website-cables-servers-amazon.

intermediaries to comply with local laws on these issues in the jurisdictions where they operate, even if those laws may deviate from international human rights standards. For example, Canada has a criminal defamation law on the books, which includes possible prison terms. This runs counter to international human rights standards, which hold that defamation should be treated as a civil, rather than a criminal, matter and that imprisonment is never a legitimate response to defamation. However, if a Canadian judge authorised a warrant for user information related to a criminal defamation investigation, it seems reasonable to expect an intermediary to comply with the order. On the other hand, one would hope that a similar request in Azerbaijan, where the government is notorious for using criminal defamation laws to target journalists and other critical voices, might raise a red flag.

Although the line can be difficult to draw, where an intermediary encounters a case of their systems or services being subverted to support a clear and grave violation of human rights, they have a responsibility to take action to avoid or mitigate complicity. This can include refusing to turn over records that support a political prosecution or to participate in widespread systems of repression, such as China's Great Firewall. It is worth noting that most global tech companies only maintain a physical presence in a few countries. Outside of those States, governments have no real legal means to compel compliance with their demands, other than by threatening to deny the company access to their market. Twitter, for example, only has assets or employees in the United States, the United Kingdom, Ireland, Japan and Germany, so the government of Pakistan would have no power to seize their property or jail their employees. The only possible sanction that Twitter would face for failing to obey an order of the Pakistani government would be to be blocked in that country.

Open Net Korea

South Korea has a vast State surveillance system over the Internet, which was brought to the public's attention by a major civil society lawsuit. Domestic companies' policy of demanding real names from new users, along with their resident registration numbers, exacerbated this by making accounts easily traceable. As a result, South Korean users began to switch from domestic private sector intermediaries to foreign ones outside the reach of South Korean warrants. Similarly, when the Prosecutors' Office announced plans to search and seize messages from Kakao Talk, the leading chat app in South Korea, for the purpose of investigating defamation of public officials, users began migrating to the foreign chat app Telegram, which provides device-to-device encryption. As the exodus grew, DAUM-KAKAO, the operator of Kakao Talk, announced in October 2014 that it would no longer comply with any wiretap order on chat messages, citing technical challenges with fulfilling the requests for real-time information. Although the exodus itself was not directly related to wiretap orders, consumer privacy concerns were appeased by this publicity stunt, along with two actual shifts in policy, namely

that Daum-Kakao began publishing the country's first transparency report on surveillance requests and takedown requests and also began offering the option of device-to-device encryption. This led to its competitor Naver following suit. A year later, when their market position had stabilised, Daum-Kakao's non-compliance policy was retracted.

Being shut out of a country is obviously not a consequence to be taken lightly, given the very real commercial implications this has. And acting ethically with that result may not be very useful in practice, since the company's market share may simply be taken over by less scrupulous competitors. However, where clear abuses of human rights are involved, companies cannot simply wash their hands of complicity any more than merchants selling conflict diamonds can. If the major players put up a unified front in support of human rights, it would be difficult for a country to ban them all (although China may be an exception to this, due to the size of its internal market and its capacity to replace services with home-grown versions). This would also send a powerful message to users that companies are willing to defend their interests. Relevant factors to take into account when determining whether a violation is significant enough to warrant noncompliance with domestic law include the number of users impacted, the severity of the interference, and the broader human rights context in which the interference takes place, including the country's overall human rights record.

Where a State-mandated interference does not qualify as a clear and grave violation of human rights, private sector intermediaries should only hand over information when subject to a legal requirement to do so and should notify users who are subject to a government request as soon as this is legally allowed. Where realistic legal avenues for contesting problematic laws or policies exist, private sector intermediaries have some responsibility to launch legal challenges in appropriate cases and to stand up for the rights of their users. Private sector intermediaries should additionally explore their options for seeking external leverage to support their position, such as soliciting diplomatic support from their home government (particularly if they are based in the United States) or from intergovernmental organisations. In seeking to mobilise against problematic policies, it may be important for intermediaries to liaise with one another and communicate clearly, in order to establish a unified front.

Stand Up For Digital Rights

Recommendations for Responding to State Attacks on Freedom of Expression:

Assessing Risks

- **Intermediaries should carry out thorough human rights impact assessments before making any significant changes that could impact human rights, such as the launch of a new product or entry into a new market, and develop strategies to mitigate any identified risks.**

Communicating With Users

- **Intermediaries should publish guides which explain their internal procedures for responding to requests for them to take action, including by providing information on users, from State actors.**
- **Intermediaries should offer specific guidance to human rights activists, or other oppressed groups, among their user base in countries where specific threats to these groups exist.**

Pushing Back

- **Intermediaries should only hand over user information when legally required to.**
- **Intermediaries should notify users who are the subject of a request from a State actor as soon as they are legally allowed to.**
- **Intermediaries should explore reasonable other avenues to push back against demands from State actors which violate human rights, including seeking diplomatic support from their home governments and intergovernmental organisations and partnering with other intermediaries in order to present a united front against problematic laws, policies or practices.**
- **Intermediaries should, in appropriate cases and where these have a realistic chance of success, pursue legal options to contest abusive laws or policies and support advocacy to change oppressive laws or policies.**

- **In more extreme cases of clear and grave violations of human rights, intermediaries should consider their options carefully, including refusing to obey even legal orders to act which would implicate them in serious human rights abuses and stopping operations in countries where their operations lead to them being complicit in serious abuses.**