GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

Intermediary liability and state surveillance

Elonnai Hickok
Centre for Internet and Society (CIS) India
www.cis-india.org

Introduction

On 30 June 2014, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights (OHCHR) was published.[1] The Report recognises the relationship between service providers and surveillance and the increasing trend of privatised surveillance, noting:

> There is strong evidence of a growing reliance by Governments on the private sector to conduct and facilitate digital surveillance. On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata. This process is increasingly formalized: as telecommunications service provision shifts from the public sector to the private sector, there has been a "delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of 'self-regulation' or 'cooperation'".[2]

This report will explore how legal requirements, practices and policies pertaining to intermediary liability are feeding into this growing trend through the incorporation of requirements for intermediaries that facilitate surveillance. In doing so, this report will explore aspects of intermediary liability policies and practices, and how these pertain to and enable state surveillance. Lastly, the report will look at gaps that exist in policies pertaining to privacy, surveillance and intermediary liability.

Intermediaries and privacy

Online communications, interactions and transactions are an integral component of our everyday lives. As such, intermediaries – including, though not limited to, search engines, social networks, cyber cafés, and internet and telecommunication service providers – play a critical role with respect to user privacy. As individuals utilise intermediary platforms on a daily and routine basis, from searching for information on the internet, to posting updates to a social media account, to using voice-over-internet-protocol (VoIP) services to connect with friends and colleagues, or using the services of a cyber café, intermediaries host, retain and have access to vast amounts of personal data of their users across the world, irrespective of jurisdiction. In this context, company practices and a country's legal regulations have a far-reaching impact on the rights – specifically privacy and freedom of expression – of both national and foreign users.

Intermediaries, governments and surveillance

The Right to Privacy in the Digital Age also notes that the internet and associated technologies allow governments to conduct surveillance on an unprecedented scale. This was highlighted by the revelations by Edward Snowden, which demonstrated the scope of access that the United States (US) government had to the data held by internet companies headquartered in the US. The revelations also underscore the precarious position that companies offering these services and technologies are placed in. Though the scope and quantity of data collected and held by an intermediary vary depending on the type of intermediary, the services offered and the location of its infrastructure, governments have recognised the important role of intermediaries – particularly in their ability to assist with state surveillance efforts by providing efficient access to vast amounts of user data and identifying potentially harmful or threatening content. Within this, there is a shift from reactive government surveillance that is based on a request and authorised order, to partially privatised surveillance, with companies identifying and reporting potential threats, retaining information, and facilitating access to law enforcement. Indeed, the OHCHR in the Right to Privacy in the Digital Age notes that the surveillance revealed by Snowden was facilitated in part

1 www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

2 Ibid.

by "strategic relationships between Governments, regulatory control of privacy companies, and commercial contracts."[3]

Intermediary liability and state surveillance

As described by the US-based Center for Democracy and Technology,[4] intermediary liability relates to the legal accountability and responsibility that is placed on intermediaries with respect to the content that is hosted and transmitted via their networks and platforms. Specifically, intermediary liability addresses the responsibility of companies with respect to content that is deemed by the government and/or private parties to be objectionable, unlawful or harmful. The Center for Democracy and Technology points out that, depending on the jurisdiction, intermediary liability requirements and provisions can be used to control illegal content online, but also can be misused to control legal content as well. As described by UK-based Article 19, provisions relating to intermediary liability can be broken down into three basic models: strict liability, where intermediaries are fully liable for third-party content; safe harbour, where intermediaries can be provided immunity from liability by meeting defined requirements; and broad immunity, where intermediaries are given immunity for third party content.[5] As pointed out by Frank La Rue in the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, legal frameworks that hold intermediaries (rather than the individual) liable for content, transfer the role of monitoring the internet to the intermediary.[6] Some jurisdictions do not have specific legal provisions addressing intermediary liability, but do issue court or executive orders to intermediaries for the restriction of content, as well as placing obligations – including technical obligations – on service providers via operating licences.

Legal provisions and orders pertaining to intermediary liability are not always limited to removing or disabling pre-defined or specified content. Requests for the removal of content can be accompanied with requests for user information – including IP address and basic subscriber information. Some jurisdictions, such as India, have incorporated retention mandates for removed content and associated information in legal provisions addressing intermediary liability.[7] Other jurisdictions, like China, require service providers to have tracking software installed on their networks, collect and retain user identification details, monitor and store user activity, report illegal activity to law enforcement, and have in place filtering software to restrict access to banned websites.[8]

Some jurisdictions are also recognising that the traditional means of seeking information from intermediaries are inefficient and often slow – particularly if the intermediary is foreign, and accessing information requires the government to follow a Mutual Legal Assistance Treaty (MLAT) process.[9] Perhaps in response to challenges posed by jurisdiction, some governments have sought "collaborations" with intermediaries to restrict illegal and offensive speech as well as identify perpetrators of the same. For example, in 2007 in India, the Mumbai Police negotiated with Google to establish a "direct line of contact"[10] with the company, which, according to news items, would allow access to IP addresses of users posting "objectionable" content on Google's social networking site, Orkut.[11] Such collaborations combine elements of intermediary liability and surveillance, and can be prone to misuse if they lack apparent oversight, legislative grounding or accountability. In this context, intermediary liability is not only about content online, but also encompasses the collection and disclosure of data associated with that content and of users producing and viewing such content.

3 Ibid.

4 https://cdt.org

5 Article 19. (2013). *Internet Intermediaries: Dilemma of liability*. London: Article 19. www.article19.org/data/files/Intermediaries_ENGLISH.pdf

6 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, 17 April 2013. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

7 The Information Technology (Intermediaries Guidelines) Rules, 2011, Rule 3(4). deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf

8 Frydnamm, B., Hennebel, L., & Lewkowicz, G. (2007). *Public Strategies for Internet Co-Regulation in the United States, Europe, and China*. Brussels: Université Libre de Bruxelles. www.philodroit.be/IMG/pdf/BF-LH-GL-WP2007-6.pdf

9 Mutual Legal Assistance Treaties are formal agreements reached between governments to facilitate cooperation in solving and responding to crimes. A critique of the MLAT process has been that it is slow and inefficient, making it a sub-optimal choice for governments when faced with crimes that demand immediate response. For more information see: Kindle, B. (2012, February 14). MLATS are powerful weapons in financial crime combat, even for private sector. *Association of Certified Financial Crime Specialists*. www.acfcs.org/mlats-are-powerful-weapons-in-counter-financial-crime-combat-even-for-private-sector Some intermediaries, such as Facebook, have specified that foreign governments seeking user account data must do so through the MLAT process or letters of rogatory. For more information see: https://en-gb.facebook.com/safety/groups/law/guidelines

10 Pahwa, N. (2007, March 14). Updated: Orkut to Share Offender Data With Mumbai Police; Google's Clarification. *Gigaom*. gigaom.com/2007/03/14/419-updated-orkut-to-share-offender-data-with-mumbai-police-googles-clarifi

11 Chowdhury, S. (2014, July 30). Mumbai Police tie up with Orkut to nail offenders. *The Indian Express*. archive.indianexpress.com/news/mumbai-police-tie-up-with-orkut-to-nail-offenders/25427

Types of content and surveillance measures

Certain types of content – namely child pornography/adult content, national/cyber security and copyright – can attract greater obligations on the intermediary to proactively facilitate surveillance and in some cases take on the role of law enforcement or the judiciary. The degree to which such obligations are backed by legal provisions varies and can range from statutory requirements, to policy initiatives, to forms of collaboration between governments, intermediaries, and self-regulatory organisation. The types of obligations and measures also vary.

Reporting of illegal content: Some of these measures are focused on the reporting of illegal or prohibited content. For example, in the US, by law, service providers must report to law enforcement any and all information with regards to child pornography. This is mandated by the Protection of Children from Sexual Predators Act, 1998.[12] Similarly, in India, under the rules defining procedural safeguards for intermediary liability, intermediaries must report cyber security incidents and share related information with the Indian Computer Emergency Response Team.[13]

Voluntary disclosure of illegal content and activity: Other measures support the voluntary disclosure of identified illegal content and activity and associated information to law enforcement. For example, under the 2002 Cyber Security Enhancement Act in the US, law enforcement can encourage service providers to reveal information pertaining to an "emergency matter". The Act further provides the service provider immunity from legal action if the disclosure was made in good faith with the belief that it was a matter of death or serious physical injury.[14]

Databases of repeat offenders: Requirements that governments are seeking to impose on service providers may also directly conflict with their obligations under national data protection standards. For example, in the context of proposed legal requirements for identifying and preventing copyright offenders under the UK Digital Economy Act, in a public statement, the service provider TalkTalk noted that the company would be required to maintain a database of repeat offenders – an action that might be illegal under the UK Data Protection Act.[15] As of July 2014, service providers, rights holders and the government have developed a form of collaboration where rights holders will "track" the IP addresses of suspected offenders. The addresses will be shared with the applicable UK service provider, who will then send a series of warning notices to the user.[16] This system is potentially dangerous as it allows for proactive monitoring of individuals' IP addresses by private parties (the rights holders) and then subsequent action by another private entity (the service provider). At no point does this system define or envision safeguards, accountability or oversight mechanisms.[17]

Measures that facilitate surveillance: Other requirements do not directly impose surveillance obligations on service providers, but can facilitate surveillance. For example, in the UK, service providers must now offer broadband filters for "adult content" automatically switched on. Users who do not wish to have the filter on are required to "opt out" of the filter.[18] These measures can make it easy to track and identify which user is potentially viewing "adult content".

Types of intermediaries and surveillance measures

Depending on services offered and jurisdiction, intermediaries can be subject to differing types and scopes of surveillance requirements. For example:

Cyber cafés: In jurisdictions like India,[19] cyber cafés are faced with legal requirements that can facilitate surveillance – such as the collection and retention of government-issued user identification, retention of user's browser history, and provision of assistance to law enforcement and other authorities when required. Cyber cafés are also strictly subject to the laws of the jurisdiction of operation.

Service providers: Similarly, service providers, even when multinational, must abide by the laws where they are operating. Unlike intermediaries such as multinational social networks or search engines, service providers are subject to the requirements found in operating licences that pertain to intermediary liability and surveillance. For example, in India, internet and telecommunication service providers are required to take "necessary measures to prevent objectionable, obscene, unauthorised,

12 Frydnamm, B., Hennebel, L., & Lewkowicz, G. (2007). Op. cit.

13 Information Technology (Intermediaries Guidelines) Rules 2011, Rule 9. deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf

14 Frydnamm, B., Hennebel, L., & Lewkowicz, G. (2007). Op. cit.

15 Jackson, M. (2014, July 19). Update: UK ISPs Agree Voluntary Internet Piracy Warning Letters Scheme. ISPreview. www.ispreview.co.uk/index.php/2014/07/big-uk-isps-agree-voluntary-internet-piracy-warning-letters-scheme.html

16 Ibid.

17 Jackson, M. (2013, August 9). UK Government to Finally Repeal ISP Website Blocking Powers. *ISPreview*. www.ispreview.co.uk/index.php/2013/08/uk-government-to-finally-repeal-isp-website-blocking-powers.html

18 Miller, J. (2014, July 23). New broadband users shun UK porn filters, Ofcom finds. *BBC*. www.bbc.com/news/technology-28440067

19 Information Technology (Guidelines for Cyber Cafe) Rules 2011, Rule 4, Rule 5, Rule 7. ddpolice.gov.in/downloads/miscelleneous/cyber-cafe-rules.pdf

or any other content, messages, or communications infringing copyright, intellectual property etc. in any form, from being carried on [their] network, consistent with the established laws of the country." Furthermore, if specific instances of infringement are reported by enforcement agencies, the service provider must disable the content immediately.[20] In the case of India, requirements for the provision of technical assistance in surveillance and retention of call detail records[21] and subscriber information are also included in the operating licences for service providers.[22]

Social networks: Social networks such as LinkedIn, Facebook and Twitter – which are often multinational companies – are not necessarily subject to the legal intermediary liability requirements of multiple jurisdictions, but they are frequently faced with requests and orders for user information and removal of content requests. To address these pressures, some companies filter content on a country basis. In June 2014 LinkedIn was criticised in the media for complying with orders from the Chinese government and filtering content in the region.[23] Similarly, Twitter was criticised by civil society for withholding content in Russia and Pakistan in May 2014, though in June 2014 the company reversed its decision and reinstated the withheld content.[24] Social media platforms are also frequently and increasingly used by law enforcement and the state for collecting "open source intelligence".[25]

20 Licence Agreement for Provision of Unified Access Services After Migration from CMTS, Section 40.3. www.auspi.in/policies/UASL.pdf

21 Call record details consist of information about a subscriber's use of mobile and broadband networks and can include: called numbers, subscriber name and address, date and time of the start and end of a communication, type of service used (SMS, etc.), international mobile subscriber identity, international mobile equipment identity, location details. For more information see: Afentis Forensics, "Telephone Evidence: Mobile telephone forensic examinations, Billing Records, Cell Site Analysis". afentis.com/telephone-evidence

22 Licence Agreement for Provision of Unified Access Services After Migration from CMTS, Section 41.10. www.auspi.in/policies/UASL.pdf

23 Mozur, P. (2014, June 4). LinkedIn Said it Would Censor in China. Now That It Is, Some Users are Unhappy. *The Wall Street Journal*. blogs.wsj.com/chinarealtime/2014/06/04/linkedin-said-it-would-censor-in-china-now-it-is-and-some-users-are-unhappy

24 Galperin, E., & York, J. (2014, June 23). Twitter Reverses Decision to Censor Content in Pakistan. *Electronic Frontier Foundation.* https://www.eff.org/deeplinks/2014/06/twitter-reverses-decision-censor-content-pakistan

25 Open source intelligence has been widely recognised as an essential tool for law enforcement and security agencies. Open source intelligence is derived from information that is publicly available from sources such as the internet, traditional media, journals, photos, and geospatial information. For more information see: Central Intelligence Agency. (2010, July 23). INTellingence: Open Source Intelligence. *Central Intelligence Agency.* https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html

Technology, intermediary liability and state surveillance

When intermediaries implement legal requirements for the blocking or filtering of content, they do so by employing different techniques and technologies such as key word filtering software, firewalls, image scanning, URL databases, technologies that enable deep packet inspection, etc.[26] Similarly, complying with legal mandates for interception or monitoring of communications also requires intermediaries to install and use technology on their networks. As pointed out by La Rue, technologies used for filtering also facilitate monitoring and surveillance as they have the ability to identify and track words, images, websites and types of content, as well as identify individuals using, producing or associated with the same.[27] For example, YouTube offers copyright holders the option of YouTube's "Content ID" system to manage and identify their content on the platform. Actions that copyright owners can choose from include muting audio that matches the music of copyrighted material, blocking a video from being viewed, running ads against a video, and tracking the viewer statistics of the video. These options can be implemented at a country-specific level.[28]

Removing the service provider from surveillance

While some governments are placing obligations on intermediaries to assist with surveillance, other governments are removing such obligations from service providers through surveillance measures that seek to bypass service providers and allow governments and security agencies to directly intercept and access information on communication networks, or measures that require service providers to allow security agencies a direct line into their networks. For example, India is in the process of implementing the Central Monitoring System, which is envisioned to allow security agencies to directly intercept communications without the assistance of service providers. Though this system removes obligations on service providers to assist and be involved in specific instances of surveillance, it also removes a potential safeguard – where

26 Bloxx. (n/d). *Whitepaper: Understanding Web Filtering Technologies*. www.bloxx.com/downloads/US/bloxx_whitepaper_webfilter_us.pdf

27 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, 17 April 2013. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

28 YouTube, "How Content ID Works". https://support.google.com/youtube/answer/2797370?hl=en

service providers can challenge or question extra-legal or informal requests for surveillance. In the 2014 Vodafone Law Enforcement Disclosure Report, the company notes that in select countries, law enforcement and authorities have direct access to communications stored on networks.[29]

The question of jurisdiction

Jurisdiction and the applicability of local law is a tension that arises in the context of intermediary liability and surveillance. Some facets of this tension include: to what extent do legal restrictions on content apply to multinational platforms operating in a country? To what extent can states access the communications passing or being stored in its territory? And to what extent do domestic protections of fundamental rights – including freedom of expression and privacy – apply to foreigners as well as nationals? The OHCHR in The Right to Privacy in the Digital Age shed some light on these questions, drawing upon a number of international instruments and firmly asserting that any interference with the right to privacy must comply with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individual.[30] Tensions around mass surveillance of foreign citizens and political leaders, and a lack of legal constructs domestically and internationally to address these tensions, have led to questions of direction and the future of internet governance – discussed at forums like NETmundial, where principles relating to surveillance and intermediary liability were raised.[31] Similarly, in March 2014, the US announced plans to relinquish the responsibility of overseeing the body tasked with regulating internet codes and numbering systems. This move has raised concerns about a backlash that could result in the division and separation of the internet, facilitating mass surveillance and content control.[32]

State surveillance and intermediary liability: The impact on the user and the role of the company

Government-initiated content restrictions and surveillance of individuals' online communications, transactions and interactions have widely been recognised as having a negative impact on users' right to privacy and a chilling effect on freedom of speech. Depending on the target and reasons, such actions by governments can have deeper human rights implications – if, for example, dissenting voices, activists and journalists are targeted. The gravity and clear human rights implications of actions related to intermediary liability and surveillance highlight the complexity of these issues. Numerous cases exist of individuals being identified and persecuted for speech shared or communicated online, and the identification of these individuals being facilitated by internet companies. For example, Yahoo! has been heavily criticised in the international media for providing the Chinese government in 2006 with user account details and the content of communications of political dissident and journalist Shi Tao – allowing police to identify and locate Shi and subsequently imprison him for ten years.[33] Instances such as the Shi Tao case demonstrate the complexity of issues related to intermediary liability and surveillance and raise questions about reasonable expectations regarding internet company practices and responses (particularly multinational companies), adequate national legislation, international guidelines, and appropriate public response. As noted in The Right to Privacy in the Digital Age, "the Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011, provide a global standard for preventing and addressing adverse effects on human rights linked to business activity. The responsibility to respect human rights applies throughout a company's global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations." This is a high standard that intermediaries must adhere to. Some companies such as Google,[34] Facebook,[35]

29 www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

30 Report of the Office of the United Nations High Commissioner for Human Rights: The Right to Privacy in the Digital Age, 30 June 2014. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

31 Powles, J. (2014, April 28). Big Business was the winner at NETmundial. *wired.co.uk*. www.wired.co.uk/news/archive/2014-04/28/internet-diplomacy-netmundial

32 Kelion, L. (2014, April 23). Future of the Internet Debated at NetMundial in Brazil. *BBC*. www.bbc.com/news/technology-27108869

33 MacKinnon, R. (2007). *Shi Tao, Yahoo!, and the lessons for corporate social responsibility.* rconversation.blogs.com/YahooShiTaoLessons.pdf

34 Google Transparency Report. www.google.com/transparencyreport

35 Facebook Global Government Requests Report. https://www.facebook.com/about/government_requests

Twitter,[36] Vodafone,[37] Microsoft,[38] Yahoo[39] and Verizon[40] have begun to shed light on the amount of surveillance and content requests that they are subject to through transparency reports. Companies like Vodafone,[41] Facebook[42] and Twitter[43] also have policies in place for addressing requests from law enforcement.

Conclusions

As demonstrated above, there is significant overlap between intermediary liability, privacy and surveillance. Yet jurisdictions have addressed these issues separately – often having independent legislation for data protection/privacy, intermediary liability and surveillance. The result is that the present legal frameworks for intermediary liability, privacy and surveillance are governed by models that do not necessarily "speak to each other". When requirements that facilitate surveillance are embedded in provisions and practices pertaining to intermediary liability, there is a risk that these requirements can omit key safeguards to surveillance that have been recognised as critical at the international level, including necessity, proportionality, legality and legitimate aim. As La Rue stressed, and as emphasised in other international reports and forums, there is a need for governments to review, update and strengthen laws and legal standards addressing state surveillance. Ideally such a review would also include legal standards for intermediary liability.

Where multi-stakeholder[44] and multilateral[45] dialogues are resulting in incremental and slow progress, some decisions by the Court of Justice of the European Union and European Parliament are calling attention and efforts to the issue.[46]

36 Twitter Transparency Report. https://transparency.twitter.com

37 Vodafone Disclosure to Law Enforcement Report. www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

38 Microsoft's Law Enforcement Request Report. www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency

39 Yahoo Transparency Report. https://transparency.yahoo.com

40 Verizon's Transparency Report for the first half of 2014. transparency.verizon.com

41 Vodafone, Human Rights and Law Enforcement: An Overview of Vodafone's policy on privacy, human rights, and law enforcement assistance. www.vodafone.com/content/index/about/about-us/privacy/human_rights.html

42 Facebook, Information for Law Enforcement. https://www.facebook.com/safety/groups/law/guidelines/

43 Twitter Guidelines for Law Enforcement. https://support.twitter.com/articles/41949-guidelines-for-law-enforcement

44 Powles, J. (2014, April 28). Op. cit.

45 RT. (2013, October 26). Germany, Brazil enlist 19 more countries for anti-NSA UN resolution. RT. rt.com/news/nsa-un-resolution-talks-788

46 Powles, J. (2014, April 28). Op. cit.