Stand Up For Digital Rights

Key Issues: Transparency and Informed Consent

The Internet has fundamentally changed our relationship with information, raising expectations regarding accessibility and making it vastly more difficult to keep secrets. It is no coincidence, for example, that a rapid expansion in recognition of the right to information coincided with the spread of digital technologies and the rise of the Internet.[1] Consumers have also grown more demanding in terms of openness on the part of private sector intermediaries, in part as a result of the increasingly powerful role that these actors play in their day-to-day lives. Where users' personal information is being stored and processed, there is also a broadly recognised right to track how this is being done, as was spelled out in the UN Human Rights Committee's General Comment on the right to privacy:

> In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data is stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or private individuals or bodies control or may control their files.[2]

Edward Snowden's disclosures, which exposed private sector involvement in secret government surveillance programmes, provided significant further impetus to calls for greater transparency.

Transparency Reports

It has now become relatively common among major tech firms to publish transparency reports.[3] Although the specific information provided varies between

[1] A rapid increase in the rate of adoption of RTI laws began in the mid-1990s. See Centre for Law and Democracy and Access Info Europe, RTI Rating Data Analysis Series: Overview of Results and Trends (2013). Available at: www.law-democracy.org/live/wp-content/uploads/2013/09/Report-1.13.09.Overview-of-RTI-Rating.pdf.

[2] Human Rights Committee, General Comment 16, adopted on 8 April 1988. Available at: tbinternet.ohchr.org/Treaties/CCPR/Shared%20Documents/1_Global/INT_CCPR_GEC_6624_E.doc.

[3] See, for example, Google's transparency report: www.google.com/transparencyreport/, Facebook's transparency report: govtrequests.facebook.com/ and Twitter's transparency report: transparency.twitter.com.

different companies, the central thrust is to profile requests to take down content and government attempts to access user information. Better practice in dealing with takedown requests is to provide statistics broken down into the reason for the request (copyright, hate speech and so on), the type of requester (government, private individual, commercial entity and so on), the date of the request, geographic information about the location of the requester and the uploader, and statistics about how the requests were ultimately disposed of. Information about how often users were notified of the requests, and after what period of time, is also useful. In addition to information about requests for material to be removed, companies should publish material about their own enforcement of their terms of service, such as where content is automatically flagged by a particular algorithm or where users have their accounts deleted for committing some sort of prohibited action.

Open Net Korea

A major problem with South Korea's current situation is that telecoms and broadband providers do not publish any sort of transparency reports. NAVER and KAKAO are the two largest portals and only began transparency reporting in December 2014. Both portals publish surveillance transparency reports, whereas only KAKAO publishes a censorship transparency report. Although Google has produced statistics on the Korean government's surveillance and censorship requests on its global transparency page, its market share in Korea is very small.

Before December 2014, the only statistics available were obtained through private sources or by legislators. These legislators worked with agencies that could make disclosure demands on the private sector intermediaries that were licensed or registered with them. For example, in November 2010, we acquired partial statistics from MP Choi Moon-soon after he obtained information from the Korea Communications Commission, and in October 2012, we obtained similar information from MP Nam Kyung-pil. An important revelation from these statistics was the steady and significant rise in the amount of URL takedowns that were privately requested under Article 44-2 of the *Network Act* for non-copyright purposes. In 2008, NAVER and DAUM, the two largest content hosts, had 70,401 and 21,546 takedowns respectively. In the first six months of 2012, there were 104,578 takedowns by NAVER and 40,538 takedowns by DAUM.

The lack of transparency among telecoms and broadband providers (which receive the majority of the surveillance requests) and poor legal requirements regarding notification results in low public awareness of the vast level of State surveillance that exists and consequently a lack of public engagement on the issue. A positive sign that the present transparency reporting could bring about change is that by producing government surveillance transparency reports, NAVER and DAUM appear to be holding themselves accountable for better performance.

Where possible, companies should publish similarly detailed information regarding the nature and processing of requests by governments for user information. However, this type of reporting can be limited by legal restrictions. In the United States, for example, private sector intermediaries are only legally allowed to disclose information about National Security Letters[4] in highly aggregated ranges (for example, between 1,000 to 1,999).[5] These restrictions should be challenged wherever possible. Major tech firms in the US are currently locked in a battle with the government over what they may reveal about their role in mass surveillance schemes.[6] Some firms have found a novel way around this by using 'warrant canaries'.[7] A warrant canary is a statement in a company's transparency report indicating that, within a set time period, it did not receive any government requests for information which were the subject of a gag order. If the company does receive such a request, it can indicate this without breaching the law by removing the statement (i.e. so that is it conspicuously declining to signal that it did not receive any requests).

Christopher Parsons

To be effective, transparency reports should do more than just disclose statistics. They should, ideally, be standardised across an industry so that analysts can understand the full extent of government agencies' attempts to compel or request information from intermediaries. Where companies have wildly different modes of reporting requests it can be impossible to ascertain the actual number of times requests are made, per year, in similar industry categories (such as telecommunications or social media). The consequence is that subscribers and analysts alike can be left without a clear understanding of the actual regularity, scope, or common rationales for data requests.[8]

Transparency reports should also include information concerning a given company's data retention policies. A production order for text messages served on a

[4] National Security Letters are orders which allow the Federal Bureau of Investigation to demand data and which are subject to a gag order forbidding the recipients from revealing details about their existence.

[5] Electronic Privacy Information Center, "National Security Letters". Available at: epic.org/privacy/nsl/.

[6] Ewen MacAskill, "Yahoo files lawsuit against NSA over user data requests", The Guardian, 9 September 2013. Available at: www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests.

[7] "Frequently Asked Questions", Canary Watch. Available at: canarywatch.org/faq.html.

[8] Christopher Parsons, "Restoring Accountability for Telecommunications Surveillance In Canada," The Mackenzie Institute, August 11, 2015. Available at: www.mackenzieinstitute.com/restoring-accountability-telecommunications-surveillance-canada/. Christopher Parsons, "Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports," Social Sciences Research Network, January 14, 2015. Available at: papers.ssrn.com/sol3/papers.cfm?abstract_id=2546032.

company that permanently retains all its subscribers' texts will likely produce significantly more data than one relating to a company that operates with a thirty-one day retention period. Providing such information allows individuals to determine the number of records which may be accessible to government authorities. Otherwise, it can be difficult for individuals to ascertain what these retention periods are.[9] Authorities, in contrast, are less likely to run into these knowledge deficits as they can determine record keeping periods by either consulting companies' (private) law enforcement authority guideline handbooks or by speaking with other security and intelligence professionals who have made requests of various private sector intermediaries in the past.

The policies adopted by private sector intermediaries to respond to State agencies' requests are often documented in companies' Law Enforcement Agency (LEA) Guideline handbooks. These sorts of handbooks "include the detailed procedures government agencies must follow to request corporate-held data, the kinds of identification government agencies must present before information will be disclosed, the time for corporations to process requests, and the costs agencies must pay for the requests to be processed."[10] Companies can choose to publish these handbooks and, in the process, clarify to government agencies and subscribers alike "what kinds of data the company stores, for how long, and under what terms it can be (and is) released" while also clarifying to subscribers "exactly how a TSP handles their personal information … when presented with different kinds of court orders."[11] Private sector intermediaries routinely receive requests from foreign State agencies for access to corporate data and these handbooks can also clarify "how the company must process foreign authorities' requests for company-held data, identify whether customers are notified of either domestic or foreign authorities' requests, outline the period of time the company can take to respond to requests, and state whether the costs incurred in fulfilling the government request must be compensated or not."[12]

These handbooks establish what exactly a company retains, for how long, and under what conditions it will disclose particular subscribers' information to government agencies. However, the more common practice is to keep such handbooks or policies confidential rather than opening up their practices to public evaluation. In the US

[9] In Canada, efforts to learn about intermediaries data retention periods were largely fruitless despite availing themselves to a range of advocacy and legal tactics. For more, see: Andrew Hilts and Christopher Parsons. (2014). "Enabling Citizens' Rights to Information in the 21st Century," *The Winston Report*, Fall 2014.

[10] Christopher Parsons, "Do Transparency Reports Matter for Public Policy? Evaluating the Effectiveness of Telecommunications Transparency Reports," Social Sciences Research Network, January 14, 2015. Available at: papers.ssrn.com/sol3/papers.cfm?abstract_id=2546032.

[11] Christopher Parsons, "The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians," Telecom Transparency Project, retrieved November 17, 2015, pp. 54. Available at: www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[12] *Ibid.*

several companies, predominantly Internet companies such as Yahoo!, Microsoft, and Google, have either published their law enforcement guideline handbooks or had them leaked to the public. No Canadian companies have published correspondingly detailed handbooks.

Terms of Service and Policies

It has become a common joke that nobody reads a company's terms of service. In 2010, as an April Fools Day prank, an online video game retailer inserted a clause into its terms stating that, by accepting, customers acknowledged that the company now owned their soul. 88 percent of customers that day (more than 7500 people) agreed to the terms.[13] Similarly, in June 2014, F-Secure, an Internet security firm, opened a public Wi-Fi connection in London the terms and conditions of which required users to "assign their first born child to us for the duration of eternity".[14] This clause also went largely unnoticed.

Although amusing, the lack of attention given to terms of service is troubling given that these terms serve as the legal basis for the relationship between the company and its users, based on the fact that users formally accept or commit to these terms when signing up for the service.

Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)

Most private sector intermediaries reserve the right, at their discretion, to remove content proactively when it violates the law or their own terms and conditions. The terms and conditions of these platforms are often long and difficult to understand. It is difficult for users to obtain a complete picture of all the content that can be removed because these rules are often scattered in different sections of one or more documents. Since users are unlikely to read the entirety of a company's terms, it is easy to take an action that would authorise the removal of the content or an account suspension.

The fact that users so rarely pay attention to their content also effectively gives companies a licence to draft these terms incredibly broadly. For many companies, it is difficult for even a careful reader to deduce the practical implications of their terms of service.

[13] Joe Martin, "GameStation: 'We own your soul'", bitGamer, 15 April 2010. Available at: www.bit-tech.net/news/gaming/2010/04/15/gamestation-we-own-your-soul/1.
[14] Tom Fox-Brewster, "Londoners give up eldest children in public Wi-Fi security horror show", Guardian, 29 September 2014. Available at: www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause.

For example, Facebook's Data Policy[15] says that it collects information (defined extremely broadly) about users or others, which users provide to Facebook, companies operated by Facebook or third-party partners. The Policy says that this information is used to provide services, personalise content, market to users, conduct surveys and research, show advertisements and promote security across their services. The Policy says that this information can be shared with third-party apps or websites, and that Facebook may share any user information within their family of companies, or to anyone who purchases a part of Facebook's assets or services. The Policy specifies that information shared with advertisers is not personally identifiable (unless the user gives permission otherwise), but goes on to say that information is shared with vendors, service providers, and other partners who globally support their business, noting that these partners must adhere to "strict confidentiality obligations". However, the Policy also says that information may be shared in response to a legal request where required, or if necessary to detect, prevent and address illegal activity. The Policy says that Facebook will retain user information as long as is necessary for its business purposes, or until the user's account is deleted.

These terms grant Facebook incredibly broad licence. The only concrete limitations on the company's actions that they contain are a promise to anonymise information before it is provided to advertisers (unless the user gives permission or the advertisers are considered among the "vendors, service providers and other partners") and an apparent promise that once an account is deleted Facebook will delete information associated with the account.

Some claims within the Policy appear contradictory or misleading. For example, the section on responding to legal requests for user information begins with a statement that information will be shared "if we have a good faith belief that the law requires us to do so" and, in terms of requests from outside of the United States, includes a further caveat that the requests should be "consistent with internationally recognized standards". However, the Policy goes on to say that information may be shared if Facebook has a good faith belief that it is necessary to address or prevent illegal activities, which sets the bar far lower, effectively rendering the statement that requests should be legally binding and in line with international standards meaningless.

The potential breadth of action that Facebook's Data Policy grants the company was laid bare in October 2014, when the company published an academic paper revealing that it had been "experimenting" on its users, in particular regarding how slight changes to their news feed through the site could impact on their political engagement or mood.[16] The idea of a formal, academically-published experiment on

[15] Available at: www.facebook.com/full_data_use_policy.
[16] Micah L. Sifry, "Facebook Wants You to Vote on Tuesday. Here's How It Messed With Your Feed in 2012", Mother Jones, 31 October 2014. Available at: www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout.

61 million unsuspecting subjects raised concerns, particularly in light of the potential for large-scale social manipulation. The company defended the experiment by noting that it is constantly tweaking its interface and that this was merely a logical extension of routine assessments to determine how to deliver content better. Facebook's Data Policy specifically includes references to academic research. Nonetheless, it is likely that, if users who signed up for a Facebook account were presented with a clear, bold message saying that the company intended to use them to carry out social and behavioural experiments, at least a few may have reconsidered the decision.

Although Google's Privacy and Terms are clearer in some ways, they also contain vague elements.[17] For example, they state that user information may be provided to "affiliates or other trusted businesses or persons" in accordance with their Privacy Policy and any other appropriate confidentiality and security measures. Baidu, a Chinese web services company, operates under a User Agreement which is even more vague, saying only that user information "will be utilized to improve the services and web content provided for the user" and shared if required by laws, regulations or relevant government authorities, or to safeguard the company's rights and interests.[18]

Arabic Network for Human Rights Information

Etisalat Egypt, which provides mobile communications services, has terms of contract that stipulate that, "the company is committed to maintain the confidentiality and privacy of subscribers' information, and not to disclose it except under a court order or the implementation of the law or with the consent of the client." However, there is no explanation of what is meant by "the implementation of the law". It also stipulates that service can be cut should the user "[misuse] the service for purposes that may adversely affect the company financially or morally".

STC, one of Saudi Arabia's largest telecommunication companies, also uses vague and unclear contracts, including terms and conditions which provide that "the customer is committed not to misuse services in a detrimental way for the company or one of its clients or a breach of public morality or use it for non-intended purposes. In the case of a breach, the company may take the necessary steps to address it" including potentially cutting off service. There are no examples of what constitutes "harm" or "public morals" or "abuse" or any clarifying definitions whatsoever. Furthermore, there is no information available on the website informing the user of the extent of data collection about the user or the circumstances under which this information may be disclosed.

[17] Available at: www.google.com/intl/en/policies/privacy.
[18] Available at: motu.baidu.com/protocal.html.

The lack of public understanding of what, exactly, these terms and policies contain is particularly problematic since it undermines the core dynamic whereby users trade their privacy for services. The legality of this exchange is predicated on informed consent by the users regarding how their information will be collected, processed and disclosed. Where a company's terms or policies are written impossibly broadly, or in a deliberately confusing fashion, it is difficult to see how meaningful consent can exist.

This is not to minimise the legitimate challenge that private sector intermediaries face in engaging users on these issues. Some policies require users to scroll through to the end of the document before they can indicate their acceptance, while others highlight important aspects of the policy with larger or differently coloured text, and/or subdivide the agreement into a series of thematic screens which must be clicked through individually. There is no indication, however, that any of these measures are particularly effective in getting users actually to read and understand the terms. This is likely because the measures do nothing to solve a key underlying problem, which is that terms of service are usually long and difficult for a lay person to understand even when they are not written in a deliberately misleading manner. An active digital citizen may sign up for several services a week and as a result be presented with potentially hundreds of pages of legal documents.

A welcome move by some companies is to provide a simplified version of their terms of service. Disconnect, a search engine, prefaces their privacy policy with four simple statements:

> Nothing in this policy contradicts the following statements:
> 1. We don't collect any of your personal info, including your IP address, other than information you voluntarily provide.
> 2. We don't sell your personal info to advertisers or other third parties.
> 3. We share your personal info only when legally required, or when reasonably necessary to prevent harm in an emergency situation.
> 4. We retain your personal info, excluding info you make public, for no more than 30 days after you request deletion.[19]

Ultimately, there is a strong need for a common framework which would allow users to understand a company's policies clearly and with only a reasonable effort, and to compare them with those of competitors. One interesting approach is that taken by Creative Commons, which uses symbols to simplify dramatically the standards for releasing material publicly. Creative Commons offers users a "menu" of options which can be understood with minimal effort and which allows users to understand relatively complex terms easily. Although the subject matter that Creative Commons deals with is far simpler than what needs to be conveyed in many terms of service, there are indications a similar approach may be possible. One interesting initiative, "Terms of Service; Didn't Read", provides short summaries of the main points of the terms of service agreements offered by major

[19] Available at: disconnect.me/privacy. Accessed 30 May 2016.

tech services.[20] Important clauses are explained in plain language and rated on a five-point scale according to how concerned users should be about them. Disconnect embeds icons in its search results, allowing users to assess quickly and easily whether the websites comply with Do-Not-Track (DNT) requests, support encrypted connections, retain user data for long periods of time and so on.[21]

Beyond clear language, accessibility is important. Information should be posted in a visible and prominent manner, and should be posted in each of the languages in which they offer services. Where possible, this information should be consolidated, so that users do not have to navigate through a maze of different, and potentially contradictory, documents in order to obtain clear information.

Marketing and Advertising

Misleading or deceptive marketing practices are a problem in the tech world as they are in the offline world. AT&T, for example, faced a lawsuit from the United States Federal Trade Commission after they instituted throttling measures against millions of customers once they reached a particular ceiling, even though they had purchased an "unlimited" data plan.[22] AT&T defended itself, in part, by claiming that the term "unlimited" had different meanings for different companies, highlighting the lack of a standardised yardstick. The rapidity at which new tech products continue to evolve means that there is a clear need to ensure that users are clearly informed about what to expect from a product or service. This is compounded by the fact that, since many products are offered free of charge, users may not be as wary as they would if they were spending money.

In the rapidly changing digital economy, many private sector intermediaries face pressure to pull existing users into their newest product offerings. This raises obvious questions about consent and better practice is for private sector intermediaries to make new services opt-in, rather than opt-out.

Clear communication is particularly important where speech is being restricted or content is being removed. Users need to be able to understand why and how rules are applied, so that they can attempt to stay on the right side of them. For years, Reddit had a policy of not informing suspected spammers that they had been banned from posting to the site, in order to prevent spam programmes from figuring out how they were being identified. The resulting "shadowban" meant that to a user their posts appeared to go through successfully but they were invisible to everyone else. In May 2015, a user complained that he had been mistakenly banned for three

[20] Available at: tosdr.org/.
[21] Available at: disconnect.me/icons.
[22] John P. Mello Jr., "AT&T: We Told Our Customers 'Unlimited' Doesn't Mean 'Unlimited'", Commerce Times, 29 October 2014. Available at: www.ecommercetimes.com/story/81275.html.

years without even realising it.[23] Later that year, in response to a broad push for more transparency, the website announced that it was transitioning to account suspension, which is more readily visible to the subject.[24]

[23] See: "TIFU by posting for three years and just now realizing I've been shadow banned this entire time", Reddit, 6 May 2015. Available at: www.reddit.com/r/tifu/comments/351buo/tifu_by_posting_for_three_years_and_just_now/.

[24] "Account suspensions: A transparent alternative to shadowbans", Reddit, 10 November 2015. Available at: www.reddit.com/r/announcements/comments/3sbrro/account_suspensions_a_transparent_alternative_to/.

Stand Up For Digital Rights

Recommendations for Transparency and Informed Consent:

Transparency Reporting

- **Intermediaries should produce regular transparency reports which include, at a minimum:**
  - **Statistics on the number of takedown requests received, broken down by category of request, by type of requester, by the date and subject of the request, and by the location of the requester.**
  - **Statistics on the number of requests received for information about users, broken down by category, by type of requester, by date and by the location of the requester.**
  - **Information about actions intermediaries have taken proactively to enforce their terms of service, including statistics about material removed and accounts deleted.**
- **Intermediaries should publish detailed information about their procedures for responding to requests from law enforcement agencies, as well as their procedures for processing other government requests to restrict content, block services or deactivate accounts.**

Terms of Service

- **Intermediaries should take steps to ensure that their terms of service are clear to users, for example by publishing clear, concise and easy to understand summaries or explanatory guides.**
- **Intermediaries should publish their terms of service in each of the languages in which they offer services, and post this information prominently on their website.**
- **Intermediaries should support initiatives which aim to enhance understanding of their terms of service, such as "Terms of Service; Didn't Read", and implement measures to try to get users actually to read them.**
- **Intermediaries should consult with users prior to major amendments to their terms of service, notify users of amendments to their terms of**

service and make previous versions available online so that users can assess the changes.

- **Intermediaries should provide reasonable avenues of engagement for users seeking clarification of their terms of service and allow users to propose changes.**

Other Issues

- **Intermediaries should publish information about how their terms of service apply in different jurisdictions.**
- **Intermediaries should challenge legal restrictions on what information they can release about takedown and user information requests, and should explore alternative avenues to facilitate disclosure, such as the use of warrant canaries.**
- **Intermediaries should not automatically opt their users into new services.**
- **Intermediaries should be careful to avoid misleading promotional material, taking into account the rapidly evolving nature of the services that are being offered, which means that it is difficult for established industry meanings and understandings to evolve.**