CIGI

CHATHAM HOUSE
The Royal Institute of International Affairs

Global Commission on Internet Governance

ourinternet.org

PAPER SERIES: NO. 24 — JANUARY 2016

The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality

Emily Taylor

THE PRIVATIZATION OF HUMAN RIGHTS: ILLUSIONS OF CONSENT, AUTOMATION AND NEUTRALITY

Emily Taylor

Published by the Centre for International Governance Innovation and Chatham House.

CIGI

67 Erb Street West
Waterloo, Ontario N2L 6C2
Canada
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs

10 St James's Square
London, England SW1Y 4LE
United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

TABLE OF CONTENTS

ABOUT THE GLOBAL COMMISSION ON INTERNET GOVERNANCE

The Global Commission on Internet Governance was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem.

Launched by two independent global think tanks, the Centre for International Governance Innovation (CIGI) and Chatham House, the Global Commission on Internet Governance will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.

The Global Commission on Internet Governance will focus on four key themes:

- enhancing governance legitimacy — including regulatory approaches and standards;
- stimulating economic innovation and growth — including critical Internet resources, infrastructure and competition policy;
- ensuring human rights online — including establishing the principle of technological neutrality for human rights, privacy and free expression; and
- avoiding systemic risk — including establishing norms regarding state conduct, cybercrime cooperation and non-proliferation, confidence-building measures and disarmament issues.

The goal of the Global Commission on Internet Governance is two-fold. First, it will encourage globally inclusive public discussions on the future of Internet governance. Second, through its comprehensive policy-oriented report, and the subsequent promotion of this final report, the Global Commission on Internet Governance will communicate its findings with senior stakeholders at key Internet governance events.

www.ourinternet.org

ABOUT THE AUTHOR

Emily Taylor is an Internet governance expert and an associate fellow of Chatham House. She has worked in the domain name industry since 1999. Emily is co-editor of the *Journal of Cyber Policy* (Taylor & Francis) and a member of the Global Commission on Internet Governance Research Advisory Network. Her research publications include the annual *World Report on Internationalised Domain Names* (lead author); various reports on Internet protocols for the UK regulator, Ofcom; a review of the policy development process of the Internet Corporation for Assigned Names and Numbers (ICANN); a study on the domain name system in the Middle East and adjoining countries (for ICANN) and a paper on IANA's (Internet Assigned Numbers Authority's) transition (for the Global Commission). She chaired the independent WHOIS Review Team for ICANN, and served on the United Nations Internet Governance Forum's Multistakeholder Advisory Group. For 10 years, she was at Nominet as director of legal and policy. She is a director of several Internet companies, including Oxford Information Labs, which specializes in data mining and statistical analysis.

Business is collecting way more information than it should. We now have a stalker economy where customers become products.... Every time we — collectively — have had a choice between convenience and privacy/security, we've chosen convenience.

—Al Gore (2014)

EXECUTIVE SUMMARY

The Internet enables the free flow of information on an unprecedented scale but to an increasing extent the management of individuals' fundamental rights, such as privacy and the mediation of free expression, is being left in the hands of private actors. The popularity of a small number of web platforms across the globe confers on the providers both great power and heavy responsibilities. Free-to-use web platforms are founded on the sale of user data, and the standard terms give providers rights to intrude on every aspect of a user's online life, while giving users the Hobson's choice of either agreeing to those terms or not using the platform (the illusion of consent). Meanwhile, the same companies are steadily assuming responsibility for monitoring and censoring harmful content, either as a self-regulatory response to prevent conflicts with national regulatory environments, or to address inaction by states, which bear primary duty for upholding human rights. There is an underlying tension for those companies between self-regulation, on the one hand, and being held accountable for rights violations by states, on the other hand. The incongruity of this position might explain the secrecy surrounding the human systems that companies have developed to monitor content (the illusion of automation). Psychological experiments and opaque algorithms for defining what search results or friends' updates users see highlight the power of today's providers over their publics (the illusion of neutrality). Solutions could include provision of paid alternatives, more sophisticated definition and handling of different types of data — public, private, ephemeral, lasting — and the cooperation of all stakeholders in arriving at realistic and robust processes for content moderation that comply with the rule of law.

INTRODUCTION

In the so-called "stalker" economy, as Al Gore (2014) has termed it, customers become products and business collects much more information than it should. He suggests that "we are rapidly approaching a gag point" at which consumers reject current norms and reassert their right to privacy. But in such a contested and controlled environment, what constitutes individual privacy, and how plausible would a reassertion of it be?

Many factors contribute to the current anxiety: the popularity of "free" services based on targeted advertising; decreasing technological costs and increasing capacity to process and store big data in novel ways; a tendency for surveillance to be enabled through "cosy, voluntary relationships" (Anderson 2015a) between governments and a handful of technical providers; the reach and power of a handful of (mostly US-based) companies with billions of users; and galloping technological innovation without a parallel track on ethics to guide decision makers — "not everything that technically can be done, should be done" (Omand 2015, 16).

There is a burgeoning field of scholarship encompassing the intersection of human rights with online life. It is not possible or desirable to attempt comprehensive coverage of this rich field in one short paper. Beyond its scope are online state surveillance; the details of former National Security Agency (NSA) contractor Edward Snowden's revelations; the response of the technical community to alleged systematic weakening of encryption standards; the security risks arising from data breaches (such as the Sony hack, or the alleged targeting of Reuters by the Syrian army through a third-party advertiser). While the paper briefly alludes to the tendencies of states to enlist the assistance of private companies in mass surveillance, or even copyright enforcement, this is not its primary focus.

The Snowden documents have sparked legal challenges in more than one country, many of which are still working their way through the system.[1] This paper does not speculate on their likely outcomes.

CONTEXT

Human Rights: The Legal Matrix

The Universal Declaration of Human Rights (UDHR) was adopted in 1948 by the newly formed United Nations General Assembly, following "massive violations of fundamental rights immediately before and during World War II" (Gardbaum 2008, 750). The UDHR is founded on the concept that "the peace and security of mankind are dependent on mutual respect for the rights and freedoms of all" (Roosevelt 1948).

The UDHR was followed by, and provides the basis for, UN treaties and a patchwork of legally binding instruments and enforcement mechanisms at both the regional and the

1 Note that the Court of Justice of the European Union judgment in *Schrems v Data Protection Commissioner* (6 October 2015) Case C-362/14 (http://curia.europa.eu/juris/documents.jsf?num=C-362/14) was issued after this paper was written.

national level.[2] Recognition for fundamental rights is also enshrined in some national constitutions and domestic laws,[3] which broadly reflect the UDHR in form and substance. The UDHR has also influenced legal thinking and the harmonization of laws in Europe (Harris et al. 2014, 34).

Which Human Rights?

While this report focuses mainly on privacy and freedom of expression, all human rights are interdependent and indivisible (OHCHR n.d.). For example, poor privacy protection has an impact on freedom of expression, freedom of assembly and the peaceful enjoyment of property (Mendel et al. 2012). In *A Question of Trust: Report of the Investigatory Powers Review*, David Anderson (2015b, 25) uses the "catch-all word '*privacy*' as an imprecise but useful shorthand for such concepts." This paper adopts the same approach.

While some rights — such as the right to life, not to be tortured, not to be held in slavery — are absolute, others are not; for example, states have a right of derogation from most human rights in times of public emergency. Other rights, such as privacy and freedom of expression, are subject to limitations. But the sources are clear that "any limitations of these rights should be exceptions to the norm, and be based on legitimate purposes. Likewise, limitations of any right need to be according to law, and be necessary and proportionate."[4]

Why Pay Attention to Private Companies?

States, not private actors, have legal obligations to respect, protect and fulfill human rights. That these obligations apply online, as well as off-line, is well established — for example, in the influential Human Rights Committee's General Comment 34 (UN 2011b), resolutions of the Human Rights Council (UN 2012) and UN General Assembly,[5] and the NetMundial "Multistakeholder Statement" (NETmundial 2014). The reason for fixing states, rather than companies, with human rights obligations, is clear. The defining quality of a state is its "monopoly of the legitimate use of physical force within a given territory" (Weber 1946). Other than human rights standards, few checks and balances exist over the power of states to make or enforce laws in their territory. In contrast, companies (for the most part) have no coercive powers and are subject to national laws and regulations. This is why some human rights experts view a focus on private company actions as a distraction — the proper recourse, in their view, being for states to regulate or legislate to restrain market excesses.

Paying attention to private companies when evaluating risks to fundamental rights online is important for two reasons. First, both states and the private sector Internet platforms have shared interests in storing, processing and correlating big data, albeit for different reasons (security for the former; advertising revenues for the latter). At the same time, the market for web platforms is becoming more concentrated in the hands of a small number of companies. This alignment of powerful interests threatens an insidious erosion of fundamental rights and makes it unlikely that governments — who rely on private sector data and skills — would legislate or regulate to limit big data collection by Internet platform providers.

Second, the cross-border nature of the Internet makes it difficult to understand where responsibilities lie — with one state, many states, the private sector or a shifting combination of all of them? Moreover, the substantive issues are difficult — the scope of individuals' right to privacy; how to operate censorship of online content in an international, multicultural environment. It is tempting for states to park the issues in the "too difficult" pile and hope that someone else will take responsibility. There is evidence that the actions and inactions of states are placing private companies in the incongruous position of having to mediate users' fundamental rights.

Companies' Potential Impact — Off-line and Online

Experience in the off-line world demonstrates that real harms can occur to individuals through the actions of private companies. When Royal Dutch Shell exploited oil reserves in the Ogoniland, Nigeria, from the 1950s onwards "villagers lived with gas flares burning 24 hours a day (some for more than 30 years), and air pollution that produced acid rain and respiratory problems" (International Crisis Group 2008). Peaceful protests by villagers escalated into armed conflict and finally the execution of protesters, including Ken Saro Wiwa, in 1994. Eventually, Shell withdrew from Ogoniland (ibid.).

The Nigerian government did not actively "delegate" any rights to Shell and Shell did not actively assume any responsibility. The Ogoniland experience illustrates how

2 For example, the International Covenant on Civil and Political Rights (Office of the United Nations High Commissioner for Human Rights [OHCHR] 1966). At the regional level, the European Convention on Human Rights (1950, 87 UNTS 103; ETS 5) has been described by David Harris et al. as having comparatively strong enforcement mechanisms through the European Court of Human Rights. Other mechanisms include the American Convention on Human Rights (1969, 1144 UNTS 123, in force 1978, 23 parties), and the African Charter on Human Rights and Peoples' Rights (1981, 1520 UNTS 143, ILM 59 (1981) in force 1986, 53 parties).

3 For example, constitutions of Austria and Spain; the European Convention (which prevails over the national constitution in the Netherlands; the UK Human Rights Act 1998; Canadian Charter of Rights and Freedoms, Canada Act 1982.

4 See OHCHR (1966, articles 4(1) and 4(2)).

5 For a good summary of UN resolutions recognizing human rights online, see Finnegan (n.d.).

large-scale human rights harms can arise through the passivity of states and their failure to take affirmative action.

In the virtual world, too, private company actions can have a direct impact on human lives. A classic example is the story of Beijing journalist Shi Tao. In 2004, he used his Yahoo email account, which had been set up under a pseudonym, to send an article to a pro-democracy website in New York. Yahoo complied with the Chinese authorities' request to reveal his identity. Shi Tao was arrested and sentenced to 10 years in prison. The Shi Tao case reveals how difficult it can be for multinationals to navigate between the legal requirements of host countries and accepted international standards: "It had taken two years of being pummelled by Congress, human rights groups, the media and shareholders before Yahoo finally shed its head-in-the-sand, lawyer-driven posture and actually took moral responsibility for what had happened" (MacKinnon 2012).

Guiding Principles on Business and Human Rights

Recognition of the impact that private actors, in particular multinationals, can have on human rights led to the development of guiding principles on business and human rights by the special representative of the UN Secretary-General on human rights and transnational corporations and other business enterprises, John Ruggie. The Ruggie Principles (UN 2011a) are a non-binding "protect, respect and remedy" framework for multinationals and were a breakthrough in a process that had been deadlocked for many years.

Despite endorsement by the UN Human Rights Council (in 2011), the Council of Europe (2014a) and adoption by Internet companies in "the Silicon Valley Standard" (Access n.d.), there is little evidence that the Ruggie Principles have had an impact on the culture or practices of "big tech." The Council of Europe's Commissioner on Human Rights observes that the Ruggie Principles do not deal with situations "where states make demands of companies that would lead companies into violations of international human rights law" and that "there is little other than moral rectitude or public relations pressure that can create incentives for online intermediaries to defend human rights" (Council of Europe 2014b).

Another example is the Global Network Initiative's work to advance human rights policies in information and communication technology companies; its membership includes Facebook, Google, LinkedIn and Yahoo (Global Network Initiative 2012).

BIG DATA AND PROFILING

Moore's law — after George E. Moore, the co-founder of Intel Corporation — states that computer capacity doubles approximately every two years.[6] With that increase naturally comes an exponential growth in data storage and a decrease in associated costs, as well as the hidden requirement, driven by business and national security concerns, to make sense of the information glut. The questions then arise: how is this done, who is doing it and with what justification?

The Internet has brought about a transformation in the quantity of digital data. Each day users send out 500 million tweets and upload 240 million photographs to Facebook; Google processes data that is "thousands of times the quantity of all printed material in the US Library of Congress" (Mayer-Schönberger and Cuker 2013, 8). While the quantity of non-digital data remains fairly static, digital data is doubling every three years. If all the digital data existing in 2013 were "placed on CD-ROMs and stacked up, they would stretch to the moon in five separate piles" (ibid., 9).

The Uses of Big Data

Big data — the ability to mine and make sense of enormous electronic files — is at the heart of the business models of today's Internet platforms. Big data allows the platforms to offer "free" services to users, financing their operations by enabling advertisers to target audiences with implausible precision. The author has personal experience of one small-scale example: a friend's start-up opera company in Oxford, England, was recently looking for soloists. Using Facebook's services, the company could specify that its advertisements be shown to conservatory-trained soprano and tenor soloists, aged between 25 and 30 years and based in the European Union. The advertising was cheap and the company was inundated with perfectly qualified candidates. The power of big data profiling is seen in the ability to match advertisers with potential targets with such precision.

On a much larger scale, big data can help improve public health by enabling authorities to respond to epidemics more rapidly. In much of the developed world, doctors are obliged to file with the authorities, within two weeks, every instance of a patient presenting with flu symptoms. Data mining of Google search queries relating to flu symptoms provides results that correlate almost perfectly with off-line historic official data relating to flu epidemics, but with an important difference. Unlike the official data (which

6 See www.intel.com/content/www/us/en/silicon-innovations/moores-law-technology.html.

has at least a two-week lag), Google's data is available in real time.[7]

Big Data: Human Rights Risks

As ever, the technology has charged ahead of the policy analysis, with impacts already evident on privacy, freedom of expression and risks of discrimination. The corollary of the revolution in data analysis is that the same tools can be used for the purposes of repression.

The argument that "you have nothing to fear if you have nothing to hide" is enlisted by governments and companies to justify surveillance or big data processing. According to these reductive, "superficial incantations" (debunked by Solove 2007), privacy has only negative connotations, of protecting the scoundrel or the wrongdoer. Privacy is difficult to define, dependent on context, shifting and elusive, but it is a fundamental right, essential to individuals' autonomy, intimacy, dignity and ability to form an opinion.

Erosion of privacy by powerful actors (whether state or private) can cause insidious harm; as Evgeny Morozov (2013, 189) has said, "Given enough data and the right logarithms, all of us are bound to look suspicious." This idea echoes the famous epigram attributed to Cardinal Richelieu, "Qu'on me donne six lignes écrites de la main du plus honnête homme, j'y trouverai de quoi le faire pendre" (Only give me six lines written in the hand of the most honest man, and I will find something there to hang him by) (quoted in Stevenson 1964, 2259).

The human rights impact of compulsive data collection in an off-line, paper-based context (although severe) is somewhat limited by the difficulty and cost of making any sense of it. For example, "by the early 1980s the Stasi[8] had about 85,000 regular employees and about a million and a half full- and part-time informers" (Clay Large 2001). Within a space of 40 years, the Stasi had amassed four miles of files, "more…than had been collected in the whole of Germany from the Middle Ages to the end of the Second World War" (Vaizey 2014).

Unlike the Stasi's unsiftable heaps of paper, digital data is searchable, indexed and correlated. It is usable, and used.

Automated Tracking and Profiling

The ways in which private companies track online user behaviour, and their implications for privacy, are well explored in academic and industry literature (see, for example, Deibert 2013; MacKinnon 2012; Schneier 2015; Mayer-Schönberger and Cukier 2013). Cookies, social plug-ins and canvas fingerprinting are used throughout the Web. Their persistent popularity is partly due to the convenience they offer users. Session cookies allow browsers temporarily to store data entered into online forms before submission. Security cookies enable secure transactions upon which online banking and e-commerce depend. Social plug-ins enable users to share articles through Twitter, Facebook and other social networks. Single log-ins (for example, "Sign in with Facebook") enable users to interact with sites without creating hundreds of user profiles.

The trade-off for this convenience is "a shockingly extensive, robust, and profitable surveillance architecture" (Schneier 2015). Dozens of different companies' cookies are tracking users on popular sites; one site[9] installed 200 tracking cookies on a user's browser. DoubleClick (a Google company) enables targeted advertising to follow users as they browse. Single log-ins enable Facebook and other providers to track users — even those who are not logged into Facebook (ibid.).

Whereas the privacy implications of cookies have been well understood by policy makers for more than a decade, other tracking techniques might not be covered by the relevant legislation. Canvas fingerprinting and other tracking methods (such as evercookies and respawning) are widely used, even by the White House (Eckerslley and Opsahl 2014). These techniques uniquely identify users from their devices, are not transparent to users and are difficult to disable without significant loss of functionality.[10]

A whole industry of data intermediaries has emerged. Companies such as Datalogix and Acxiom collect consumer data "from numerous sources, largely without consumers' knowledge" (Federal Trade Commission 2014), sharing data with each other and creating profiles or categories of consumers, some of which make sensitive inferences about ethnicity, income levels or health-related conditions: "expectant parent," "diabetes interest," "cholesterol focus" (ibid.). Profiling and categorization can be beneficial for consumers: credit card fraud prevention relies on identifying breaks from a consumer's standard patterns of spending (Schneier 2015); targeted advertising has the potential to inform consumers about products or services they might enjoy. At the same time, profiling "can unwittingly lead to discrimination on grounds of race, gender, religion or nationality" (Council of Europe 2014b). It can also invade privacy: a father complained to the budget retailer Target that his teenage daughter had been sent coupons for baby products. It turned out that Target's "pregnancy prediction score" knew more than

7 See www.google.org/flutrends/about/how.html.

8 The Stasi (Ministerium für Staatssicherheit, abbrev.) was the state security service of the German Democratic Republic from 1950 to 1989.

9 Dictionary.com, 2010 (per Schneier 2015).

10 For an explanation on how canvas fingerprinting works, see Acar et al. (2014); Mowery and Shacham (2012).

the girl's father did — his daughter was, indeed, pregnant (Duhigg 2012).

Data Anonymization: An Imperfect Form of Protection

So long as data is anonymized, what harms can arise to individuals? Unfortunately, it is straightforward to reverse anonymization, and metadata can be just as revealing as the underlying content, if not more so. Our relationships, what we do and correlations between different data sets provide the key to identify individuals from anonymized data. This fact has been demonstrated many times: when AOL released 20 million items of search data in 2006, researchers identified individuals by correlating different items in their search history, and, in 2008, 10 million movie rankings by 500,000 anonymized Netflix customers were de-anonymized by comparing rankings and time stamps with the public International Movie Database's rankings and time stamps (Schneier 2015). In an experiment carried out at Carnegie Mellon University in 2000, researchers were able to de-anonymize 1990 US census data for 87 percent of the population based on three data items: zip code, gender and date of birth (Sweeney 2000).

The scale of Internet data increases the fragility of anonymization as a protection. The artist Eric Fischer creates artwork based on publicly available data (Fischer 2010). He has produced world maps based on location data of 6.3 billion tweets (Fischer 2014). Fischer explains how he filters the data to eliminate duplicates: "Showing the same person tweeting many times within a few hundred feet also makes the map very splotchy, so I filter out those near-duplicates too" (ibid.). It makes for a much clearer map, but it is also a reminder that each data point can be traced back to an individual.

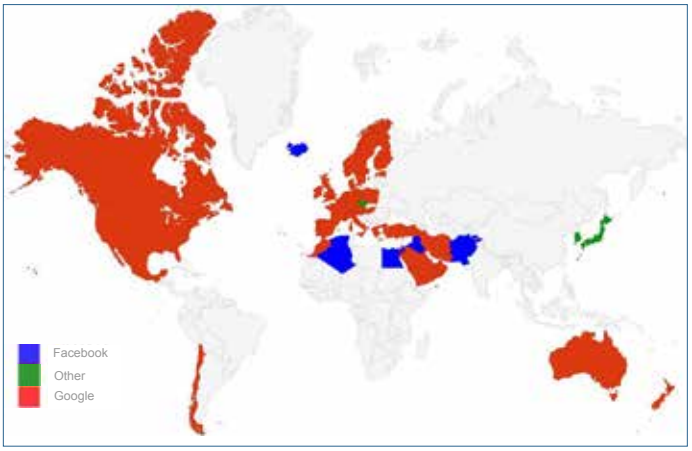
THE HUMAN RIGHTS RISKS OF BIG DATA COLLECTION

A Global Platform, with a Few Big Players

Competition between companies results in greater user choice and can provide a more diverse range of human rights protections. As markets become concentrated and people depend on a few essential platforms, the providers' rules have more impact on individuals' rights.

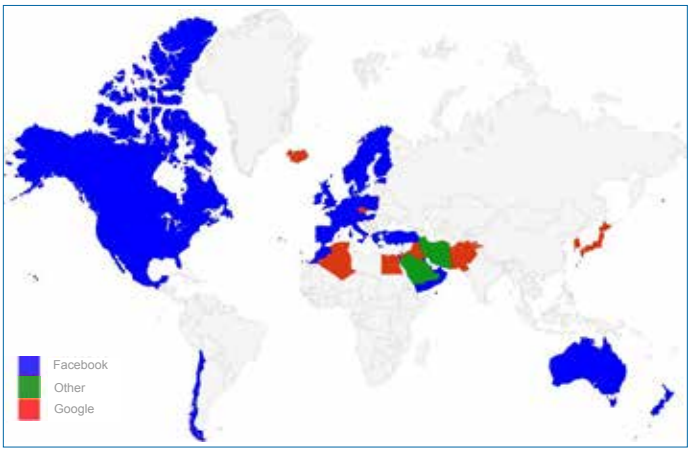
There might be a billion websites online[11] but the world's 2.9 billion Internet users spend their time on just a handful of platforms. For this study, the author undertook a comparison, based on Mark Graham and Stefano De Sabbata's "Age of Internet Empires" (2013), of the most popular sites across all 34 countries of the Organisation for Economic Co-operation and Development (OECD) and 17 countries from the Arab states and Central Asia.[12] The sample countries are geographically, economically and culturally diverse but the top websites in every country are the same[13] (see Figures 1, 2 and 3, and Table 1).

Figure 1: Most Popular Website by OECD Country and Arab States, 2015



Source: Author; data from Alexa.com.

Figure 2: Second-most Popular Website by OECD Country and Arab States, 2015



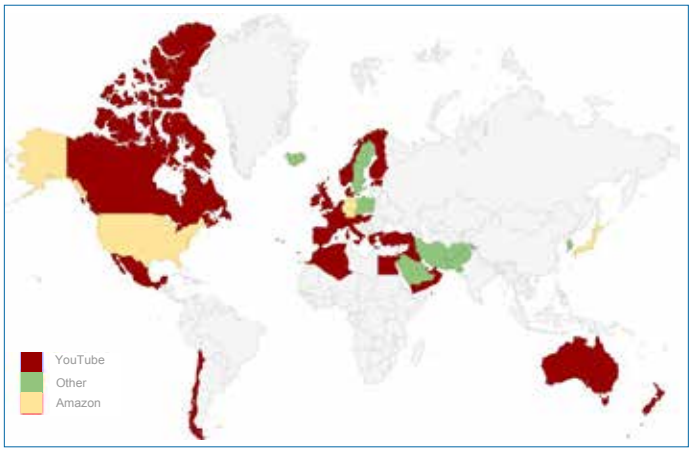
Source: Author; data from Alexa.com.

11 According to Internet Live Stats, 957,208,000 websites, compared with 23,500 in 1995 (www.internetlivestats.com/total-number-of-websites/).

12 Analysis took place in May and June 2015, using Alexa.com. Countries sampled: Afghanistan, Algeria, Bahrain, Egypt, Iraq, Islamic Republic of Iran, Jordan, Kuwait, Morocco, Oman, Pakistan, Palestine, Qatar, Saudi Arabia, Turkey, United Arab Emirates and Yemen.

13 Median rankings across the 51 countries sampled.

Figure 3: Third-most Popular Website by OECD Country and Arab States, 2015



Source: Author; data from Alexa.com.

Table 1: Ranking of Top Sites Across OECD Countries, Arab States and Central Asia

	OECD	Arab States and Central Asia
Facebook.com	1	2
Google.com	2	1
YouTube.com	3	4
Google.local*	4	3
Wikipedia.org	5	7
Yahoo.com	6	5
Amazon (local)	7	–
Twitter.com	8	6

* "Google.local" means the local version of Google, for example, google.co.uk, google.ae, google.co.ma, google.dz. Across the Arab States and Central Asia sample, some countries also featured another country's local version of Google in their top 10 sites. Google sites occupy four of Algeria's top 10 sites: Google.dz (number 2), YouTube.com (number 3), google.com (number 4), google.fr (number 6) (see www.alexa.com/topsites/countries/DZ); google.com.sa is in Sudan's top 50 sites (number 22).

Source: Author. Ranking derived from mode score and number of instances in top 10, analyzing data from Alexa.com by country.

Google sites typically feature three times (google.com, google.local and YouTube) in the top 10 sites of every country sampled. The only exceptions are where particular countries have banned YouTube (Iran and Pakistan) or where there is no local service for Google (for example, Yemen and the United States, where google.com and YouTube.com feature but google.local does not). Other sites included in the 10 most popular sites across the entire sample are Wikipedia (42 countries), Yahoo.com (32 countries), Amazon (.com or .local, 26 countries), Twitter (20 countries).

This is not to say that the top websites are homogeneous across all the countries studied or that a YouTube user in the Republic of Korea will consume the same material as a user in Egypt or the United States. For example, 37 of the 50 most popular sites in Turkey are local and do not appear on any other country's top 50. The significance of the concentration at the top of the lists lies in the long tail typically experienced in Internet traffic, meaning that the top handful of sites account for the lion's share of traffic. When Google experienced a short outage in 2013, total web traffic dropped by 40 percent (Geere 2013). When Facebook was down for an hour in January 2015, "social traffic"[14] dropped by 80 percent (Ratomski 2015).

STANDARD TERMS ANALYSIS: THE ILLUSION OF CONSENT

The impact that large Internet platforms can have on individuals' fundamental rights is well recognized, forming part of the "Ranking Digital Rights" project,[15] the Electronic Frontier Foundation's (EFF's) annual "Who Has Your Back?" report (2015b), and Take Back the Tech's (2014) scorecard on social media and violence against women.

The concentration of web traffic within a handful of private for-profit platforms lends significance to the terms of service and privacy policies, which set out the rules of the road, expected standards of user behaviour and the rights of platform providers to access, edit, delete and share user data.

This study analyzed the standard terms of agreement of Google (including YouTube), Facebook, Yahoo, Twitter and Amazon. Table 2 highlights terms that have an impact on the user's fundamental rights of privacy and freedom of expression.

The terms give the providers unfettered rights to access, delete and edit user data, including location data, and to share user data with unspecified third parties (for example, advertisers). None of the providers have clear deletion policies for user data or metadata, with the limited exception of Twitter.[16]

Metadata is information about a communication, distinct from the content of a communication. Metadata tells you

14 "Social traffic" is web traffic flowing from a social network to another site. In 2014, an estimated 30 percent of total web traffic was "social traffic"; see Wong (2015).

15 The Ranking Digital Rights project's "Corporate Accountability Index" was launched in November 2015 (after this paper was written). The project's 31 indicators include analysis of terms of service as part of a broader focus on the many aspects of policies and practice that can impact human rights; see MacKinnon (2015).

16 Twitter commits, in its Terms of Service (https://twitter.com/tos?lang=en) and its privacy policy (https://twitter.com/privacy?lang=en), to deleting one aspect of user data — log-data — within 18 months.

Table 2: Analysis of Websites' Standard Terms of Agreement

	Google	Facebook	Yahoo	Amazon	Twitter	YouTube
Unfettered right of provider to access user data	√	√	√	√	√	√
Access to private chat, emails	√	√	√	√	√	√
Access to location, GPS, IP address, Wi-Fi points and cell towers without further user consent	√	√	√		√	√
Right to delete any user data without notice		√	√	√	√	√
Right to modify any user data without notice	√	√	√	√	√	√
Right to share user data with law enforcement	√	√	√	√	√	√
Right to share user data with advertisers without user opt-out	√	√	√		√	√
No clearly stated deletion policy for user data and metadata	√	√	√	√		√
California law exclusive jurisdiction	√	√			√	√
No right for EU citizens to elect for home court	√	√	√		√	√
Unfettered right for provider to unilaterally change terms	√	√	√	√	√	√
Community standards include right to take down material that is not illegal in provider's home country	√	√	√	√	√	√

Note: GPS = Global Positioning System; IP = Internet protocol
Source: Author.

about the communication — for example, where a user was when a photo was taken, what telephone number was called and the duration of a call.[17] It is sometimes called communications data or user data.

Retention of user data is also a controversial area. The Court of Justice of the European Union recently ruled that the Directive requiring providers to keep communications data on all users was incompatible with fundamental rights and therefore void.[18] The Directive covered mandatory retention of data by communications providers, the data to be produced at the request of law enforcement. However, the Internet platforms are thought to keep user data for their own purposes. Apart from Twitter, which clearly states that it will delete logging data after 18 months, none of the other platforms' terms explain how long they keep data.[19] The human rights impact of data retention on the ability to create profiles, or to confirm a future suspicion, has rightly been highlighted as a human rights risk by commentators as diverse as Cardinal Richelieu and Evgeny Morozov.

Facebook (2015b) offers users the ability to download their data. It is all there: every wall post, every photograph (content with a public quality); the text, time and date of each and every long-forgotten private chat (content with a transient or private quality). There is no expiry date — the data comprises the user's activity ever since he or she joined the platform. The download tool, according to Austrian student Max Schrems, only gives a "fraction of the data Facebook stores about you" (Schrems n.d.)." When Schrems made a data subject access request to Facebook in 2011, he received a CD containing more than 1,200 pages of data.[20]

Each "like" is also recorded. Research shows that automated analysis of "likes" alone can "accurately predict a range of highly sensitive personal attributes…. The model correctly discriminates between homosexual and heterosexual men in 88% of cases, African Americans and Caucasian Americans in 95% of cases, and between Democrat and Republican in 85% of cases" (Kosinski, Stillwell and Graepel 2013). Other attributes that analysis can correctly predict include religious views, use of addictive substances and parental separation (ibid.), all from transient "likes." Facebook remembers what humans forget.[21]

17 For more about metadata, see Guardian US Interactive Team (2013).

18 The *Digital Rights Ireland* case, C293/12 and C594/12, of April 2014. See, in particular, paragraph 65: "It must therefore be held that Directive 2006/24 entails a wide-ranging and particularly serious interference with those fundamental rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary." http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=179241.

19 Major Internet platform providers were approached for interviews for this study. Apart from Google, none responded.

20 See Robinson (2015). Schrems later went on to win a preliminary point referred to the Court of Justice of the European Union, resulting in a declaration that the US Safe Harbor Decision is invalid (http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf).

21 For more on forgetting and remembering, see Mayer-Schönberger (2009).

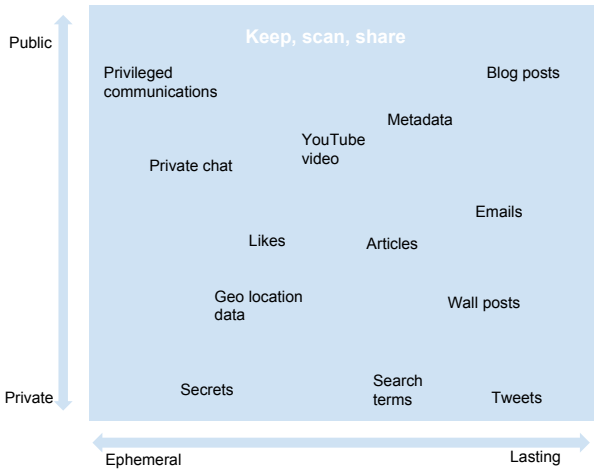
Of particular concern is the intrusion into communications that — in other contexts — have a quality of privacy, for example, email communications, private chat or messaging (Figure 4). For example, Google's terms of service affect more than 425 million Gmail users,[22] and provide no restriction on its ability to scan email content, which potentially includes:

- Communications between journalists and sources. The Court of Justice of the European Union has held that only "an overriding requirement in the public interest" can justify lifting confidentiality protections for such communications.[23] In 2014, Microsoft admitted reading a third-party blogger's Hotmail emails to identify the source of a leak relating to Windows 8 (Hern 2014). The company was able to use its control of the email platform to identify a journalist's source, access which did not require judicial permission for the company.

- Communications protected by attorney-client privilege. In the recent Belhadj case,[24] the UK government conceded that its interception of privileged communications had been unlawful. If interception of such communications by a state on the grounds of national security could not be justified, what possible justification could a private company have for such intrusion?

- Communications between medical practitioners and patients, discussing sensitive medical data. The ability to scan such communications in bulk potentially places Google at a commercial advantage as it diversifies into other business streams, such as automobile insurance (Winkler 2015). After a public outcry, the UK government was forced to put on hold a scheme to sell National Health Service records to insurance companies; private platform provider terms already incorporate the user's consent to share or sell such data, without any feedback to the user on what information has been shared and with whom.

Figure 4: User Data on Proprietary Platforms Today



Source: Author.

Companies are not directly required to conform with international human rights standards but they are required to comply with national laws, which should be consistent with human rights conventions. There is clearly an implementation gap and a lack of guiding standards for today's leading Internet platforms. The standard terms — particularly those of the "free" platforms Google/YouTube, Facebook, Twitter and Yahoo — do not incorporate concepts such as necessity and proportionality, which moderate intrusions into rights of privacy under human rights law. There is little evidence of "reasonableness," a flexible safeguard that guides interpretation of consumer contract terms across the European Union according to unfair contract terms legislation.

A recent study (Van Alsenoy et al. 2015) on the legality of Facebook's terms cites concerns relating to data protection and unfair contract terms, which have a close nexus to human rights (privacy). The report describes updates to terms governing the provider's use of location data as "vague and broad." The report concluded that "there is no longer any mention of limiting the storage or use of location data to the time necessary to provide a service." Facebook has disputed the report's findings.

European consumer protection law limits or excludes certain contractual terms that might create "significant imbalances in the rights and obligations of consumers… and suppliers."[25] Examples relevant to human rights include terms "excluding or hindering the consumer's right to take legal action or exercise any other legal

22 Yohana Desta's (2014) list of the 12 things dwarfed by Gmail's user base includes the population of the United States (318 million), Twitter users (214 million), Yahoo Mail users (273 million as of January 2014) and the number of household cats and dogs in the United States (83.3 million).

23 *Goodwin v United Kingdom* [GC], no. 17488/90, paragraph 39, ECHR 1996-II.

24 *Belhadj and others v Security Service and other,* IPT/13132-9/H, judgment of 29 April 2015. www.judiciary.gov.uk/judgments/investigatory-powers-tribunal-belhadj-and-others-v-security-service-and-others-judgment-and-determination/.

25 EU Council Directive 93/13/EEC of 5 April 1993 on Unfair Terms in Consumer Contracts OJ 1993 L95 p29, annex to Article 3(3) (j) and (q).

remedy,"[26] which invokes the human right to effective remedy through competent national tribunals (UN 1948, article 8). The standard terms of the popular websites — Google, Facebook, Twitter and Yahoo — contain exclusive law and jurisdiction clauses specifying California law and courts, with a few exceptions for EU citizens.[27] Only Amazon allows users to opt for their home court and laws.

Opting to resolve disputes exclusively in the supplier's home courts according to the supplier's national law provides a significant home field advantage to the supplier, not least by deterring consumers against bringing litigation in the first place (particularly where there are language barriers as well as geographic barriers). It takes an unusually determined and resilient individual, such as Max Schrems, to litigate against a multinational in a foreign jurisdiction.[28]

Amazon — and, to some extent, Twitter — present slightly more balanced terms. Amazon has different terms for various jurisdictions. Its terms in EU member states show awareness of not only privacy laws but also unfair contract terms legislation. So, Amazon customers have a right to elect their home jurisdiction for disputes, and Amazon gives its users a right to opt in to location data.[29] Twitter recently announced that it would automatically strip location metadata from uploaded photographs, and it also has a clear deletion policy for log-data (18 months), which the other providers do not.

The UK's Independent Reviewer of Terrorism Legislation, David Anderson (2015a), said, in the context of government surveillance, "Each intrusive power must be shown to be necessary, clearly spelled out in law, limited in accordance with international human rights standards and subject to demanding and visible safeguards." Of course, it is governments' coercive powers that in part necessitate such safeguards. However, we have seen that highly sensitive information can be derived from users' interaction with popular platforms; we have seen that the platforms' standard terms provide few, if any "demanding and visible safeguards" governing use and retention of data. The reliance on — largely fictional — user consent provides an apparent legal justification for grossly intrusive powers. Processes for protecting individuals from harassment are opaque or non-existent, and the extent of data processing is loosely described by most (with the exception of Amazon). It is difficult to understand how the terms could be "in accordance with international human rights standards."

As Ronald Deibert (2013, para. 977) put it, "To repeat, the reason behind this data collection is advertising."

Alignment of State and Corporate Interests

States are attracted to big data honey pots, as the Snowden documents and the transparency reports by leading Internet companies make clear. The trend for governments seeking data from private sector networks is relentlessly upward: Facebook's first transparency report (January–June 2013) recorded 27,000 government requests for data relating to 39,000 user accounts from 71 countries. By December 2014 there had been a 28 percent increase in the number of user accounts affected, and a 22 percent increase in the number of states requesting data.[30]

The implications of states co-opting private company data for the purposes of counter-terrorism or surveillance is a substantial field of scholarship in itself. Their relevance to this study is the increasing reliance by states on private companies' skills — and data. The Snowden documents indicate that the US NSA and the UK's Government Communications Headquarters have paid "millions of dollars" to private companies, including popular Internet platforms and telephone companies, to cover the cost of compliance with requests for user data (MacAskill 2013; Ball, Harding and Garside 2013).

In *The Master Switch*, Tim Wu (2010, 298) predicted (pre-Snowden) that "should Facebook ever see a benefit in aligning itself with a government...clearly it could serve as one of the better spying tools ever created." Bruce Schneier (2015, 86) develops the thought (post-Snowden): "As long as these companies are already engaging in mass surveillance of their customers and users, it's easier for

26 Unfair Terms in Consumer Contracts OJ 1993, L95, Annex to Article 3(3)(q). For further discussion on this point, see Joined Cases C-240/98 to C-244/98 *Océano Grupo Editorial and Salvat Editores* [2000] ECR I4941, paragraph 24: "It follows that where a jurisdiction clause is included, without being individually negotiated, in a contract between a consumer and a seller or supplier within the meaning of the Directive and where it confers exclusive jurisdiction on a court in the territorial jurisdiction of which the seller or supplier has his principal place of business, it must be regarded as unfair within the meaning of Article 3 of the Directive in so far as it causes, contrary to the requirement of good faith, a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer."

27 Facebook refers EU citizens with a privacy dispute to the Irish data protection authority. EU citizens in dispute with Yahoo are referred to the laws and courts of Ireland.

28 Despite the exclusive law and jurisdiction clause (15.1 of Facebook's terms of service), the data processor in the European Union is Facebook Ireland. Schrems brought his original complaint to the data protection authorities of Ireland. The case is being appealed to the Austrian Oberlandesgericht. See www.europe-v-facebook.org. The preliminary question was determined in October 2015 — see http://curia.europa.eu/juris/documents.jsf?num=C-362/14 — leading to the invalidation of the US Safe Harbor Decision.

29 Studies related to organ donation (cited in Kahneman 2011) show the different effect of opt-in and opt-out. In countries operating an opt-out regime, the percentage of organ donors is 86 percent (in Sweden) and 100 percent (in Austria); in countries operating an opt-in regime, the percentage of organ donors is much lower: for example, four percent (in Denmark) and 12 percent (in Germany).

30 See https://govtrequests.facebook.com/# for Facebook transparency reports.

them to comply with government demands and share the wealth with the NSA. And as long as governments keep demanding access and refrain from legislating protections, it's easier to design systems to allow it. It's a powerful feedback loop: the business model supports the government effort, and the government effort justifies the business model."

The interdependence of private-sector business models with government surveillance poses a risk to the fundamental rights of individuals. Private sector actors become enmeshed within the law enforcement machinery, and the predictive powers of big data present democratic risks. Evgeny Morozov (2013, 189) says, "While Facebook might be more effective than the police in predicting crime, it cannot be allowed to take on these policing functions without also adhering to the same rules and regulations that spell out what the police can and cannot do in a democracy."

The risks arise through an imperceptible process of erosion as much as from any intent, as individuals become desensitized to sharing private things in public. This point leads to the question of how much individuals care about erosion of privacy. First, however, consider the ways in which the large web platforms have become drawn into moderating freedom of expression.

Platforms or Publishers?

Private platforms have a measure of choice in how they construct their standard contracts, but another key way in which popular providers have an impact on human rights has arisen almost by default. Despite sincere commitments to freedom of expression, and the legal incentives to maintain neutral intermediary status, popular web platform providers have become drawn into making decisions to remove or moderate content.

Google, Facebook and YouTube are perceived as platforms on which it is the users who generate content and communicate with one another. Unlike traditional publishers, the Internet providers do not screen content prior to publication. It would be futile to attempt traditional editorial control, such is the speed and scale at which new content is generated (300 hours of video are uploaded to YouTube every minute[31]). The providers are classified as intermediaries.

For more than a decade, concerns relating to images of child abuse and copyright infringement have provided the backdrop for ever-increasing liability of intermediaries and the erosion of so-called "mere conduit" protections.[32] Private sector solutions, such as the Internet Watch Foundation in the United Kingdom and INHOPE, an international network of hotlines dealing with illegal content online, first established by Internet service providers, have been effective in combatting child abuse images. Another self-organized response is the EFF's Manila Principles (2015a), which set out guidance for laws and content restriction policies.

The difficulties of having private sector entities decide on complex issues such as the intersection between privacy and freedom of expression is illustrated with the example of Google's "Right to Be Forgotten" process.

Google and the Right to Be Forgotten

A Spanish individual brought a case against Google, complaining that news articles reporting on his historic (and resolved) financial difficulties remained at the top of Google search results on his name. The Court of Justice of the European Union[33] required Google to respect individuals' "right to be forgotten" by removing from search engine results links to historic web content. In response to the judgment, Google created a system to handle complaints.[34] To date, Google's system has handled more than 250,000 requests relating to 900,000 URLs (Williams 2015).

The systems, criteria and people involved in screening and making judgments to take down materials are not widely discussed. The quality of decisions under Google's Right to Be Forgotten process has been criticized. Even the privacy-orientated European Commission, after the process had been invoked to remove articles from the BBC business service, said that the ruling should not allow people to "Photoshop their lives" (quoted in Cooper 2014).

Part of the problem is that there is not enough information to determine how far Google's process fulfills basic rule of law requirements. The identity of those making the decisions is not revealed, nor are other due process considerations, such as whether decision-makers are subject to conflict-of-interest checks, which factors are taken into account and which are excluded in reaching decisions, and what rights of appeal exist for the parties. A small number of case studies are published, but reasoned decisions are not. An open letter to Google signed by 80 experts in technology and privacy law recently called for greater transparency in the process (Kiss 2015).

31 See www.youtube.com/yt/press/en-GB/statistics.html.

32 "The burden of such policing is transferred to private intermediaries, such as search engines and social network platforms, through laws that widen liability for proscribed content from the original speaker to all intermediaries" (UN 2013).

33 See *Google Spain v AEPD & Costeja-González* [2014] EUECJ C-131/12.

34 Google's Right to be Forgotten form "Search removal request under data protection law in Europe," https://support.google.com/legal/contact/lr_eudpa?product=websearch.

By contrast, ICANN's Uniform Domain-Name Dispute Resolution Policy (UDRP) has been in place since 1999 and has handled more than 40,000 cases — a single process to deal with domain disputes in any jurisdiction. It has provided a model for other domain name dispute mechanisms. Cases are filed online; there are written submissions, independent decision makers, published decisions; online materials offer guidance to practitioners and — in some variants of the UDRP, such as the .uk registry's (Nominet) Dispute Resolution Service and ICANN's Uniform Rapid Suspension process — the possibility of appeal. The UDRP and other domain name dispute mechanisms conform well to the rule of law.

It is true that the volume of content, and therefore of disputes, on the popular platforms is far greater than the volume of domain name disputes, but why should this be Google's problem to solve? Jonathan Zittrain (2014) responds, "If Google can process 70,000 requests, so can and should the data protection authorities." Zittrain reminds us that neither Google nor any other large platform provider has actively sought this work. They have had it thrust upon them by a mixture of inaction by states and ad hoc court decisions. But, having taken on the job, Google should be applying rule-of-law principles (open justice, conflict of interest, transparency, appeal). The example of the UDRP shows that a mixture of transparency, outsourcing decision making to others and automating the *process*, rather than the decision making, affords flexibility and allows dispute mechanisms to scale without sacrificing due process. According to Google, there are "no plans…to share individual decisions or aggregate them in a transparency-report-like format."[35]

CONTENT MODERATION: AN ILLUSION OF AUTOMATION

The popular web platforms, including Google, Facebook, Twitter and Yahoo, provide unprecedented opportunities for freedom of expression. Their intuitive tools have significantly lowered barriers to the publication of rich media — video, web pages and photographs — enabling individuals and small businesses to reach global audiences. Overwhelmingly, the impact on freedom of speech is positive. The US First Amendment ethos of the providers creates a permissive attitude toward all sorts of content.

But even in the most freewheeling environments, some types of content can cause real harm. Women who take a public position on social media are vulnerable to abuse — much of which is of a sexual or violent nature. In 2013, Caroline Criado Perez campaigned for the Bank of England to include at least one portrait of a celebrated woman on future bank notes. Perez suffered "life-changing psychological effects from the abuse she received on Twitter," according to evidence given in the trial of two of the "trolls" (quoted in BBC News 2014).

These are not isolated incidents. One study concluded that 40 percent of Internet users have experienced online harassment, and that young women "experience certain types of harassment at disproportionately high levels," namely cyberstalking, online sexual harassment and physical threats (Duggan et al. 2014). Mary Beard (2014) places the phenomenon within the classical world's tradition of rhetorical speech and persuasion, in which "women who claim a public voice get treated as freakish androgynes." "Do those words matter?" she has asked. "Of course they do, because they underpin an idiom that acts to remove the authority, the force, even the humour from what women have to say" (ibid.).

All the large platform providers operate reactive notice-and-takedown systems. Users can flag "abuse" and content is then referred to human assessors for screening. It is difficult to obtain information about the number of complaints the providers handle or their processes. "Both Facebook and Twitter have in recent years grown more transparent about how they respond to government requests for content restriction….However...both companies are much more opaque about their internal decision-making processes around how and when their own rules are enforced" (MacKinnon et al. 2014, 152).

Sarah T. Roberts (2015) describes the tens of thousands of staff — often subcontracted through technical outsourcing companies such as Mechanical Turk or oDesk — who are removing abusive content, including hard core pornography and beheadings from users' newsfeeds: "Companies like Facebook and Twitter rely on an army of workers employed to soak up the worst of humanity in order to protect the rest of us. And there are legions of them…well over 100,000…about twice the total head count of Google and nearly 14 times that of Facebook."[36] According to Roberts, the workers "are really sophisticated. They are graduates of elite universities, providing a service so others don't have to."[37]

Facebook did not respond to requests for interviews for this paper, but Google agreed to be interviewed and gave an indication of the challenges presented: "Our enforcement team, staffed around the world, reviews flagged videos 24 hours a day, 7 days a week. We review more than 100,000 flagged videos each day. In 2014, we removed 14 million videos from YouTube that violated our Community Guidelines."[38]

35 Google UK, email follow-up to interview for this paper, March 31, 2015.

36 See also Chen (2014).

37 Sarah T. Roberts, interview for this study, December 2014.

38 Google UK, interview, March 31, 2015.

Arbitrating content issues involves complex value judgments, and — in an international context — requires sensitivity about cultural diversity and making difficult decisions about conflicts of law. Even cultures that are broadly aligned — such as the United States and Europe — still have marked differences in their approaches to controversial issues. For example:

- Reactions to the Right to Be Forgotten judgment on each side of the Atlantic have revealed differences in US and EU attitudes about privacy and freedom of expression: "In America the First Amendment's free-speech provision usually trumps privacy concerns" (*The Economist* 2014). Is the Right to Be Forgotten process a welcome redress for individuals who want to "grow and get beyond these incidents in their past" (Viktor Mayer-Schönberger, quoted in Toobin 2014) or a "terrible danger," only acceptable to "authoritarian dictators" (Wikipedia founder Jimmy Wales, quoted in Lomas 2014)?

- Determinations on copyright infringement can be complex and involve weighing whether any of the relevant exemptions apply (for example, fair use, limited terms, and the first sale doctrine),[39] yet Google complied with 97 percent of the requests it received between July and December 2011 to remove content that allegedly infringed copyright.[40] With such an implausibly high take-down rate, can one truly have confidence in the rigour of the assessment? There is simply not enough published information to be sure.

- Depictions of nudity seem more likely to offend sensibilities in the United States than in Europe. Following a campaign by "lactivists" (Burns 2007), Facebook's Community Standards now provide an express exception from its ban on nudity for pictures of breastfeeding[41]; Apple was criticized for "censoring" a "pixelated, low-res nudity — which is seen when you use a body scanning X-ray machine" in the app *Papers, Please* (Moore 2014).

- The EFF reports that "on Instagram, there have been several examples of larger women posing semi-clad, which have been taken down, or women with body hair, whereas pictures of thinner women are left up. Who is doing this? What is their demographic?"[42]

Human rights laws limit freedom of expression in certain situations, and companies are evolving self-regulatory processes to remove content that they feel would be covered by those limitations (or breach their acceptable-use policies). However, when cultural, political and legal differences become more pronounced, decisions on content moderation become more complex. For example:

- Scenes from war zones raise particular sensitivities. On the one hand, graphic depictions of individuals dying violently erode the individuals' inherent dignity (and rights to privacy) and can cause harm to vulnerable or young viewers. On the other hand, there is a clear public interest in sensitive reporting from war zones, subject to clear and consistent guidelines. Sarah T. Roberts interviews content moderators working for major web platforms, who contrast the handling of violent content from two separate conflict situations, Syria and Mexico:

  > The drug war that is going on in Mexico — a lot of the people who are on both sides were uploading videos of the war. Murders or hostages and interrogations. Stuff that we keep up for the war that is going on in Syria. The exact same content. I mean, it's for a different reason, but the content is the same. There are two sides, for all purposes it's the same content. But the argument they [the platform provider] gave me was that it wasn't newsworthy enough. The drug war….So it just feels like there is a double standard, and my understanding [from that] is that one person on the SecPol team is just passionate about the issues in the Middle East. (Quoted in Roberts 2015)

  The example illustrates a lack of consistency in approach.

- In Egypt, although homosexuality is not illegal, "homosexual acts in public are illegal and homosexuals have been convicted for breaching laws on public decency" (Gov.uk n.d.). Jillian York of the EFF recounts how a Cairo journalist allegedly colluded with police and reported on a gay men's club.[43] As a result, pictures were posted on a social network of identifiable people without their permission, in violation of the platform's terms. According to York, the pictures were a threat-to-

39 For an exploration of copyright and the online environment, as well as the dangers of outsourcing evaluation of copyright infringement to machines, see Lessig (2006, 186 ff.).

40 See www.google.com/transparencyreport/removals/copyright/faq/#compliance_rate. No data on compliance is provided beyond the six-month window July–December 2011.

41 Within the section "Encouraging respectful behavior" on its Community Standards page, Facebook (2015a) states: "We also restrict some images of female breasts if they include the nipple, but we always allow photos of women actively engaged in breastfeeding." Other allowable nudity includes "showing breasts with post-mastectomy scarring...photographs of paintings, sculptures and other art." www.facebook.com/communitystandards/.

42 Jillian York, of EFF, interview for this study, December 2014.

43 Ibid.

life situation for the men tagged in the photographs: "Egyptian friends complained to the provider. The provider [based in Silicon Valley] did not take down the pictures even though it was in clear violation of their policy. It took a phone call from the EFF before the content was removed." Does this example illustrate a clash of cultures? Would an operative in the more permissive environment of California have an understanding of the different cultural norms applying to overt displays of homosexuality in Egypt? Should the process be so vulnerable to interventions by individuals or US organizations?

- Most people would welcome a decision by Twitter to remove videos of the beheading by the Islamic State of Iraq and al-Sham (ISIS) of the American journalist James Foley. Jay Kang (2014) of *The New Yorker* points out inconsistencies in Twitter policy decisions: "It's odd to think that a company that allows thousands of other gruesome videos, including other ISIS beheadings, would suddenly step in. Twitter, for example, allows creepshot accounts, in which men secretly take photos of women in public....Where, exactly is the enforcement line?" This decision on content moderation clearly would have been difficult for whoever had to make it. When such choices are made in private, without transparency, there is greater scope for inconsistency in approach, to the detriment of fundamental rights.

Making the right decision is difficult. In extreme cases, such as images of child abuse, the content is illegal in most jurisdictions — the content is appalling, but the decision to remove it is straightforward. For the most part, the line between what is acceptable and unacceptable is not so easy to draw; decisions are difficult and nuanced, and different cultures have varying levels of tolerance.

The Association for Progressive Communications criticizes Facebook, YouTube and Twitter for their "reluctance to engage directly with technology-related violence against women, until it becomes a public relations issue" (Nyst 2014). The reluctance in part stems from the awkward transition from being neutral platforms to being publishers, a transition that the platforms have not looked for and have yet to come to terms with. On the one hand, they risk adverse publicity or alienation of their user base if they fail to act; on the other, they might erode their legal protections as intermediaries (thereby threatening their business model) if they take responsibility for user-created content on their platforms. Conflicting statements highlight the duality: Twitter's former general counsel once described the company as "the free speech wing of the free speech party" (quoted in Ball 2014). More recently, according to a leaked internal memo, Twitter's then CEO Dick Costolo said, "We suck at dealing with abuse and trolls," and promised to "start kicking these people off right and left and making sure that when they issue their ridiculous attacks, nobody hears them" (Tiku and Newton 2015).

While there is a sense that "something should be done" by *somebody*, it is less clear *what* should be done, *by whom* and *according to what criteria*.

In the absence of *somebody* coming forward to moderate online content according to the public interest and rule of law, Internet platforms have had to step into the vacuum left by public authorities. Zittrain (2014) points up the "incongruity of having Google — or any private party, for that matter — as a decision maker about rights."

To whom will content moderators be accountable? What redress mechanisms will exist for those who believe the wrong decision has been made? Difficult decisions relating to content are not confined to the Internet. The British Board of Film Classification (BBFC) publishes guidelines, conducts research on changing social values and provides brief explanations for each film classification choice. "We have a simple approach. Listen to the public, and tell the public what we're doing," says the BBFC's President Patrick Swaffer.[44]

The Internet platform providers' lack of both transparency about their processes and public commitment to human rights standards other than freedom of speech help to perpetuate what Sarah T. Roberts terms a "collective hallucination that these things are done by a machine rather than people, perpetuating a myth of the Internet as a value-free information exchange with no costs."[45] There are few public discussions about the rules applied by providers or about their workers' conditions and the psychological impact on those workers of long-term exposure to harmful content.

THE ILLUSION OF NEUTRALITY AND THE NEED FOR ETHICS

On November 2, 2010, Congressional elections were held in the United States. Interested in discovering the extent to which voter behaviour is socially influenced, researchers, with Facebook's cooperation, selected 61 million US users at random and reviewed the effectiveness of different messages posted on their timelines. Some were shown a simple link to the local polling information. For others, a clickable "I voted" button was added to the link. For others, six small thumbnail pictures of friends were also added to the link and button. A control group was shown nothing at all. The result: turnout increased by 60,000 directly, and

44 Patrick Swaffer, interview, January 6, 2015. The BBFC's vision statement is to "respond to and reflect changing social attitudes towards media content through proactive public consultations and research" (BBFC 2014) .

45 Sarah T. Roberts, interview, December 18, 2014.

through social contagion, up to 280,000 voters. Voters were most likely to vote if they saw that their friends had done so (Bond et al. 2012).

In January 2012, in a week-long experiment, researchers, with Facebook's cooperation, exposed 690,000 randomly selected users to different types of emotional content. One group was exposed to friends' positive emotional content; the other to friends' negative emotional content. The experiment showed that emotions are contagious (Kramer, Guillory and Hancock 2014).

No information is given as to how the users in each experiment were selected, whether they gave consent and whether they were screened for vulnerabilities (for example, depression or suicidal thoughts). Off-line psychological experiments are subject to stringent ethics, yet no information was provided in the Facebook studies as to how they satisfied ethical requirements.

The experiments highlight concerns about the power of large platform providers to influence human behaviour. The platforms are not as neutral as they seem. Content that users take for granted as being neutral — search results, friends' updates — are personalized. The algorithms of the leading providers are secret, so users do not understand why Facebook thinks a user prefers one friend over another. Search engines "restrict or modify search results for many…commercial and self-regulatory reasons, including user personalization and enforcement of companies' own rules about what content is acceptable to appear on their services" (MacKinnon et al. 2014, 11-12) but it is not clear how those decisions are made.

Of course, it is not good business to betray the trust of your users, and the companies — surprised by the backlash last time (see, for example, D'Onfro 2014) — might decide to do things differently in future. But the decision will be theirs alone. The experiments were pre-consented to in their terms and conditions.

Today's major providers have not only the platforms with which to experiment on their unwitting users but also privileged access to sensitive data. Some scholars have called for popular online service providers to be designated "information fiduciaries," thereby creating obligations — similar to those of lawyers or doctors — not to use the information entrusted to them for outside interests (Balkin 2014).

ANALYSIS: PUBLIC ATTITUDES ABOUT PRIVACY

What does the Internet-using public think about Internet providers' intrusion into their privacy or curtailment of their freedom of expression? Does the public care? Do people understand what is happening to their data? Even if they do know, and do care, what can they do about it, short of opting out of online life (and thereby much of off-line life, too)?

Is Human Nature Changing?

One possibility is that the Internet has changed people, or at least their attitudes to what should be private or public. Noam Chomsky refers to "the exhibitionist character of the internet," noting that "younger people are less offended by this than the older generation" (quoted in Harvey 2013). While Chomsky is correct in saying that companies seem to be conspiring with young people — and not only young people — to parade their private lives in public, concluding that human nature has changed does not follow — at least not without reviewing some other possibilities.

It is more likely that the Internet platforms are not quite attuned to the subtleties of human interactions. Facebook's CEO Mark Zuckerberg (quoted in Kirkpatrick 2010, 199) stated, "You have one identity. The days of you having a different image for your work friends or co-workers...are probably coming to an end pretty quickly." Schneier (2015, chap. 10) takes Zuckerberg to task for his "remarkable naiveté": "We are not the same to everyone we know and meet. We act differently when we're with our families, our friends, our work colleagues and so on….It's not necessarily that we're lying, although sometimes we do; it's that we reveal different facets of ourselves to different people. This is something innately human. Privacy is what allows us to act appropriately in whatever setting we find ourselves."

It is also difficult for people to conceptualize that there is a dual audience for their Internet content: their friends on the one hand, the platform provider and those it chooses to share with on the other. "Viewing a YouTube video seems like a private action. Searching for medical information about a recently diagnosed condition in the privacy of one's living room seems like a private action" (DeNardis 2014). Sharing with one's friends within a social network feels like a social action with known recipients. The online platforms support this illusion, giving users an array of intuitive tools to control their privacy settings, even at the level of individual updates. So, users can choose whether their content goes to friends, friends-of-friends (on average 31,000 others[46]) or is public. Choices might depend on which facets of ourselves a particular post reveals. But certain choices are off limits. The standard terms analysis above shows how the world's most popular platform providers give themselves and third-party advertisers

46 According to Keith Hampton et al. (2012): "At two degrees of separation (friends-of-friends), Facebook users in our sample can on average reach 159,569 other Facebook users. However, the relatively small number of users with very large friends lists, who also tended to have lists that are less interconnected, overstates the reach of the typical Facebook user. In our sample, the maximum reach was 7,821,772 other Facebook users. The median user (the middle user from our sample) can reach 31,170 people through their friends-of-friends."

unfettered access to user content, including the ability to delete, edit and share that content with any third party. Individuals have no user tools or any chance to opt out to limit what the platform can do with their data.

Does the Public Trust Companies' Data Handling?

Survey evidence suggests that while there might be some tolerance, even support, for government gaining access to data in certain circumstances,[47] attitudes harden when it comes to private companies. "Public surveys have shown particularly low levels of trust in relation to phone companies and ISPs in dealing with data. A recent survey showed only between 4% and 7% had high levels of trust in such companies to use their data appropriately. They also show a general lack of confidence in the security of everyday channels, social media being viewed as the least secure" (as cited by Anderson 2015b, 34). A study of 23,000 Internet users from across the world for the Global Commission on Internet Governance indicates that 74 percent of users are concerned about companies monitoring online activities and then selling that information.[48] According to the Pew Research Center, 93 percent of adults say that being in control of *who* can get information about them is important; 90 percent say that controlling *what* information is collected about them is important (Madden and Rainie 2015).

So, either there is a gap between what people are saying in their survey responses and what they are doing online, or something else is at play.

Does the Public Understand the Deal?

It is known that few people read or have the legal training to understand privacy policies. One study estimates that "if all American Internet users were to annually read the online privacy policies word-for-word each time they visited a new site, the nation would spend about 54 billion hours reading privacy policies" (McDonald and Cranor 2008, 563). Ian Brown and Christopher T. Marsden (2013, 54) comment that "there is increasing evidence from behavioural economics that a 'consent' model has significant failings…. Privacy-related decisions are heavily context specific, dependent, for example on how much a user is thinking about privacy at the time, along with his or her trust in the other party and often-inaccurate assumptions about how data will be used."

My Way or the Information Superhighway

It is evident that the standard terms of today's leading providers provide no mechanisms for users to opt out of having their data shared with third parties; nor are there paid alternatives (without advertising) for most services.

Google currently has more than 90 percent of the European search market. Facebook has 1.3 billion users. The existing all-or-nothing deal risks excluding people from what have become intrinsic parts of daily life.

Providers also exhibit a homogenous approach to data: communications that are private in nature seem to be handled in the same way as communications that are more public; information that, in off-line life, humans are programmed to forget — such as the content of most chat conversations, or where we were at a particular date and time — is stored indefinitely, apparently in the same way as more permanent content, for example, YouTube videos.

CONCLUSIONS AND RECOMMENDATIONS

Human rights laws apply to states, not to private companies, reflecting the different realities for governments versus private entities. Governments can pass whatever legislation they wish, subject only to human rights standards. Meanwhile, private companies are subject to a plethora of laws. When a successful company starts to operate on a multinational basis, the regulatory and legal landscape becomes complex. Multinationals often have to contend with conflicting laws, regulations and norms across the international field of their operations.

However, multinationals can have an impact on human rights and the Ruggie Principles of "protect, respect and remedy" offer a framework to help companies understand and respond to their responsibilities. At the same time, states must be vigilant in monitoring the impact private actors have on human rights, redressing imbalances where necessary. While the impact of companies in the off-line world can be direct and obvious, online companies' acts or omissions can also lead to direct harm. A more insidious harm is that the erosion of fundamental rights becomes normalized.

The early, open phase of the Internet's development has given way to a highly concentrated market for web content provision. Today's popular Internet platforms have lowered the barriers to freedom of expression and access to knowledge. Attitudes about sharing what used to be considered private might be changing. At the same time, the complexity of today's online data market and the unpredictable afterlife of our online communications when correlated with other big data sources make traditional consent models (which underpin the business models of the big platforms) ineffective. How can a provider frame

47 See, for example, TNS-BMRB Polling January 23–27, 2014: 71 percent of respondents "prioritise reducing the threat posed by terrorists and serious criminals even if this erodes people's right to privacy."

48 "CIGI-Ipsos Global Survey on Internet Security and Trust." November 24, 2014. www.cigionline.org/internet-survey.

terms that give consent for uses of data that have not yet been thought of, except by giving themselves the widest possible scope?

While people might be fairly relaxed about the reprocessing of data that is public in nature, such as tweets, blogs or YouTube videos, the picture is less clear with communications that appear private and transient — such as chat or location data. Nevertheless, these data are being scanned, processed and sold in just the same way.

States are seeking ways to reduce the cost and increase the effectiveness of surveillance by using online data — and states have to rely on the skills, resources and data of private companies. Commentators have noted the "powerful feedback loop" in which the ever-more intrusive data collection and processing by the private sector support the desire of governments to process such data for national security purposes. The current situation aligns the interests of two powerful actors: states and multinationals. This alignment poses democratic risks, as well as making regulatory interventions to limit such data collection unlikely.

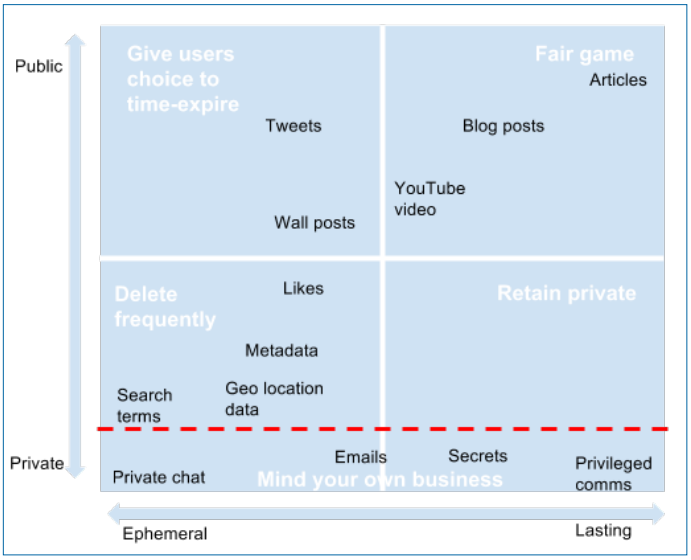
What Needs to Happen?

States need to review and, if necessary, reassert their human rights obligations in the online environment, rather than rely on ad hoc mediation of these rights by private companies.

Companies need to differentiate between private and public communications in their terms, and to limit their intrusion into private communications to what is necessary, proportionate and pursuant to a legitimate aim. Rather than treating all types of user data as homogenous (and fair game), policy makers need to recognize that not all data is created equal and that certain types of communications, such as legally privileged, intimate, confidential information and emails, need to be kept away from prying eyes — even of the platform providers. Meanwhile, other types of communications that are inherently ephemeral in nature should automatically expire and be deleted from the platform providers' systems (see Figure 5 for a possible model).

Particular care is required when dealing with data of young and vulnerable users. Google is piloting a service, YouTube Kids, in the United States, which limits advertising (della Cava 2014),[49] but it is not clear how far the tracking and mining of user behaviour and data are also limited.

Figure 5: User Data on Proprietary Platforms — An Evolution?



Source: Author.

In the first instance, companies are best placed to make such distinctions through self-regulatory mechanisms, as these are likely to be more practical across national borders than a hodgepodge of national regulation. Platform providers might extend tools for users with which to make privacy choices such as expiry dates or preferences, which would also include limits of intrusion for the platform providers themselves.

There needs to be a collective effort for platform providers to arrive at deletion policies for data that is ephemeral in nature (such as chat messages) or which could give rise to human rights risks (such as historic location data).

Many users are not concerned about what happens to their data, or accept it as part of the bargain in using a free platform. Others do care, and they should be offered some alternative — such as a limited opt-out or an option of a paid subscription — other than exclusion from services that are now becoming embedded in daily life.

Recent judgments from the Court of Justice of the European Union reasserting fundamental rights in the online environment stand in stark contrast to the lack of leadership shown by states, which appear fearful of ensuring that powerful multinational platform providers are fulfilling the states' human rights obligations.

Other actors need to assist multinationals to arrive at realistic and robust processes for content moderation that comply with international human rights standards. Processes need to be more transparent; the decision makers and their freedom from conflicts of interest need to be clearly identified; and appeals mechanisms need to be introduced.

49 See "Advertising on YouTube Kids" about the restrictions on advertising: https://support.google.com/youtube/answer/6168681.

Pleading that the Internet is always different — digital exceptionalism — can be misleading. The scale of the Internet's data generation and management is enormous and the international nature of its services lends complexity. But these issues — and their potential solutions — are not unique to the digital world. An abundance of hard-learned lessons from other sectors, such as film classification, or even the extraction industries, could provide insight into the task of navigating the issues and responding to changing social attitudes. It should be possible to evolve independent monitoring bodies using the combined efforts of private, voluntary and state vehicles.[50] Most importantly, this work must be done transparently, effectively and responsibly.

Acknowledgements

I would like to thank the many people who have helped and guided me with this project: The team at CIGI, Eric Jardine, Samantha Bradshaw, Lynn Schellenberg and Fen Hampson, and at Chatham House, Caroline Baylon, Hannah Bryce and Patricia Lewis. Members of the Global Commission on Internet Governance, especially the incomparable Laura DeNardis, who provided invaluable input on early ideas for this paper. Professor Ian Brown of the Oxford Internet Institute, for suggestions about sources and reading materials. Sarah Roberts of Western University, London, Canada, for background on content moderation practices and for generously sharing extracts from her research. Jillian York of EFF (always an inspiration), for real-life examples from the Middle East. Patrick Swaffer of the BBFC, for patiently explaining approaches to content moderation in the off-line environment. Thanks also go to: Brittany Smith of Google, the only representative of the big online platforms who agreed to be interviewed (or even to answer emails from me). Rebecca MacKinnon, Jean-Jacques Sahel and many others who have helped me. Will Eaves, who gave editorial advice on early drafts, and my family — Lucien, Alice and Patrick — who put up with a very distracted wife and mother for too many months. Lastly, my thanks to the late Caspar Bowden, whose work I have long admired, who spoke with me at length for this project, and to whom this paper is respectfully dedicated.

50 For example, the BBFC is a private, non-profit company, its president appointed by the Secretary of State; CARA (Classification and Rating Administration), the US system for film classification, is voluntary; the Swedish Media Council has taken on a role originally done by the police.

WORKS CITED

Acar, Gunes, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan and Claudia Diz. 2014. "The Web Never Forgets: Persistent Tracking Mechanisms in the Wild." Session at the 21st ACM Conference on Computer and Communications Security, Scottsdale, AZ, November 5.

Access. n.d. "Silicon Valley Standard." https://s3.amazonaws.com/access.3cdn.net/d9369de5fc7d7dc661_k3m6i2tbd.pdf.

Alexa.com. 2015. "The Top 500 sites in each country or territory." www.alexa.com/topsites/countries.

Anderson, David. 2015a. "Statement by the Independent Reviewer of Terrorism Legislation on Publication of the Report of the Investigatory Powers Review ('A Question of Trust')." Press release, June 11. https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/#more-2364.

———. 2015b. *A Question of Trust: Report of the Investigatory Powers Review*. H M Government, June 15. https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf.

Balkin, J. 2014. "Information Fiduciaries in the Digital Age." *Balkanization* (blog), March 5. http://balkin.blogspot.co.uk/2014/03/information-fiduciaries-in-digital-age.html.

Ball, James. 2014. "Twitter: from free speech champion to selective censor?" *The Guardian*, August 21. www.theguardian.com/technology/2014/aug/21/twitter-free-speech-champion-selective-censor.

Ball, James, Luke Harding and Juliette Garside. 2013. "BT and Vodafone among telecoms companies passing details to GCHQ." *The Guardian*, August 2. www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.

BBC News. 2014. "Two guilty over abusive tweets to Caroline Criado-Perez." BBC.com, January 7. www.bbc.co.uk/news/uk-25641941.

BBFC. 2014. *BBFC Guidelines 2014 Research Report*. www.bbfc.co.uk/sites/default/files/attachments/2014%20Guidelines%20Research.pdf.

Beard, Mary. 2014. "The Public Voice of Women." *London Review of Books* 36 (6): 11–14. www.lrb.co.uk/v36/n06/mary-beard/the-public-voice-of-women.

Bond, Robert M., Christopher J. Fariss, Jason J. Jones, Adam D. I. Kramer, Cameron Marlow, Jaime E. Settle and James H. Fowler. 2012. "A 61-million-person experiment in social influence and political mobilization." *Nature* 489: 295–98. doi:10.1038/nature11421.

Brown, Ian and Christopher T. Marsden. 2013. *Regulating Code: Good Governance and Better Regulation in the Information Age.* Cambridge MA: MIT Press.

Burns, Matt. 2007. "Breast Isn't Best on Facebook." *TechCrunch*, September 7. http://techcrunch.com/2007/09/07/breast-isnt-best-on-facebook/.

Chen, Adrien. 2014. "The laborers who keep dick pics and beheadings out of your Facebook feed." *Wired*, October 23. www.wired.com/2014/10/content-moderation/.

Clay Large, David. 2001. *Berlin: A Modern History.* London, England: Allen Lane.

Cooper, Paul. 2014. "Embarrassed EC: Right to be forgotten not a right to 'Photoshop your life.'" IT Pro Portal, July 4. www.itproportal.com/2014/07/04/embarrassed-ec-says-right-be-forgotten-not-designed-photoshop-your-life-google-eu-robert-peston-bbc/#ixzz3uyQls6xv.

Council of Europe. 2014a. *Recommendation CM/Rec(2014)6 of the Committee of Ministers to Member States on a Guide to Human Rights for Internet Users* (adopted by the Committee of Ministers on April 16, 2014, at the 1197th meeting of the Ministers' Deputies). https://wcd.coe.int/ViewDoc.jsp?id=2184807.

———. 2014b. "The Rule of Law on the Internet and in the Wider Digital World." Issue Paper by the Council of Europe Commissioner for Human Rights. www.coe.int/t/dghl/standardsetting/media/cdmsi/Rule_of_Law_Internet_Digital_World.pdf.

Deibert, Ronald. 2013. *Black Code: Inside the Battle for Cyberspace.* Toronto, ON: McClelland & Stewart.

della Cava, Marco. 2014. "Google to revamp its products with 12-and-younger focus." *USA Today*, December 3. www.usatoday.com/story/tech/2014/12/03/google-products-revamped-for-under-13-crowd/19803447/.

DeNardis, Laura. 2014. *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Desta, Yohana. 2014. "12 Things Gmail's User Base Dwarfs in Size." Mashable.com, April 1. http://mashable.com/2014/04/01/gmail-user-base-size/.

D'Onfro, Jillian. 2014. "Facebook Apologizes for Its Huge Psychological Experiment on Users and Explains How It Will Do Future Research Differently." *Business Insider*, October 2. www.businessinsider.com/facebook-cto-mike-schroepfer-apologizes-for-facebook-experiment-2014-10?IR=T.

Duggan, Maeve, Lee Rainie, Aaron Smith, Cary Funk, Amanda Lenhart and Mary Madden. 2014. "Online Harassment." Pew Research Center, October. www.pewinternet.org/files/2014/10/PI_OnlineHarassment_102214_pdf1.pdf.

Duhigg, Charles. 2012. "How Companies Learn Your Secrets." *The New York Times Magazine*, February 16. www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=1&_r=2&hp.

Eckersley, Peter and Kurt Opsahl. 2014. "White House Website Includes Unique Non-Cookie Tracker, Conflicts with Privacy Policy." EFF, July 22. www.eff.org/deeplinks/2014/07/white-house-website-includes-unique-non-cookie-tracker-despite-privacy-policy.

EFF. 2015a. "Manila Principles on Intermediary Liability: Best Practices Guidelines for Limited Intermediary Liability for Content to Promote Freedom of Expression and Innovation." Version 1.0, March 24. www.eff.org/files/2015/10/31/manila_principles_1.0.pdf.

———. 2015b. "Who Has Your Back? 2015: Protecting Your Data from Government Requests." www.eff.org/who-has-your-back-government-data-requests-2015#download.

Facebook. 2015a. Community Standards. www.facebook.com/communitystandards/.

———. 2015b. "Help Center. Manage Your Account: Downloading Your Info." www.facebook.com/help/131112897028467/.

Federal Trade Commission. 2014. *Data Brokers: A Call for Transparency*. May 2014. www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

Finnegan, Shawna. n.d. "United Nations Resolutions Recognizing Human Rights Online." Association for Progressive Communication blog. www.apc.org/en/blog/united-nations-resolutions-recognising-human-rights.

Fischer, Eric. 2010. "Locals and Tourists." www.flickr.com/photos/walkingsf/sets/72157624209158632/with/4671589629/.

———. 2014. "Making the most detailed tweet map ever." Mapbox blog, December 3. www.mapbox.com/blog/twitter-map-every-tweet/.

Gardbaum, Stephen. 2008. "Human Rights as International Constitutional Rights." *European Journal of International Law* 19 (4): 749–68.

Geere, Duncan. 2013. "Google goes down for a few minutes, web traffic drops 40 percent." *Wired.co.uk*, August 17. www.wired.co.uk/news/archive/2013-08/17/googledip.

Global Network Initiative. 2012. "Participants." http://globalnetworkinitiative.org/participants/index.php?qt-gni_participants=1#qt-gni_participants.

Gore, Al. 2014. "A fireside chat with Al Gore," 2014 Southland Conference: Technology + Southern Culture, Nashville, TN, June 9–12.

Gov.uk. n.d. "Egypt Travel Advice." Updated November 18, 2015, still current at December 17, 2015. www.gov.uk/foreign-travel-advice/egypt/local-laws-and-customs.

Graham, Mark and Stefano De Sabbata. 2013. "Age of Internet Empires." Internet Geographies, Oxford Internet Institute. geography.ii.ox.ac.uk.

Guardian US Interactive Team. 2013. "A Guardian Guide to Your Metadata." *The Guardian*, June 12. www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000.

Hampton, Keith, Lauren Sessions Goulet, Cameron Marlow and Lee Rainie. 2012. "Why most Facebook users get more than they give." Pew Research Center, February 3. www.pewinternet.org/2012/02/03/why-most-facebook-users-get-more-than-they-give/.

Harris, David, Michael O'Boyle, Edward Bates and Carla Buckley, eds. 2014. *Law of the European Convention on Human Rights.* 3rd ed. Oxford, England: Oxford University Press.

Harvey, Fiona. 2013. "NSA surveillance is an attack on American citizens, says Noam Chomsky." *The Guardian*, June 19. www.theguardian.com/world/2013/jun/19/nsa-surveillance-attack-american-citizens-noam-chomsky.

Hern, Alex. 2014. "Former Microsoft employee arrested over Windows 8 leaks." *The Guardian*, March 20. www.theguardian.com/technology/2014/mar/20/former-microsoft-employee-arrested-over-windows-8-leaks?view=desktop.

International Crisis Group. 2008. "Nigeria: Ogoni Land after Shell." Crisis Group Africa Briefing No. 54. International Crisis Group, September 18. www.crisisgroup.org/~/media/Files/africa/west-africa/nigeria/B054%20Nigeria%20Ogoni%20Land%20after%20Shell.pdf.

Kahneman, Daniel. 2011. *Thinking Fast and Slow.* New York, NY: Farrar, Straus and Giroux.

Kang, Jay Caspian. 2014. "Should Twitter have taken down the James Foley video?" *The New Yorker*, August 21. www.newyorker.com/news/news-desk/twitter-taken-james-foley-video.

Kirkpatrick, David. 2010. *The Facebook Effect: The Inside Story of the Company That Is Connecting the World*. New York, NY: Simon and Schuster.

Kiss, Jemima. 2015. "Dear Google: open letter from 80 academics on the 'right to be forgotten.'" *The Guardian*, May 14. www.theguardian.com/technology/2015/may/14/dear-google-open-letter-from-80-academics-on-right-to-be-forgotten.

Kosinski, Michal, David Stillwell and Thor Graepel. 2013. "Private traits and attributes are predictable from digital records of human behavior." *Proceedings of the National Academy of Sciences of the United States of America* 110 (15): 5802–5. www.pnas.org/content/110/15/5802.full.

Kramer, A. D. I., Jamie E. Guillory and Jeffrey T. Hancock. 2014. "Experimental evidence of massive-scale emotional contagion through social networks." *Proceedings of the National Academy of Sciences of the United States of America* 111 (29): 8788–90.

Lessig, Lawrence. 2006. *Code Version 2.0.* New York, NY: Perseus Books.

Lomas, Natasha. 2014. "Jimmy Wales Blasts Europe's 'Right to Be Forgotten' Ruling as a 'Terrible Danger.'" *TechCrunch*, June 7. http://techcrunch.com/2014/06/07/wales-on-right-to-be-forgotten/.

MacAskill, Ewen. 2013. "NSA paid millions to cover Prism compliance costs for tech companies." *The Guardian*, August 23. www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid.

MacKinnon, Rebecca. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom.* New York, NY: Basic Books.

———. 2015. "Corporate Accountability Index 2015." Ranking Digital Rights Project. https://rankingdigitalrights.org/project-documents/2015-indicators/.

MacKinnon, Rebecca, Elonnai Hickok, Allon Bar and Hae-in Lim. 2014. "Fostering Freedom Online: The Role of Internet Intermediaries." UNESCO Series on Internet Freedom. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf.

Madden, Mary and Lee Rainie. 2015. "Americans' Attitudes about Privacy, Security and Surveillance." Pew Research Center, May 20. www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

Mayer-Schönberger, Viktor. 2009. *Delete: The Virtue of Forgetting in the Digital Age.* Princeton, NJ: Princeton University Press.

Mayer-Schönberger, Viktor and Kenneth Cukier. 2013. *Big Data: A Revolution That Will Transform How We Live, Work and Think*. London, England: John Murray.

McDonald, A.M. and L. F. Cranor. 2008."The Cost of Reading Privacy Policies." *Journal of Law and Policy* 43: 540–65.

Mendel, Toby, Andrew Puddephatt, Ben Wagner, Dixie Hawtin and Natalia Torres. 2012. *Global Survey on Internet Privacy and Freedom of Expression*. UNESCO Series on Internet Freedom. Paris, France: UNESCO. http://unesdoc.unesco.org/images/0021/002182/218273e.pdf.

Moore, Bo. 2014. "Apple's ridiculous censorship of the nudity in *Papers, Please*." *Wired*, December 12. www.wired.com/2014/12/papers-please-ios-censored/.

Morozov, Evgeny. 2013. *To Save Everything, Click Here.* New York, NY: Perseus Book Group.

Mowery, K. and H. Shacham. 2012. "Pixel Perfect: Fingerprinting Canvas in HTML5." Session at the Web 2.0 Security & Privacy 2012 Workshop, San Francisco, CA, May 24. www.w2spconf.com/2012/papers/w2sp12-final4.pdf.

NetMundial. 2014. "NetMundial Multstakeholder Statement." Netmunidal, April 24. netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf.

Nyst, Carly. 2014. "End violence: Women's rights and safety online." Association for rogressive Communications, July. www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf.

OHCHR. 1966. International Covenant on Civil and Political Rights (1966, 999 UNTS 171). www.ohchr.org/en/professionalinterest/pages/ccpr.aspx.

———. n.d. "What are Human Rights." www.ohchr.org/en/issues/pages/whatarehumanrights.aspx.

Omand, David. 2015. *Understanding Digital Intelligence and the Norms That Might Govern It*. Global Commission on Internet Governance Paper Series No. 8. Waterloo, ON: CIGI. www.cigionline.org/publications/understanding-digital-intelligence-and-norms-might-govern-it.

Ratomski, Andrew. 2015 "Impact of Facebook Downtime on Global Traffic." *GoSquared Engineering* (blog), January 27. https://blog.shareaholic.com/social-media-traffic-trends-01-2015/.

Roberts, Sarah T. 2015. "Behind the Screen: Digitally Laboring in Social Media's Shadow World." Unpublished manuscript, Western University, London, ON.

Robinson, Duncan. 2015. "Facebook wins latest case in class action privacy battle." *Financial Times*, July 1. http://app.ft.com/cms/s/4914b45c-1fd1-11e5-aa5a-398b2169cf79.html?sectionid=topics/topics/Data_protection.

Roosevelt, Eleanor. 1948. "The Struggle for Human Rights." Speech given at the Sorbonne, Paris. www.americanrhetoric.com/speeches/eleanorroosevelt.htm.

Schneier, Bruce. 2015. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York, NY: W. W. Norton & Co.

Schrems, Max. n.d. "Get your Data! Make an Access Request at Facebook!" *Europe versus Facebook* (blog). http://europe-v-facebook.org/EN/Get_your_Data_/get_your_data_.html.

Solove, Daniel. 2007. "'I've got nothing to hide' and other misunderstandings of privacy." *San Diego Law Review* 44: 745.

Stevenson, Burton, ed. 1964. *The Home Book of Quotations, Classical and Modern*. 9th ed. New York, NY: Dodd, Mead.

Sweeney, Latanya. 2000. "Simple demographics often identify people uniquely." Carnegie Mellon University. http://dataprivacylab.org/projects/identifiability/paper1.pdf.

Take Back the Tech. 2014. "Take Back the Tech's! Report Card on Social Media and Violence Against Women." www.takebackthetech.net/sites/default/files/2014-reportcard-en.pdf.

The Economist. 2014. "On being forgotten." *The Economist*, May17.www.economist.com/news/leaders/21602219-right-be-forgotten-sounds-attractive-it-creates-more-problems-it-solves-being.

Tiku, Nitasha and Casey Newton. 2015. "Twitter CEO: 'We suck at dealing with abuse.'" *The Verge*, February 4. www.theverge.com/2015/2/4/7982099/twitter-ceo-sent-memo-taking-personal-responsibility-for-the.

Toobin, Jeffrey. 2014. "The Solace of Oblivion." *The New Yorker*, September 29. www.newyorker.com/magazine/2014/09/29/solace-oblivion.

UN. 1948. General Assembly resolution 217 A, *Universal Declaration of Human Rights,* A/RES/217 (111) (10 December 1948). www.un.org/en/universal-declaration-human-rights/.

———. 2011a. *Report of the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises, John Ruggie; Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, A/HRC/17/31. March 21. www.ohchr.org/Documents/Issues/Business/A-HRC-17-31_AEV.pdf.

———. 2011b. Human Rights Committee, 102nd Session General Comment No. 34, July. www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf.

———. 2012. General Assembly resolution 20.8, *The promotion, protection and enjoyment of human rights on the Internet*, A/HRC/RES/20.8 (16 July 2012). http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.

———. 2013. General Assembly. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank la Rue*, A/HRC/RES/23.40 (17 April 2013). www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

Vaizey, Hester. 2014. *Born in the GDR: Living in the Shadow of the Wall.* Oxford, England: Oxford University Press.

Van Alsenoy, Brendan, Valerie Verdoodt, Rob Heyman, Jef Ausloos, Ellen Wauters and Güneş Acar. 2015. *From Social Media Service to Advertising Network: A Critical Analysis of Facebook's Revised Policies and Terms*. Draft report for Belgian Privacy Commission, March 31. www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-2.pdf.

Weber, Max. 1946. "Politics as a Vocation." In *From Max Weber: Essays in Sociology*, edited by Hans H. Gerth and C. Wright Mills, 77–128. Oxford, England: Oxford University Press.

Williams, Rhiannon. 2015. "Telegraph stories affected by EU 'right to be forgotten.'" *The Telegraph*, September 3. www.telegraph.co.uk/technology/google/11036257/Telegraph-stories-affected-by-EU-right-to-be-forgotten.html.

Winkler, Rolfe. 2015. "Google Wants to Sell You Auto Insurance." *Wall Street Journal* (blog), January 8. http://blogs.wsj.com/digits/2015/01/08/google-wants-to-sell-you-auto-insurance/.

Wong, Danny. 2015. "In Q4, Social Media Drove 31.2% of Overall Traffic to Sites [REPORT]." *Shareaholic Reports* (blog), January 26. https://blog.shareaholic.com/social-media-traffic-trends-01-2015/.

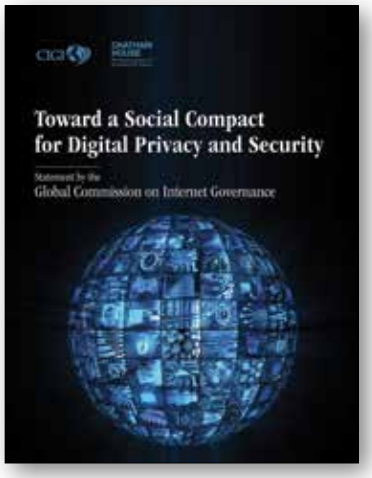
Wu, Tim. 2010. *The Master Switch: The Rise and Fall of Information Empires*. New York, NY: Knopf.

Zittrain, Jonathan. 2014. "Righting the right to be forgotten." *Future of the Internet* (blog), July 14. http://futureoftheinternet.org/2014/07/14/righting-the-right-to-be-forgotten/.

CIGI PUBLICATIONS
ADVANCING POLICY IDEAS AND DEBATE

Global Commission on Internet Governance

The Global Commission on Internet Governance (GCIG) was established in January 2014 to articulate and advance a strategic vision for the future of Internet governance. The two-year project conducts and supports independent research on Internet-related dimensions of global public policy, culminating in an official commission report that will articulate concrete policy recommendations for the future of Internet governance. These recommendations will address concerns about the stability, interoperability, security and resilience of the Internet ecosystem. Launched by two independent global think tanks, the Centre for International Governance Innovation and Chatham House, the GCIG will help educate the wider public on the most effective ways to promote Internet access, while simultaneously championing the principles of freedom of expression and the free flow of ideas over the Internet.



Toward a Social Compact for Digital Privacy and Security

Statement by the Global Commission on Internet Governance

On the occasion of the April 2015 Global Conference on Cyberspace meeting in The Hague, the Global Commission on Internet Governance called on the global community to build a new social compact between citizens and their elected representatives, the judiciary, law enforcement and intelligence agencies, business, civil society and the Internet technical community, with the goal of restoring trust and enhancing confidence in the Internet. It is now essential that governments, collaborating with all other stakeholders, take steps to build confidence that the right to privacy of all people is respected on the Internet. This statement provides the Commission's view of the issues at stake and describes in greater detail the core elements that are essential to achieving a social compact for digital privacy and security.

Finding Common Ground

A Briefing Book Prepared for the Global Commission on Internet Governance

This briefing book contextualizes the current debate on the many challenges involved in Internet governance. These include: managing systemic risk — norms of state conduct, cybercrime and surveillance, as well as infrastructure protection and risk management; interconnection and economic development; and ensuring rights online — such as technological neutrality for human rights, privacy, the right to be forgotten and the right to Internet access.

GLOBAL COMMISSION ON INTERNET GOVERNANCE PAPER SERIES

The Regime Complex for Managing Global Cyber Activities
GCIG Paper Series No. 1
Joseph S. Nye, Jr.

Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate
GCIG Paper Series No. 2
Tim Maurer and Robert Morgus

Legal Mechanisms for Governing the Transition of Key Domain Name Functions to the Global Multi-stakeholder Community
GCIG Paper Series No. 3
Aaron Shull, Paul Twomey and Christopher S. Yoo

Legal Interoperability as a Tool for Combatting Fragmentation
GCIG Paper Series No. 4
Rolf H. Weber

Innovations in Global Governance: Toward a Distributed Internet Governance Ecosystem
GCIG Paper Series No. 5
Stefaan G. Verhulst, Beth S. Noveck, Jillian Raines and Antony Declercq

The Impact of the Dark Web on Internet Governance and Cyber Security
GCIG Paper Series No. 6
Tobby Simon and Michael Chertoff

On the Nature of the Internet
GCIG Paper Series No. 7
Leslie Daigle

Understanding Digital Intelligence and the Norms That Might Govern It
GCIG Paper Series No. 8
David Omand

ICANN: Bridging the Trust Gap
GCIG Paper Series No. 9
Emily Taylor

A Primer on Globally Harmonizing Internet Jurisdiction and Regulations
GCIG Paper Series No. 10
Michael Chertoff and Paul Rosenzweig

Connected Choices: How the Internet is Challenging Sovereign Decisions
GCIG Paper Series No. 11
Melissa E. Hathaway

Solving the International Internet Policy Coordination Problem
GCIG Paper Series No. 12
Nick Ashton-Hart

Net Neutrality: Reflections on the Current Debate
GCIG Paper Series No. 13
Pablo Bello and Juan Jung

Addressing the Impact of Data Location Regulation in Financial Services
GCIG Paper Series No. 14
James M. Kaplan and Kayvaun Rowshankish

Cyber Security and Cyber Resilience in East Africa
GCIG Paper Series No. 15
Iginio Gagliardone and Nanjira Sambuli

Global Cyberspace Is Safer than You Think: Real Trends in Cybercrime
GCIG Paper Series No. 16
Eric Jardine

The Emergence of Contention in Global Internet Governance
GCIG Paper Series No. 17
Samantha Bradshaw, Laura DeNardis, Fen Osler Hampson, Eric Jardine and Mark Raymond

Landmark EU and US Net Neutrality Decisions: How Might Pending Decisions Impact Internet Fragmentation?
GCIG Paper Series No. 18
Ben Scott, Stefan Heumann and Jan-Peter Kleinhans

The Strengths and Weaknesses of the "Brazilian Internet Bill of Rights": Examining a Human Rights Framework for the Internet
GCIG Paper Series No. 19
Carolina Rossini, Francisco Brito Cruz, Danilo Doneda

The Tor Dark Net
GCIG Paper Series No. 20
Gareth Owen and Nick Savage

The Dark Web Dilemma: Tor, Anonymity and Online Policing
GCIG Paper Series No. 21
Eric Jardine

One in Three: Internet Governance and Children's Rights
GCIG Paper Series No. 22
Sonia Livingstone, John Carr and Jasmina Byrne

Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity
GCIG Paper Series No. 23
Samantha Bradshaw

Available for free download at www.cigionline.org/publications

CIGI
Centre for International Governance Innovation
www.cigionline.org

ABOUT CIGI

The Centre for International Governance Innovation is an independent, non-partisan think tank on international governance. Led by experienced practitioners and distinguished academics, CIGI supports research, forms networks, advances policy debate and generates ideas for multilateral governance improvements. Conducting an active agenda of research, events and publications, CIGI's interdisciplinary work includes collaboration with policy, business and academic communities around the world.

CIGI's current research programs focus on three themes: the global economy; global security & politics; and international law.

CIGI was founded in 2001 by Jim Balsillie, then co-CEO of Research In Motion (BlackBerry), and collaborates with and gratefully acknowledges support from a number of strategic partners, in particular the Government of Canada and the Government of Ontario.

Le CIGI a été fondé en 2001 par Jim Balsillie, qui était alors co-chef de la direction de Research In Motion (BlackBerry). Il collabore avec de nombreux partenaires stratégiques et exprime sa reconnaissance du soutien reçu de ceux-ci, notamment de l'appui reçu du gouvernement du Canada et de celui du gouvernement de l'Ontario.

For more information, please visit www.cigionline.org.

ABOUT CHATHAM HOUSE

Chatham House, the Royal Institute of International Affairs, is based in London. Chatham House's mission is to be a world-leading source of independent analysis, informed debate and influential ideas on how to build a prosperous and secure world for all. The institute: engages governments, the private sector, civil society and its members in open debates and confidential discussions about significant developments in international affairs; produces independent and rigorous analysis of critical global, regional and country-specific challenges and opportunities; and offers new ideas to decision-makers and -shapers on how these could best be tackled from the near- to the long-term. For more information, please visit: www.chathamhouse.org.

CIGI MASTHEAD

Executive

President	Rohinton P. Medhora
Director of the International Law Research Program	Oonagh Fitzgerald
Director of the Global Security & Politics Program	Fen Osler Hampson
Director of Human Resources	Susan Hirst
Director of the Global Economy Program	Domenico Lombardi
Vice President of Finance	Mark Menard
Director of Communications and Digital Media	Joseph Pickerill
Chief of Staff and General Counsel	Aaron Shull

Publications

Managing Editor, Publications	Carol Bonnett
Publications Editor	Jennifer Goyder
Publications Editor	Patricia Holmes
Publications Editor	Nicole Langlois
Publications Editor	Kristen Scott Ndiaye
Publications Editor	Lynn Schellenberg
Graphic Designer	Sara Moore
Graphic Designer	Melodie Wakefield

Communications

Communications Manager	Tammy Bender	tbender@cigionline.org (1 519 885 2444 x 7356)

CIGI
67 Erb Street West
Waterloo, Ontario N2L 6C2
tel +1 519 885 2444 fax +1 519 885 5450
www.cigionline.org

CHATHAM HOUSE
The Royal Institute of International Affairs
10 St James's Square
London, England SW1Y 4LE, United Kingdom
tel +44 (0)20 7957 5700 fax +44 (0)20 7957 5710
www.chathamhouse.org

RECYCLED
Paper made from recycled material
FSC® C023070