UTRECHT JOURNAL OF
INTERNATIONAL AND EUROPEAN LAW

Yael Ronen, 'Big Brother's Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers' (2015) 31(80) Utrecht Journal of International and European Law 72, DOI: http://dx.doi.org/10.5334/ujiel.cs

RESEARCH ARTICLE

Big Brother's Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers

Yael Ronen[1]

[1] Professor of international law, Sha'arei Mishpat Academic Center, Hod Hasharon, and Minerva Center for Human Rights, Hebrew University in Jerusalem, Israel
yael.ronen@mail.huji.ac.il

Following the 2013 revelations on the extent of intelligence gathering through internet service providers, this article concerns the responsibility of internet service providers (ISPs) involved in disclosure of personal data to government authorities under the right to privacy, by reference to the developing, non-binding standards applied to businesses under the Protect, Respect and Remedy Framework. The article examines the manner in which the Framework applies to ISPs and looks at measures that ISPs can take to fulfil their responsibility to respect the right to privacy. It utilizes the challenges to the right to privacy to discuss some aspects of the extension of human rights responsibilities to corporations. These include the respective roles of government and non-state actors, the extent to which corporations may be required to act proactively in order to protect the privacy of clients, and the relevance of transnational activity.

Keywords: privacy; corporations; Internet; surveillance; human rights; non-state actors

1. Introduction

In the summer of 2013, the international and domestic human rights and intelligence communities broke into a frenzy following the disclosure by a former employee of the US National Security Agency (NSA) of documents regarding surveillance of private electronic communications by the US and other governments. While the practice of electronic surveillance was widely known previously, the 2013 revelations brought to light the staggering amount of data collected – reaching 97 billion pieces of intelligence from computer networks worldwide in March 2013 alone[1] – and, importantly for the purposes of this article, the extent of involvement by internet and service providers (ISPs) in the process.

Responsibility for electronic surveillance lies first and foremost with the government conducting or demanding it,[2] and has been addressed primarily in those terms.[3] The present article addresses a less discussed aspect of the matter, namely the responsibility under international human rights standards of the ISPs involved in disclosure to government authorities of clients' personal data and communications.[4] By acting in partnership with the government, ISPs may become complicit in violations of the right to privacy. The article thus touches upon one of the often-mentioned manifestations of the universalisation of international law, namely the attempt at expansion of human rights obligations to corporations.

Interest in accountability of ISPs for involvement in governmental surveillance is not an entirely new phenomenon. Since the mid-2000s ISPs have been accused of complicity in governmental violation of human rights in

[1] Tamir Israel and Katitza Rodriguez, 'Using Domestic Networks to Spy on the World' (*Electronic Frontier Foundation*, 13 June 2013) <https://www.eff.org/deeplinks/2013/06/spies-without-borders-i-using-domestic-networks-spy-world>

[2] Well-publicized examples are the UK's Tempora and the Russian SORM, but other examples with less catchy names abound.

[3] See Alex Sinha, 'NSA Surveillance Since 9/11 and the Human Right to Privacy' (2014) 59 Loyola Law Review 861; Marko Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' Harvard International Law Journal (forthcoming)

[4] Private actors may be involved in other aspects of encroachment on privacy of communications, such as by developing technologies that enable mass or invasive surveillance. Human Rights Council, 'Report by special Rapporteur Frank La Rue on the Promotion and Protection of the Right to Freedom of Opinion and Expression', UN Doc A/HRC/23/40 (17 April 2013) para 75 ('2013 Report of the Special Rapporteur')

China, including through disclosure of client data, which in some cases has led to arrests of political dissidents.[5] In some cases legal proceedings have been brought against ISPs for complicity in governmental action that violated human rights. Pursuit of ISPs' legal responsibility raises a variety of questions of principle, ranging from the applicability of human rights law to corporations, to delineating the extent of involvement by a corporation in the violation of rights that would constitute complicity. This article considers some of these questions in the context of the special character of ISPs and explores the implications possible answers would have.

Part 2 sets out the factual background to the article, namely the phenomenon of electronic surveillance through ISPs as an infringement of the right to privacy under international human rights law. Part 3 describes the manner in which this framework has been extended to corporations on a non-binding basis through the UN Guiding Principles on Business and Human Rights (UN Guiding Principles or UNGP). Part 4 looks more closely at the framework applied to corporations, highlighting the idiosyncrasies of ISPS against the premises of the UNGP's framework. Parts 5 through 7 examine the consequences of these idiosyncrasies for ISPs concerned with ensuring the right to privacy of their clients and their communications: Part 5 focuses on the fact that ISPs operate under the domestic law of states; Part 6 considers various policies and measures which ISPs can take to ensure the privacy of their clients, taking note of how the special characteristics of ISPs' operations relate to the premises of the UNGP, such as the role of financial incentives; and Part 7 examines measures that ISPs can take to prevent violations of the right to privacy.

2. The right to privacy and electronic surveillance

Privacy is the presumption that individuals have an area of autonomous presence and action, with or without interaction with others, which is free from excessive state or other unsolicited intervention. The right to privacy is also the ability of individuals to determine who may have information about them and how that information is to be used. Privacy in communication entails that individuals can exchange information and ideas in a space that is beyond the reach of all others; that they can verify that their communications are sent and received only by their intended interlocutors; and that they can maintain anonymity, which allows free expression without fear of retribution or condemnation.[6]

As communications of all types is increasingly conducted online, some have questioned the relevance of the notion of privacy. It has been argued that the conveyance and exchange of personal information via electronic means is a conscious compromise, in which individuals voluntarily surrender previously private information in return for digital access to their choice of goods, services and information. In light of this voluntary deal, it has been suggested that the accessing and interception by governments through mass security surveillance is not an infringement on the privacy of affected individuals.[7] The UN High Commissioner for Human Rights has rejected these propositions, stating that they reveal a limited appreciation of the right to privacy and of the legitimate parameters for security surveillance.[8] Moreover, these approaches assume that clients can refuse to surrender information and forego the use of electronic means of communication. In the present state of technological dependency, such refusal would effectively mean foregoing significant social interaction, to such an extent that it cannot, in fairness, be offered as an option.

Disclosure and collection of internet and other communication data encroach directly on individuals' right to privacy. It consequently also impacts on their freedom of expression and association. Indirectly, disclosure and collection of data may affect other rights, such as liberty and bodily integrity. Yet, since many such rights may be subject to limitations, disclosure of data does not necessarily amount to a violation of the right to privacy (or other rights). Such limitations may include state surveillance measures for the purposes of administration of criminal justice, prevention of crime or protection of national security. However, such interference is permissible only if it takes place under a law that clearly outlines the conditions whereby individuals' right to privacy can be restricted; measures encroaching upon this right must be taken on the basis of a specific decision by a state authority expressly empowered by law to do so, usually the judiciary; and they must respect the principle of proportionality.[9]

---

[5] Human Rights Watch, '"Race to the Bottom": Corporate Complicity in Chinese Internet Censorship' (2006) 18 Human Rights Watch 31–33

[6] 2013 Report of the Special Rapporteur n 4 paras 22–23

[7] Navy Pillay, 'Opening Remarks by Ms. Navi Pillay United Nations High Commissioner for Human Rights to the Expert Seminar: The right to privacy in the digital age', (Palais des Nations, Geneva 24 February 2014) <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?LangID=E&NewsID=14276>

[8] ibid

[9] Human Rights Council, 'Report of the Special Rapporteur Frank La Rue on the Promotion and Protection of the Right to Freedom of Opinion and Expression' (16 May 2011) UN Doc A/HRC/17/27 para 59

Governmental collection of data from ISPs takes place under various frameworks, such as executive orders for disclosure or for direct access to the data, contractual relations, as well as through covert operations. Some governments require device manufacturers and network management companies to install software that allows surveillance and monitoring of communications. In Russia, for example, internet suppliers are obliged to buy and install surveillance equipment, granting the government direct and unlimited access to all electronic data.[10] Russian communication law already obliges internet service providers to disclose all information required by law enforcers and the administrative code details the fines that are levied for failure to do so.[11] In other jurisdictions, such as in the US and in EU member states, government often require that data collected by the companies be shared with it.[12] For example, the leaked documents revealed that the telephone company Verizon had been ordered to hand over all metadata associated with all telephone communications originating or terminating within the US, as well as calls wholly within the US. Another major revelation regarding the US surveillance activity was the existence of the PRISM program. The full parameters and capacities of PRISM remain unclear, but at its most innocuous, PRISM appears to be a database capable of interacting directly with the networks of participating ISPs through a series of portals whose specific features and capacities are negotiated and developed with each participating company. Orders for clients' data are issued under the Foreign Intelligence Surveillance Act and sent to the respective companies, who review them and make use of the portal to respond to the orders electronically. Various reports describe PRISM as providing access to emails, online chats (video and voice), photos, file transfers, search queries, online social networking details and more.[13]

While lack of commitment to privacy and freedom of expression in China and Russia perhaps surprises few (China is not party to the ICCPR),[14] the 2013 revelations on data gathering by US and other governments has had that effect. The surprise could be dismissed as a show of naïveté,[15] grounded in misconceptions as to how far governments would go in pursuit of national interests, and what constitutes a 'human rights-friendly' jurisdiction. With respect to the latter, data disclosure illustrates an interesting shift: Standard indicators of risks to human rights, which include political instability, corruption, systematic state disregard for human rights, socio-economic factors, lack of access to effective remedy, and the existence active or latent conflict,[16] would largely exclude North America and Western Europe.[17] Encroachment on electronic data privacy, however, is the malaise of rich, developed states, where electronic communication usage is highly pervasive.[18]

That said, one must acknowledge that the criticism of the encroachment on the right to privacy in China and Russia does differ from the criticism regarding Western states on more 'traditional' analytical grounds: In the former case, the encroachment on privacy is perceived as facilitating repression of political dissent and persecution of human rights defenders,[19] goals which international human rights law does not view as legitimate grounds for limiting rights. The demands by Western governments, on the other hand, are in pursuit of a legitimate purpose, namely the protection of national security or law enforcement, and the critique is not so much on the permissibility of surveillance activity in principle, as it is on its extent in practice.

---

[10] Andrei Soldatov and Irina Borogan, 'Russia's Surveillance State' (2013) 30 World Policy Journal <http://www.worldpolicy.org/journal/fall2013/Russia-surveillance>

[11] Thomas Peter, 'Russian internet laws could make ISPs liable for user's crimes' *Russia Today* (Moscow, 18 February 2013), <http://rt.com/politics/russian-internet-law-providers-448/>

[12] Shift and the Institute for Human Rights and Business, 'ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights' (European Commission, undated) 12

[13] Israel and Rodriguez n 1

[14] China ranks 'not free' on the Freedom House ranking, graded 7 and 6 (7 being the lowest grade available) for political rights and civil liberties, respectively. Russia ranks 'not free' on the Freedom House ranking, graded 6 and 5 (7 being the lowest grade available) for political rights and civil liberties, respectively; see Freedom House, 'Freedom in the World 2014'(2014) 18

[15] The public outrage could also be dismissed as hypocritical, considering that the indignation was over the violation of constitutional rights of US citizens rather than on the human rights of all individuals, including foreigners who have been subject to aggressive US surveillance for over a decade

[16] Shift and the Institute for Human Rights and Business n 12 30–31

[17] The ICT Sector guidelines refer to evaluation standards such as those of Freedom House, where north American and Western European states receive the highest scores on political rights and civil liberties. Freedom House n 14

[18] Internet penetration estimates as of June 2012 are 78.6% in North America, 67.6% in Oceania, 63.2% in Europe, 42.9% in Latin America, 40.2% in the Middle East, 27.5% in Asia and 15.6% in Africa, information available at <http://www.internetworldstats.com/stats.htm>

[19] Soldatov and Borogan n 10

3. Extending human rights responsibilities to corporations

Interest in control over the activities of corporations emerged in the 1970s as part of the vindication of the New International Economic Order put forward by developing countries in order to revise the international economic system in their favour, focusing on transnational activity. Developed states were interested in protecting their corporations against discriminatory treatment in developing states, while developing states were interested in ensuring that transnational corporations did not interfere in their sovereign pursuit of economic objectives.[20] Moreover, there was concern regarding the impact of multinational corporations based in Europe and North America, which established manufacturing subsidiaries in developing countries in order to benefit from cheap labour and raw materials.[21] In 1976 the Organisation for Economic Co-operation and Development adopted the Guidelines for Multinational Enterprises (OECD MNE Guidelines). For over three decades, these guidelines were the only comprehensive, multilaterally endorsed code of conduct for multinational corporations.[22] The debate concerning the responsibilities of business in relation to human rights intensified in the 1990s, as transnational production expanded into increasingly difficult areas.[23] As a result, in 1995 work began under the auspices of the UN Commission of Human Rights to develop standards to regulate the activities of transnational corporations. Early attempts at this endeavour[24] failed, largely due to the refusal of powerful corporations to subject themselves to legally-binding obligations. In 2005, in an attempt to move beyond the stalemate, then-UN Secretary-General Kofi Annan appointed John Ruggie as Special Representative to clarify the roles and responsibilities of states, corporations and other social actors in the business and human rights sphere. Ruggie's work culminated in 2011 with the presentation of the UN Guiding Principles, which were endorsed by the Human Rights Council.[25] The Guiding Principles are based on extensive research and consultations with representatives from government, business and civil society, including trade unions, NGOs and legal and academic experts, across all continents.

The UN Guiding Principles establish the Protect, Respect and Remedy framework, which rests on three pillars: first, the state's duty to protect against human rights abuses by third parties; second, the corporate responsibility to respect human rights, namely to act with due diligence to avoid infringing on the rights of others and to address adverse impacts that occur; and third, greater access by victims to effective remedies, both judicial and non-judicial. Under the Framework, the primary responsibility under human rights law remains with states. It is states that are under a duty to protect against human rights abuses committed by third parties, including corporations. In contrast, corporations are not directly bound by international human rights law. Rather, they have a non-legally binding responsibility to respect human rights. This responsibility applies across the corporations' business activities and through their relationships with third parties connected with those activities.

The UN Guiding Principles embody a certain consensus on a global standard of expected conduct. They have been incorporated and acknowledged by other soft-law instruments on corporate responsibility, such as the revised OECD MNE Guidelines of 2011, the International Finance Corporation's Performance Standards and the International Organization for Standardization's ISO 26000 Social Responsibility Guide; and there are numerous other platforms acting to integrate human rights policies into corporate governance which have adopted standards that go beyond the UN Guiding Principles. For example, the UN Global Compact, launched in 2000, calls on corporations to make a general commitment to support, respect and promote internationally recognized human rights and to avoid complicity in human rights abuses by governments of states in which they operate.[26] The Global Compact is addressed directly to corporations, and has been signed by over 10,000 businesses.[27]

Another platform of particular interest in the present context is the Global Network Initiative (GNI). It is a group of companies, civil society organizations, investors, and academics that has adopted a collaborative

---

[20] Olivier de Schutter, *International Human Rights Law: Cases, Materials, Commentary* (CUP 2010) 396

[21] Council of Europe Parliamentary Assembly, Committee on Legal Affairs and Human Rights, 'Explanatory Memorandum by Mr Haibach, Rapporteur' (27 September 2010) Doc 12361 para 33

[22] ibid

[23] For an early but still pertinent analysis of the notion of international human rights obligations for corporations see Steven R. Ratner, 'Corporations and human rights: a theory of legal responsibility' (2001) Yale Law Journal 443

[24] See eg The Draft Norms on the Responsibilities of Transnational Corporations and Other Business Enterprises with Regard to Human Rights (2003) UN Doc E/CN.4/Sub.2/2003/12, adopted by the Sub-commission of the then UN Commission on Human Rights but rejected by the Commission

[25] UN Human Rights Council 'Guiding Principles on Business and Human Rights' (16 June 2011) UN Doc A/HRC/17/31 ('UN Guiding Principles')

[26] <http://www.unglobalcompact.org/AboutTheGC/TheTenPrinciples/principle1.html>

[27] <http://www.unglobalcompact.org/HowToParticipate/Business_Participation/index.html>

approach to protect and advance freedom of expression and privacy in the data and communication technology sector. Participant corporations are Evoca, Facebook, Google, Microsoft, Procera Networks, Websense and Yahoo.[28]

The term 'responsibility' rather than 'duty' indicates that the framework does not impose legal human rights obligations directly on corporations, although elements of the framework may be reflected in domestic laws. Indeed, a crucial element for the acceptance of the UN framework was that the responsibility of corporations remain non-binding, to the exclusion of the secondary issues of liability and enforcement. The present article, however, focuses on the substantive content of the responsibility rather than on its enforceability.[29]

4. Changing relationship between state and corporations

According to the UN Guiding Principles, '[t]he responsibility of business enterprises to respect human rights applies to all enterprises regardless of their size, sector, operational context, ownership and structure. Nevertheless, the scale and complexity of the means through which enterprises meet that responsibility may vary according to these factors and with the severity of the enterprise's adverse human rights impacts'.[30] Despite this universal formulation, the drafting of the UN Guiding Principles was informed by particular types of corporate activity that brought about direct and adverse human rights conditions. These were transnational, labour-intensive textile industries, and transnational corporations involved in exploitation of natural resources. These corporations' operations and relationships with governments have been fundamental to shaping the Guiding Principles. While these operations and relationships may be applicable to many corporate sectors and activities, they do not exhaustively cover all potential corporate involvement in human rights abuses. Specifically, the issues arising with respect to ISPs acting under executive orders are very different from those that arise with respect to the transnational corporations, whose conduct generated the activity which led to the Guiding Principles.

First, regulation of transnational corporate activity has always been perceived as a necessary response to the increasingly autonomous and unconstrained operation of corporations. Because of the financial strength of these corporations, host governments have proven unwilling and unable to impose and enforce human rights standards on them through domestic law. By applying human rights standards directly on corporations, the Guiding Principles aim to fill the gap in compliance, notwithstanding the continuing obligation of states to protect individuals from harm by third parties, including corporations. But in contrast with the corporations described above, the conduct of ISPs in the context of disclosure of data is not outside the realm of governmental control, but, on the contrary, directly within it: the companies in question are acting in compliance with governmental orders authorized by law. The governments in question are able and very much willing to impose domestic law on these corporations, but it is precisely that law which jeopardizes the enjoyment of human rights.

A related novelty is that while ISPs are not the initiators of potential violations, they are nonetheless in a unique position to prevent or mitigate them. This is first and foremost because the content of the demand for disclosure is confidential, as is, sometimes, the very existence of the demand. Potential victims are therefore not aware of their vulnerability. ISPs are at times the only actors who can raise the alarm when rights are at risk of being violated. In addition, a potential violation may be evident only in light of the massiveness of the data-gathering, the impact of which only the ISPs are in a position to gauge. Since ISPs are the keepers of the data sought, their ability to prevent and avoid government interference is furthermore crucial for the safeguarding of rights. This aspect of the relationship is significant with respect not only to disclosure mandated by law, but also to covert tapping of data.

Another difference between ISPs and the corporations whose activities generated the international debate leading to the Guiding Principles is the significance of transnational activity. The 'traditional' activity informing

[28] Global Network Initiative, '2012 Annual Report Fact Sheet' <http://globalnetworkinitiative.org/sites/default/files/GNI%202012%20Report%20Handout%20English.pdf>

[29] UN Guiding Principles n 24, Commentary to Guiding Principle 12. Domestic law may also make such a distinction, eg the FIAS Amendments Act 2008, which grants immunity to private companies from legal action when they cooperate with US government agencies in intelligence collection. FISA Section 404(a)(4) ('Protection from Liability.—Subsection (l) of section 105B of the Foreign Intelligence Surveillance Act of 1978, as added by section 2 of the Protect America Act of 2007, shall continue to apply with respect to any directives issued pursuant to such section 105B'. Subsection (l) provide: '(l) Notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section')

[30] UN Guiding Principles n 24, Principle 14

the drafting of the UN Guiding Principles consisted of corporations registered in one country and operating in another.[31] In the case of Western corporations in the textile industry for example, transnational production is crucial for profitability, inter alia because it permits evasion of costly compliance with human rights standards which would be imposed in home states. Extraterritoriality has thus permitted *evasion* of the applicability of stringent human rights standards. In the case of ISPs, transnational activity plays an entirely different role. It does not relocate production activity, but increases the market for the services and products that ISPs sell.[32] Moreover, clients' right to privacy is at risk within the home state no less than elsewhere. Thus, relocation abroad may be a means for ISPs to *shield* clients from invasion of their privacy rather than to expose them to violation of their rights. In both cases, extraterritorial activity evades governmental control. The difference is that in the latter case the control is perceived as rights-protecting, while in the former it is rights-infringing.

Finally, if 'traditional' abuse of human rights by corporations was incentivized by profit seeking, it is now acknowledged that the relationship between human rights compliance and financial profit is more complex. Certainly, ISPs may profit from the violation of clients' rights, or at least from collaboration with the government, whether directly in those cases where the ISP is reimbursed or paid for providing the data requested,[33] or indirectly where collaboration with the government incentivizes the latter to make the ISP lucrative business offers in future.[34] But complicity in human rights abuses can also lead to bad publicity and to consumer backlash, thereby undercutting profitability. Adherence to human rights standards may therefore be a rational economic choice for corporations and not only a moral choice.[35] ISP compliance with executive orders that jeopardise the right to privacy may be unprofitable even in the immediate term. At the same time, in order to minimize vulnerability to executive orders, ISPs would have to compromise profit in the immediate term (for example by refusing to comply with executive orders under pain of contempt of court, or by refraining from the collection of data at the risk of losing advertising income which builds on the use of that data). The profit-compliance calculus therefore takes on new dimensions.

Combined, these factors call into question the suitability of the accepted framework for corporate responsibility as developed so far to ISPs involved in data disclosure. Analysis of the obstacles in this context can serve to illustrate a wider issue, namely the limitations of the Protect, Respect and Remedy Framework in co-opting corporations into human rights compliance. The remainder of this article examines how ISPs may fulfil their responsibility to respect clients' privacy. It considers how such measures correspond to the underlying premises of the Framework.

5. Applying the Protect, Respect and Remedy Framework to actors subject to domestic law

UN Guiding Principle 13 states that the responsibility to respect human rights requires that business enterprises:

> (a) Avoid causing or contributing to adverse human rights impacts through their own activities, and address such impacts when they occur;
> (b) Seek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts.

These provisions cover a wide array of manners in which corporations may undesirably become involved in the perpetration of human rights abuses by other actors.[36] The UNGP do not define or establish spe-

[31] See eg the UN Guiding Principles n 24, Commentary to Principle 7 on states' support for business respect for human rights in conflict-affected areas suggests that in conflict-affected areas, home states have a role to play in assisting corporations and host states to ensure that businesses are not involved with human rights abuse

[32] Where ISPS do engage in transnational production, they face similar challenges as other corporations, eg Charles Kernaghan, 'China's Youth Meet Microsoft' (The National Labor Committee, April 2010), <http://www.globallabourrights.org/reports/Chinas_Youth_Meet_Micro.pdf>

[33] See eg Daniel Hurst, 'Government Will Pay Telcos and ISPs under Metadata Retention Bill' *The Guardian* (London, 30 October 2014) <http://www.theguardian.com/australia-news/2014/oct/30/metadata-retention-bill-will-require-data-to-be>

[34] James Farrar, 'Should Google, Microsoft or anyone else divest & disengage from China?' (ZDNet, 17 January 2010) <http://www.zdnet.com/article/should-google-microsoft-or-anyone-else-divest-disengage-from-china/>

[35] Council of Europe Parliamentary Assembly, Committee on Legal Affairs and Human Rights n 21 para 31

[36] International Commission of Jurists, 'Corporate Complicity & Legal Accountability - Report of the International Commission of Jurists Expert Legal Panel on Corporate Complicity in International Crimes, Volume 1: Facing the Facts and Charting a Legal Path' (2008) 3

cific criteria for conduct that constitutes 'contribution' or a 'direct link'. In the terms of the classification adopted by the Global Compact and endorsed by the Special Representative during the preparatory work on the Protect, Respect and Remedy Framework,[37] ISPs are at risk of being in direct complicity with the government, when they knowingly provide goods or services that assist the state in a violation.[38] From this it follows that the primary responsibility of corporation, if not the only one, is to refrain from certain actions. That is nonetheless difficult when domestic law imposes an obligation to collaborate with the government. In fact, ISPs accused of complicity in government violations of the right to privacy and other rights have cited the obligation to comply with domestic laws as their defence.[39]

Under international law, domestic legal constraints are no excuse for non-compliance with international law.[40] However, this rule is grounded in an understanding of the law as applicable to states. Implicit in this rule is the ability of the state to avoid conflict by amending its domestic law which conflicts with the international norm. The same cannot be said with respect to corporations. Those may be bound by a domestic norm which is inconsistent with international human rights law, and they do not have the capacity to change this norm. This difference may bear on the responsibility of corporations.

The notion of a non-state actor being bound by conflicting norms under domestic law and under international law is no longer a novelty. For example, under international criminal law, a legal obligation to obey orders may relieve a person from criminal responsibility, provided that the person did not know that the order was unlawful, and the order was not manifestly unlawful,[41] or mitigate the severity of the punishment.[42] The question is whether an analogy ought to be made from criminal responsibility to the non-legal responsibility of corporations. The former concerns criminal conduct, while the latter concerns conduct that aside from being regulated by non-binding norms, is not necessarily criminal in nature. One argument may be that if concessions are made for the benefit of criminals, they surely must be made for the benefit of less serious violators. On the other hand, the consequences of compliance with unlawful orders under criminal law, namely criminal sanctions, are potentially harsher than the consequences of compliance by a legal person with unlawful non-criminal domestic law, and therefore concessions are more called for in the former case. Another matter is the fact that the illegal character of a norm violating international criminal law is likely to be discernible (even if not manifest), while compliance or violation of human rights standards are ultimately dependent on value judgments; if a defence of compliance is available in the former case, to a person who committed an international crime, a fortiori it should be available in the latter case, to a legal person which violated human rights standards. On the other hand, the nature of corporate activity is such that corporations are more likely than individuals to be involved in repeat conduct that may amount to violation of rights. This may impact on the credibility of a claim of good faith by the corporation. In conclusion, it is difficult to argue that corporate responsibility for violations of international human rights law should be necessarily stricter or more lenient than the individual responsibility for violations of international criminal law.

One might suggest that the introduction of non-state actors into the world of human rights obligations justifies an entirely different approach, namely the revision of the human rights interest-balancing process, to accommodate the different functions of the various types of actors. Such a revision could include 'compliance with domestic law' as a legitimate ground for encroaching on rights so as to relieve the non-state actor of the burden of conflicting obligations. This proposition is objectionable on a number of grounds. First, as a matter of policy, 'compliance with domestic law' as a ground for permissible limitations (by corporations) on rights (of individuals) is problematic, since it exacerbates the already existing incentive for states to delegate their authority to other actors in order to evade their own responsibility.[43]

Second, it is questionable whether such a ground responds to the difficulty described above, given that the ability of corporations to rely on it is limited. This is related to the fact that corporations are in a vertical

---

[37] <http://www.unglobalcompact.org/aboutthegc/thetenprinciples/principle2.html>, cited in Human Rights Council, 'Clarifying the Concepts of "Sphere of influence" and "Complicity", Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and other Business Enterprises' (5 May 2008) UN Doc A/HRC/8/16 para 58

[38] Andrew Clapham and Scott Jerbi, 'Categories of Corporate Complicity in Human Rights Abuses' (2000–01) 24 Hastings International and Comparative Law Review 339, 342

[39] 'Yahoo Plea over China Rights Case' *BBC* (London, 28 August 2007) <http://news.bbc.co.uk/2/hi/asia-pacific/6966116.stm>

[40] With respect to treaty obligations this is explicit in the Vienna Convention on the Law of Treaties (entered into force 27 January 1980) 1155 UNTS 331, art 27

[41] Rome Statute of the International Criminal Court (entered into force 1 July 2002) 2187 UNTS 90, art 33(1)(a)

[42] IMT Statute art 8, Report of the Secretary-General pursuant to paragraph 2 of Security Council Resolution 808(1993), UN Doc S/25704 (3 May 1993), adopted by the Security Council in Resolution 827 (25 May 1993) (ICTY Statute), art 7(4); Statute of the International Criminal Court for Rwanda, annexed to UNSC Res 955(1994) (8 November 1994) UN Doc S/RES/955 art 6(4)

[43] Scott Jerbi, 'Business and Human Rights at the UN: What Might Happen Next?' (2009) 31 Human Rights Quarterly 299, 305

relationship with the state, and suffer from lack of information. The examples offered by the UN Guiding Principles (drawing on the Global Compact) are such where the existence of the violation is quite evident: the forced relocation of peoples in circumstances related to business activity, suppression of a peaceful protest against business activities or the use of repressive measures while guarding company facilities, systematic discrimination in employment law against particular groups on the grounds of ethnicity or gender.[44] In contrast, collaboration in surveillance by the government is not so patently a violation of the right to privacy. The primary difficulty for the corporation to evaluate the legality of disclosure is not the legitimacy of the purpose of the surveillance (national security) but its proportionality to the injury that is caused. For an ISP to determine whether disclosure of information to the government would be in line with its human rights responsibilities, it must know the purpose of the governmental demand, the potential benefit which can accrue to the government from the disclosure, and the harm that is likely to be caused to the client whose data is disclosed. But ISPs are not privy to the state's information or to its assessment of the situation, concerns or intentions. Consequently, ISPs cannot evaluate whether their own conduct would be in compliance with human rights standards or not.

Again, guidance might be sought from other situations in which one actor may incur responsibility through its cooperation with another actor, whose conduct it cannot control. For example states that extradite or deport individuals may be exposing those individuals to risk of rights violation by the states of destination. However, the relationship between the sending state and the state of destination is horizontal. Thus, where the question of potential violations of human rights by a state of destination arises, international law does indeed place limitations on the scope of permissible conduct, through the principle of non-refoulement,[45] or through the prohibition on the deportation or extradition of a person to a state where he or she would be in real risk of being subject to torture[46] or of a flagrant denial of justice.[47] Furthermore, states are able – and are required – to exercise discretion as to whether to cooperate with other states. They may request assurances and guarantees that no violations would occur, and they can evaluate the credibility of those assurances. Corporations do not have the same luxury, since they operate within a vertical relationship, under a domestic legal regime, which they are not empowered to modify. They should therefore not be encumbered with the responsibility for the conduct of the state.

Resolving the quandary of corporations being simultaneously bound in opposite directions is not a matter merely of a policy choice. If the responsibility of corporations is to be made legally binding, it would require a restructuring of international human rights law to accommodate a new level in the hierarchy of relationships:[48] still inferior to the state but no longer on par with individuals who are potential victims. The presently non-binding character of the Framework enables this matter to remain unaddressed. However, the practical challenges to the Framework will have to be addressed if the coherence of the international human rights legal regime is to be preserved.

The UN Guiding Principles provide that corporations should '[c]omply with all applicable laws and respect internationally recognized human rights, wherever they operate' and '[s]eek ways to honour the principles of internationally recognized human rights when faced with conflicting requirements'.[49] Similarly, the OECDE MNE Guidelines provide that corporations 'should not and are not intended to place an enterprise in situations where it faces conflicting requirements. … [I]n countries where domestic laws and regulations conflict with the principles and standards of the Guidelines, enterprises should seek ways to honour such principles and standards to the fullest extent which does not place them in violation of domestic law'.[50] These formulations offer two directives: first, they acknowledge the conflicting requirements facing corporations and concede the need to comply with domestic law. So long as the standards are not binding, it is only natural that domestic norms, which *are* binding, would take priority; should the UN Guiding Principles

[44] Human Rights Council n 35 para 58

[45] Convention relating to the Status of Refugees (came into force 22 April 1954) 189 UNTS 150 (Refugee Convention), as amended by its Protocol (entered into force 4 October 1967) 606 UNTS 267 art 33(1)

[46] Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (entered into force 26 June 1987) 1465 UNTS 85 art 3(1); *Soering v United Kingdom* App no 14038/88, A/161 (ECtHR, 7 July 1989) para 111

[47] *Othman (Abu Qatada) v the UK* App no 8139/09 (ECtHR, 17 January 2012) paras 269–285

[48] For preliminary thoughts on whether a new human rights regime ought to be devised for non-state actors see Yaël Ronen, 'Human Rights Obligations of Territorial Non-State Actors' (2013) 46 Cornell International Law Journal 21. For a discussion of the formal changes that would be necessary see David Kinley and Junko Tadaki, 'From Talk to Walk: The Emergence of Human Rights Responsibilities for Corporations at International Law' (2004) 44 Virginia Journal of International Law 931, 993–1021

[49] UN Guiding Principles n 24 Principle 23(a), (b)

[50] OECD 'OECD Guidelines for Multinational Enterprises' (2011), I.2

(or other standards) develop into binding law, the point of balance may change. For example, in light of the difficulties facing corporations, it is arguable that the obligation to comply with domestic law should be given some significance in assessing their conduct in terms of international human rights standards. It is not proposed that a domestic legal obligation be viewed as *permitting* a violation of rights, but it may *excuse* it (to borrow a term from criminal law).[51] This distinction clarifies that the domestic law itself does not justify violation of international law, but the conflict of commitments exempts the corporation from responsibility; correspondingly, the state, which faces no such conflict, cannot rely on its domestic law to justify its conduct. Furthermore, it may be that where the violation is egregious and manifest, the corporation too would not be exempt from responsibility, in the same manner as an individual is not exempt from criminal liability in the case complying with manifestly unlawful orders. In this vein, the UN Guiding Principles provide that corporations should '[t]reat the risk of causing or contributing to gross human rights abuses as a legal compliance issue wherever they operate',[52] indicating that certain conduct may amount to violation of the law, whether domestic or international.

Secondly, these formulations suggest that a corporation might be required to take positive steps to ensure the privacy of its clients. GNI has drafted Principles on Freedom of Expression and Privacy, which expressly state that 'Information and Communications Technology (ICT) companies have the responsibility to respect *and protect* the freedom of expression and privacy rights of their users'.[53] The Principles expressly address the context of governmental demands for data disclosure, stating that '[p]articipating companies will respect *and protect* the privacy rights of users when confronted with government demands, laws or regulations that compromise privacy in a manner inconsistent with internationally recognized laws and standards'.[54] There are various ways by which corporations can avoid or minimize potential conflict between the disclosure orders under domestic law and international standards for the protection of clients' privacy. The appropriateness of measures would depend on the specific circumstances, including their relevance to the particular state environment, and to the capacity of the ISP. The following is a discussion of some such measures.

6. Measures to avoid causing or contributing to violation of the right to privacy

6.1 Exhausting domestic procedural requirements

It has been noted above that ISPs do not have the capacity to evaluate the lawfulness of demands made upon them in terms of their necessity and proportionality. But they do have the capacity to evaluate the compliance of demands with procedural requirements. At times, this is a sufficient measure to thwart demands, since those are not always made in full compliance with formalities.[55]

At a minimum, ISPs should practice strict adherence to the procedures provided by the law authorising the executive demand.[56] Such an approach is practicable for any corporation, since it requires a minimal investment of resources (which is the main factor in evaluating practicability of a measure), both when compared with the benefit that could accrue to the client, and in absolute terms. Both the Global Compact[57] and the GNI Implementation Guidance call on corporations to request clear communications, in writing, that explains the legal basis for government demands for personal data including the name of the requesting government entity and the name, title and signature of the authorized official.[58] In this spirit, Yahoo! has reported that it employs rigorous procedural protections under applicable laws in response to government

---

[51] On the distinction with respect to the ICC Statute see Otto Triffterer, 'Article 33' in Otto Triffterer (ed),*Commentary on the Rome Statute of the International Criminal Court* (2nd edn, CH Beck, Hart, Nomos 2008) 913, 919–921

[52] UN Guiding Principles n 24 Principle 23(c)

[53] In the present context, it would appear appropriate to interpret 'protect' as 'take positive action'. For the proposition that corporations should not shy from monitoring state action rather than merely their own, ie 'protect' in the legal sense, see Stephanos Anastasiadis, 'Toward a View of Citizenship and Lobbying Corporate Engagement in the Political Process' (2014) 53 Business and Society 260

[54] Global Network Initiative, Principles, Preamble and Privacy Principle, 1–2 <http://globalnetworkinitiative.org/principles/index.php>

[55] Christopher Soghoian, 'An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government' (2011) 12 Minnesota Journal of Science and Technology 191, 218

[56] ibid199–200

[57] Annie Golden Bersagal, 'Meeting the Responsibility to Respect in Situations of Conflicting Legal Requirements', A Good Practice Note endorsed by the United Nations Global Compact Human Rights Working Group on (UN Global Compact 13 June 2011) 11–12

[58] Global Network Initiative, 'Implementation Guidelines' 6 <http://globalnetworkinitiative.org/sites/default/files/GNI_-_Implementation_Guidelines_1_.pdf>

requests.[59] Specifically with respect to China it reported that when it had operational control of Yahoo! China it[60]

> took steps to make clear our Beijing operation would comply with disclosure demands only if they came through authorized law enforcement officers, in writing, on official law enforcement letterhead, with the official agency seal, and established the legal validity of the demand. Yahoo! China only provided information as legally required and construed demands as narrowly as possible. Information demands that did not comply with this process were refused. [61]

What the law requires may be controversial. In the US, for example, courts have rejected the government's interpretation of relevant legislation. While, as discussed below, ISPs may not always be in a position to challenge the validity of a disclosure order, they may have a choice of adopting a more restrictive interpretation of the law than the government has adopted.[62]

6.2 Informing clients about government data requests

Unless they are gagged by law or a court order, ISPs should inform clients of government orders relating to them personally. Ideally, notice should be provided prior to sharing the client's data with the government in order to give the client an opportunity to seek legal counsel and oppose the access request.[63] A client is usually in a better position than a company to challenge a government order against him- or herself, and of course, the client has more incentive to do so. Giving notice does not require the ISP to take a side or to engage in significant expenditure, merely to pass on important information to the client.

A related practice is the publication of law enforcement guidelines for requests for client data. These might provide clients with insight into issues such as whether the ISP requires a warrant for content; what types of data it retains, and what kind of legal process the ISP requires for law enforcement to obtain various kinds of data; how long data is generally held by the ISP, and how long will it be held in response to a retention request; whether the ISP has an exception for emergency or other kinds of disclosures; under what conditions data may be shared with governments or other third parties;[64] whether the ISP asks for or receives reimbursement for the costs incurred in complying with a request for data. This practice has been advocated by the European Commission,[65] and has been adopted more widely.[66] The information should enable clients to choose the ISP they regard as the least harmful to their interests. Of course, unlike other policies that corporations may advertise, law enforcement practices are difficult to monitor, and there are no means of verifying whether the ISPs actually comply with the guidelines that they advertise.

6.3 Challenging orders in court

Other measures may be more difficult to demand of ISPs. For example, an ISP can institute legal process to challenge the content of a demand. Such a measure would be particularly appropriate where a demand appears on its face to be excessively intrusive, for example when it covers a non-specific period of electronic activity, or a large group of unspecified clients.[67] In both cases, the order would be falling short of the requirement that the risk posed by the individual client be indicated. In other cases, however, the ISP could not easily evaluate the justification for the order, since it is privy to the knowledge of neither the government nor the person in question, and therefore it cannot estimate the prospects of its challenge. Moreover, challenging demands for disclosure through legal process is action that requires investment of resources.

---

[59] Human Rights Watch n 5 36

[60] ibid 37

[61] Letter from Gowlings to the Office of the Privacy Commissioner of Canada (14 December 2011) available at <https://www.priv.gc.ca/media/nr-c/2014/let_140430_e.pdf>

[62] Soghoian n 53 215–219

[63] Nate Cardozo et al '2014 Who Has Your Back? Which Companies Help Protect Your Data from the Government?' (Electronic Frontier Foundation 15 May 2014) 14

[64] Human Rights Watch n 5 78

[65] Commission n 12 21

[66] Cardozo et al n 63 15–16

[67] John Yoo suggests that the creation by the security agency of a database covering billions of communication records which are irrelevant to the security threat is not an excess of power, if one regards not the individual record as the relevant item but the database itself, since it is the data mining from the database that would advance the investigation. John Yoo, 'The Legality of the National Security Agency's Bulk Data Surveillance Programs' (2013) Harvard Journal of Law and Public Policy, text following note 41

The feasibility of a legal process depends, inter alia, on the financial capacity of the ISP. The responsibility to challenge orders through legal process should therefore be restricted to what is reasonable in the specific circumstances.[68]

This raises a further question, of what constitutes a 'reasonable' action that an ISP should take to ensure a right. The standard of such 'reasonableness' should differ from the standard of reasonableness with respect to state action. First, broadly stated, international law leaves states a wide margin of discretion in determining their budgetary priorities. This renders positive measures (as instituting legal process would be) almost outside the realm of obligation. There is an exception to this broad financial discretion of states in the form of core obligations within specific rights, compliance with which is not subject to financial constraints. This exception reflects the fact that governments are established, mandated and obligated under international law to fulfil certain social and other functions. The role which economic constraints may play in their decision making is therefore circumscribed. In contrast, corporations are entities that are created primarily for the purpose of making financial gain; that is their *raison d'etre*. Constraining their financial discretion would limit their operation fundamentally.[69]

In conclusion, ISPs should not be encumbered with the same level of demand as that which may be imposed on states. They should be burdened with positive obligations that require investment of resources only in exceptional circumstances, when the conduct at stake goes to the very core of the right, or where the financial investment is indisputably minimal, and thus does not adversely affect the corporation, regardless of its financial situation.

6.4 Non-collection and non-retention of data

Another way in which ISPs can minimize governmental encroachment on (and consequently potential violation of) clients' privacy is by minimizing the amount of data that they keep in their possession. This can be done by giving clients the option of choosing from a range of privacy setting and helping them understand the implication of their choice.[70] For example, European Union law requires ISPs to provide internet users with 'clear and comprehensive' information about the purposes of personal data processing, and is offered the right to refuse such processing.[71] The effectiveness of such regulation is nevertheless questionable, given that the consent of clients is rarely truly 'informed'.[72] Moreover, few ISPs will publicly acknowledge or advertise the technologies that they use, making it almost impossible for consumers to pick a service provider based on the degree to which their information is protected and retained.[73]

Relatedly, ISPs can limit the period of time during which data is retained.[74] But ISPs are not enthusiastic about non-retention, and in the US, for example, changes in data retention policies have occurred usually in one direction: towards greater retention.[75] Moreover, numerous states have adopted legislation that makes data retention mandatory. The EU, for example, adopted a Data Retention Directive in 2006, which compels all ISPs and telecommunications service providers operating in Europe to collect and retain a subscriber's incoming and outgoing phone numbers, IP addresses, location data, and other key data for a period of six months to two years. This applied to all European citizens, including those not suspected or convicted of any crime. The highly controversial Directive has received mixed reactions in member states, with the constitutional courts in some states having issued decisions striking down data retention laws for violating human rights.[76] In April 2014 the European Court of Justice declared the Directive invalid on the ground that it had, inter alia, exceeded the limits of proportionality in its interference with the rights to privacy and personal

---

[68] For relevant practice in the US see Cardozo et al n 6 3–16

[69] But see the critique on viewing corporations purely as economic actors as opposed to also political actors, Jan Wouters and Leen Chanet, 'Corporate Human Rights Responsibility: A European Perspective' (2008) 6 Northwestern Journal of International Human Rights 262; Ingo Pies et al, 'The Political Role of the Business Firm: An Ordonomic Concept of Corporate Citizenship Developed in Comparison With the Aristotelian Idea of Individual Citizenship' (2014) 53 Business & Society 226

[70] Shift and the Institute for Human Rights and Business n 12 21

[71] European Parliament and Council of the European Union Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) [2012] OJ L 201 37–47, art 5(3)

[72] Joasia A Luzak, 'Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy' (2014) 37 Journal of Consumer Policy 547

[73] Soghoian n 53 195

[74] Dane Jasper, 'Help us, protect your privacy online' (*Sonic.net*, 1 August 2011, <https://corp.sonic.net/ceo/2011/08/01/help-us-protect-your-privacy-online/>

[75] Soghoian (n 53) 213

[76] Electronic Frontier Foundation, 'Mandatory Data Retention' available at <https://www.eff.org/issues/mandatory-data-retention>

data protection of individuals guaranteed, by the Charter of Fundamental Rights.[77] However, states outside the European Union such as Serbia and Iceland have also adopted data retention laws.

7. Measures to prevent violations of the right to privacy

UNGP 19, on the operationalization of the responsibility,[78] requires the following:

> In order to prevent and mitigate adverse human rights impacts, business enterprises should … and take appropriate action'… (b) Appropriate action will vary according to: (i) Whether the business enterprise causes or contributes to an adverse impact, or whether it is involved solely because the impact is directly linked to its operations, products or services by a business relationship; (ii) The extent of its leverage in addressing the adverse impact.

Where a corporation causes or may cause an adverse human rights impact, it should take the necessary steps to cease or prevent the impact, and use its leverage to mitigate any remaining impact to the greatest extent possible. Leverage is the ability to effect change in the wrongful practices of an entity that causes harm if it is directly linked to their activity. Leverage might exist when a corporation collaborates with other actors.[79]

When the corporation lacks the leverage to prevent or mitigate adverse impacts, it should consider ending the relationship. Among the factors that will enter into the determination of the appropriate action in such situations are how crucial the relationship is to the corporation and the severity of the abuse: the more severe the abuse, the more quickly the corporation will need to see change before it takes a decision on whether it should end the relationship.[80]

The distinction between the responsibility not to contribute to a violation and the responsibility to prevent it may not always be clear cut, but for convenience, it is useful to distinguish between measures which ISPs can and ought to take to avoid contributing or facilitating the violation of identifiable clients, and those which they can and should take to impact on government policy, thereby affecting the general population of clients. The previous section addressed the former category, the present section addressed the latter.

7.1 Transparency reports

Transparency reports provide the public, clients as well as non-clients, with data on ISPs' responses to governmental demands. Unlike the law enforcement guidelines considered earlier, transparency reports report practice rather than policy, by providing aggregated data. Transparency reports should include the number of government demands the ISPs receive, and whether they are official demands such as warrants or unofficial requests. The practice of transparency reports, originally led by Google, is spreading among US-based ISPs.[81]

Transparency reports do not affect requests regarding specific individuals, and accordingly it would be difficult to sustain a claim that their publication compromises national security. At the same time, they increase the cost for the government, in terms of international opprobrium and related negative consequences, of having in place national laws that conflict with internationally recognized human rights.[82] They may therefore lead to a change of policy, thereby preventing would-be violations.

7.2 Relocation outside the state

When less severe measures for mitigating conflict between domestic and international law are unavailable or ineffective, the question of divestment or disengagement may arise as a last resort.[83] There are a few precedents of such a move, principally Yahoo!'s and Google's pullouts from China in 2005 and 2010.[84] Commentators have been divided on whether these moves were triggered by moral scruples or by financial

---

[77] C-293/12 and C-594/12 *Digital Rights Ireland Ltd. v. Minister for Communications, Marine and Natural Resources (2014)*, <http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&rid=1>

[78] See also UN Guiding Principles n 24, Commentary to Principle 19

[79] UN Guiding Principles n 24, Commentary to Principle 19; See also Commentary to the OECD Guidelines n 50, 7, summarising principles II.A.12–13

[80] UN Guiding Principles n 24 Commentary to Principle 19

[81] Cardozo et al n 57 15; see eg Infsecurity, 'Yahoo Joins the Disclosure Clan with First Transparency Report' *Infsecurity* (September 10, 2013) <http://www.infosecurity-magazine.com/view/34452/yahoo-joins-the-disclosure-clan-with-first-transparency-report/>

[82] Bersagal n 53 12

[83] Human Rights Watch n 5 37

[84] Alexa Olesen, 'Google China Fallout: Google's Exit Angers China' *Huffington Post* (New York, 23 May 2010)

calculations,[85] but since the corporations' invoke human rights abuses as the ground for their pullout, the question arises whether this is a step that ought to be demanded of ISPs.

The notion that respect for human rights may require divestment is not explicit in the UN Guiding Principles' due diligence requirement. The Commentary to the Guiding Principles addresses 'situations in which the enterprise lacks the leverage to prevent or mitigate adverse impacts and is unable to increase its leverage. Here, the enterprise should consider ending the relationship'.[86] Similarly, the OECD MNE Guidelines link continuation of the relationship between a corporation and a supplier with risk mitigation efforts, including, where appropriate as a last resort, disengagement with the supplier after failed attempts at mitigation.[87] In the case of a relationship mandated by law, ending it in order to prevent risking rights could effectively require shutting down the activity of the corporation in the state in question, or even altogether. Since the demand under the UN Guiding Principles is to take 'appropriate' measures to prevent and mitigate adverse human rights impacts,[88] rather than to take 'every means possible', disengagement that would result in shutting down would probably not be deemed required. Indeed, the Commentary acknowledges that '[a] relationship could be deemed as crucial if it provides a product or service that is essential to the enterprise's business, and for which no reasonable alternative source exists'.[89] In that case, according to the Commentary, 'for as long as the abuse continues and the enterprise remains in the relationship, it should be able to demonstrate its own ongoing efforts to mitigate the impact and be prepared to accept any consequences – reputational, financial or legal – of the continuing connection'.[90] In the context of ISPs required to disclose clients' information, this means that the corporation might continue to operate in the state involved, as long it continues to challenge specific orders where possible and take other measures as discussed here. It would nonetheless be vulnerable to legal and other challenges.

However, it is clear that neither the UN Guiding Principles nor the OECD MNE Guidelines envisage a situation where the relationship is between a corporation and a state acting in sovereign capacity (in which case the relationship is not strictly one of 'business'); nor do they envisage abuse of power by the corporation's own home state. In other words, while the guidelines call on corporations to restrain their international expansion where appropriate for the protection of human rights, they offer no guidance on whether corporations should relocate from their home states.

As a general shortcoming of divestment, critics argue that it is an inherently ineffective measure of human rights protection, because the withdrawal of one corporation would merely lead to the entry of another corporation which is less committed to ensuring human rights. While this is sometimes the case in practice,[91] a corporation may not exonerate itself from responsibility by arguing to be the lesser evil, namely that other corporations would be more injurious to rights. There are, nonetheless, strong arguments why divestment, while always permitted, should not be demanded. A demand to relocate outside a rights-violating state would require corporations to rate states according to their respect for privacy and other related rights, and balance this against the costs involved in relocation and in providing services from outside the state. Moreover, an unlimited responsibility to relocate would mean that corporations are responsible for shielding their clients from any number of states, namely the-ones-to-which-they-should-not-relocate. These are clearly excessive demands. They are all the more so where divestment implies relocating from the corporation's own home state, in which case it might effectively need to close down business altogether.

8. Conclusion

The extensive use of private, electronic technologies has deprived governments of the control they had previously exercised over communications and consequently, of their ability to monitor individuals' interactions. To recoup this power, states now turn to the private actors to whom control over the communication has been transferred, namely ISPs. This changes the paradigm for the protection of the right to privacy. No longer is the state the guarantor of rights, it is now in the position of encroaching on them; the private

[85] Rebecca Fannin, 'Why Google Is Quitting China', *Forbes* (15 January 2010) <http://www.forbes.com/2010/01/15/baidu-china-search-intelligent-technology-google.html>; Molly Wood, 'Google leaving China: Better late than never' *CNet* (26 March 2010) <http://news.cnet.com/8301-31322_3-20001309-256.html>

[86] UN Guiding Principles n 24,Commentary to Principle 19

[87] OECD Guidelines n 50 Commentary para 23

[88] UN Guiding Principles n 24, Principle 19 chapeau

[89] UN Guiding Principles n 24 Commentary to Principle 19

[90] UN Guiding Principles n 24 Commentary to Principle 19

[91] See eg Kit Eaton, 'Did Google Just Worsen China's Human Rights Situation?' *Fast Company* (13 January 2010) <http://www.fastcompany.com/1513933/did-google-just-worsen-chinas-human-rights-situation>; John Kline, *Ethics for International Business: Decision-Making in a Global Political Economy* (Routledge 2010) 65

actors, on the other hand, are no longer the third party against whom the state protects individuals, but potential collaborators, or, alternatively, the defenders of the rights.

An examination of the responsibility to ensure the right to privacy through the conduct of ISPs demonstrates the immense difference between these actors and states. The world of corporations is infinitely more varied than that of states. If corporations and states are two instances of collective entities comprising individuals with designated roles, the similarity ends there. Corporations operate under different legal frameworks, in the pursuit of different goals. This does not mean that there is no scope for translation of standards applicable to states also to corporations. But such translation has to take account of the differences between the types of entities. The existing standards for protecting human rights, reflected in the Protect, Respect and Remedy Framework, build on the characteristics of some corporations, which in some respects resemble states, especially in the measure of control they exercise over individuals. But when looking further afield, the diversity of corporations becomes pertinent. There is no room to assume that all corporations can be subject to the same obligations, nor that they are constrained in the same manner.

This is most strongly apparent in the fact that unlike states, which can refrain from action and thus can always respect rights at least in part, ISPs acting under legal obligations have no choice but to encroach on the right to privacy. On the other hand, ISPs may at times be in a position to influence states, either legally or through other means. Exempting them from the responsibility to do so may be not only unwarrantedly lenient, but may actually serve as a loophole for states to evade their own obligations.

Bibliography

Anastasiadis S, 'Toward a View of Citizenship and Lobbying Corporate Engagement in the Political Process' (2014) 53 Business and Society 260

Clapham A and Jerbi S, 'Categories of Corporate Complicity in Human Rights Abuses' (2000–01) 24 Hastings International and Comparative Law Review 339

de Schutter O, *International Human Rights Law: Cases, Materials, Commentary* (CUP 2010) DOI 10.1017/CBO9780511779312

Cardozo N et al '2014 Who Has Your Back? Which Companies Help Protect Your Data from the Government?' (Electronic Frontier Foundation 15 May 2014) 14

Golden Bersagal A, 'Meeting the Responsibility to Respect in Situations of Conflicting Legal Requirements', A Good Practice Note endorsed by the United Nations Global Compact Human Rights Working Group on (UN Global Compact 13 June 2011)

Jerbi S, 'Business and Human Rights at the UN: What Might Happen Next?' (2009) 31 Human Rights Quarterly 299

Kinley D and Tadaki J, 'From Talk to Walk: The Emergence of Human Rights Responsibilities for Corporations at International Law' (2004) 44 Virginia Journal of International Law 931

Luzak JA, 'Privacy Notice for Dummies? Towards European Guidelines on How to Give "Clear and Comprehensive Information" on the Cookies' Use in Order to Protect the Internet Users' Right to Online Privacy' (2014) 37 Journal of Consumer Policy

Milanovic M, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' Harvard International Law Journal (forthcoming)

Pies I et al, 'The Political Role of the Business Firm: An Ordonomic Concept of Corporate Citizenship Developed in Comparison With the Aristotelian Idea of Individual Citizenship' (2014) 53 Business & Society 226

Ratner S, 'Corporations and human rights: a theory of legal responsibility' (2001) Yale Law Journal 443 DOI: http://dx.doi.org/10.2307/797542

Ronen Y, 'Human Rights Obligations of Territorial Non-State Actors' (2013) 46 Cornell International Law Journal

Sinha A, 'NSA Surveillance Since 9/11 and the Human Right to Privacy' (2014) 59 Loyola Law Review 861

Soghoian C, 'An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government' (2011) 12 Minnesota Journal of Science and Technology 191

Triffterer O, 'Article 33' in Otto Triffterer (ed),*Commentary on the Rome Statute of the International Criminal Court* (2nd edn, CH Beck, Hart, Nomos 2008) 913 DOI 10.1017/CBO9780511894589

Wouters J and Chanet L, 'Corporate Human Rights Responsibility: A European Perspective' (2008) 6 Northwestern Journal of International Human Rights 262

Yoo J, 'The Legality of the National Security Agency's Bulk Data Surveillance Programs' (2013) Harvard Journal of Law and Public Policy

How to cite this article: Yael Ronen, 'Big Brother's Little Helpers: The Right to Privacy and the Responsibility of Internet Service Providers' (2015) 31(80) Utrecht Journal of International and European Law 72, DOI: http://dx.doi.org/10.5334/ujiel.cs

Published: 27 February 2015