A Critical Assessment on the Extraterritorial Application of Human Rights Treaties to Transnational Cyber Surveillance

Wanshu Cong*

INTRODUCTION

The issue of mass transnational cyber surveillance arises in a time when there has been a clear trend of expanding the application of human rights treaties. So it was not surprising that in the report on privacy in the digital age produced by the Office of the High Commissioner for Human Rights ["ECtHR"] in July 2014, when addressing extraterritorial surveillance and interception of communications, the report restated that "a State may not avoid its international human rights obligations by taking action outside its territory that it would be prohibited from taking 'at home'"[1] and that "[t]his holds whether or not such an exercise of jurisdiction is lawful in the first place, or in fact violates another State's sovereignty."[2] The control standard to be applied to cyber surveillance triggering jurisdiction given in this report[3] may well be controversial, but the trend recognizing extraterritorial application is certainly clear. However, the report was silent on the substantive requirements to be applied to transnational cyber surveillance. By addressing the scope of human

---

* Wanshu Cong is currently studying for her PhD at the Law Faculty of McGill University, under Professor Frédéric Mégret's supervision. Her thesis, entitled 'Human Rights in the Digital Age: A Theory of A-Territorial Human Rights', examines the reconstruction of the spatial imaginaries of human rights by means of surveillance and digital technologies used by states and individuals. She is an LLB graduate (2013) from Shantou University, China and a LLM graduate of the Geneva Academy of International Humanitarian Law and Human Rights (2014). Her research interests include legal theories, history of international law, human rights law and global governance.

1 *Right to Privacy in A Digital Age: Report of the Office of the High Commissioner of Human Rights,* UNHRC, 27th Sess, UN Doc A/HRC/27/37 (2014), at para 33 [*OHCHR*].

2 *Ibid* at para 34.

3 *Ibid*:

> "It follows that digital surveillance therefore may engage a State's human rights obligations if that surveillance involves the State's exercise of power or effective control in relation to digital communications infrastructure, wherever found, for example, through direct tapping or penetration of that infrastructure. Equally, where the State exercises regulatory jurisdiction over a third party that physical controls the data, that State also would have obligations under the Covenant. If a country seeks to assert jurisdiction over the data of private companies as a result of the incorporation those companies in that country, then human rights protections must be extended to those whose privacy is being interfered with, whether in the country of incorporation or beyond."

rights protection in separate sections, i.e., the application of the law and the substantive requirements of lawful interference on fundamental freedoms such as the right to privacy, it seemed as if once the law was applicable, the requirements applied to internal and foreign surveillance in the same way. And no distinction between internal and foreign surveillance was made in its recommendation on furthering the analysis on the principle of necessity, proportionality and legitimacy in relation to surveillance practices.[4]

In this essay, I question the appropriateness of applying the substantive requirements of lawful domestic surveillance developed from international human rights treaties and relevant case law to transnational cyber surveillance. And I argue in the negative. Therefore, for the purpose of this essay, I would not delve into the highly debatable issue of what counts as "control" in cyber surveillance and which standard of control triggers a state's jurisdiction. Instead, this essay assumes that a control test was established. In the following section, I shall examine the substantive requirements for states restricting fundamental freedoms drawn on from current human rights case law. And I shall demonstrate why these tests, which are designed for internal surveillance, will be problematic if applied to foreign cyber surveillance. My approach is territorial. And the core of the problems, I argue, is that the legal and political implications of territory and border, as currently understood, cannot provide a satisfying theoretical basis for expanding states' regulatory power extraterritorially. I understand that my territorial approach may be considered very conservative, or Westphalian, and therefore, I would address some potential responses to my arguments in the conclusion.

I. APPLYING HUMAN RIGHTS TREATIES TO TRANSNATIONAL CYBER SURVEILLANCE

Requirements for lawful domestic surviellance are understood as the conditions under which a state can lawfully restrict the right to privacy and the freedom of expression which are among the fundamental freedoms of an individual. These rights are not absolute as they allow certain limitation and derogation by the state.[5] A classic examination of the legality of limitation on fundamental freedoms and the validity of derogation can be seen, for example, from the Siracusa Principle on the Limitation and Derogation Provision in the ICCPR.[6] In the following analysis, I pick out three substantive requirements —

---

4 *Ibid* at para 51.

5 See e.g *International Covenant on Civil and Political Rights*, 19 December 1966, 999 UNTS 171, arts. 4, 17, 19 (entered into force 23 March 1976) [*ICCPR*]; *Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 UNTS 221, arts 8, 10, 15 (entered into force 3 September 1953) [*ECHR*]; *American Convention on Human Rights*, 22 November 1969, 1144 UNTS 123, arts 11, 13, 27 (entered into force 18 July 1978).

6 *The Siracusa Principles on the Limitation and Derogation Provisions in the International*

(i) being prescribed by the law; (ii) having legitimate purposes; and (iii) proportionality — to demonstrate the difficulties in their extraterritorial application.

(a) Being Prescribed by the law

The requirement of being prescribed by the law for lawful limitations means that the law which serves the basis of limiting the fundamental freedoms should be accessible to the public and produce foreseeable legal consequences. For a territorial sovereign state, this requirement prohibits secret legislation which is deemed as tyrannical and inconsistent with the rule of law and democratic accountability.[7] Publishing and distributing the law to the people is thus an obligation of the state towards the general public. It is assumed that a properly promulgated law satisfies the accessibility requirement. Adding up to the requirement of accessibility is the qualitative requirement of foreseeability. The law should not only be promulgated publicly, but its content should be formulated with sufficient precision to allow people to regulate their behaviours.[8] There is meanwhile a maxim that ignorance of the law by someone cannot excuse his/her illegal conduct. Underlying this maxim and the requirement of accessibility and foreseeability of the law is a reciprocal relationship between the sovereign and its subjects. As state itself is territorial, such a reciprocal relationship — the mutual obligations between states and people — is restricted by territory. So for non-citizens, as long as they remain outside the territory of a state, they do not owe obligations to obey the law of that state. But upon the entry to a state by a foreigner, it is presumed that the foreigner is informed of the local laws and is obliged to obey them.

This spatial presumption of accessibility and foreseeability of the law is difficult to maintain in cyberspace where the conduct of individual may be subject to multiple jurisdictions, depending on the route and destination of the informational flow. And even the laws are published in most jurisdictions and many states have official websites and databases dedicated to publishing domestic legislations, it is not reasonable to assume that individuals will be able to know all the laws of other countries which could be potentially applicable to them.

Furthermore, in the situation of surveillance and espionage, it is not that individuals actively contact a foreign state by actively circulating and making materials accessible in that state, like what usually happen in defamation cases,[9]

Covenant on Civil and Political Rights, UN Commission on Human Rights, 41st Sess, UN Doc E/CN.4/1985/4, Annex (1984).

7 Christopher Kutz, "Secret Law and the Value of Publicity" (2009) 22:2 Ratio Juris 197.

8 See e.g. *Rotaru v Romania* [GC], No 28341/95, [2000] V ECHR 192, 8 BHRC 449, at para.52.

9 Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge: Cambridge University Press, 2007) at 111.

but the opposite. More importantly, such contact is without the knowledge of the impacted persons. Secrecy is the whole point of surveillance and espionage. When a state carries out internal surveillance against its own people, publicity of the surveillance law does not negate the secrecy of specific surveillance operation.[10] Therefore, in a domestic setting, there is no contradiction between the accessibility requirement of the law and the nature of surveillance. However, in the situation of transnational cyber surveillance, the secrecy of the surveillance operation would mean that people are unable to tell not only whether they are being spied, but also by whom they are being spied, needless to say the domestic legal basis of the surveilling state for such surveillance operations. Currently, there seems to be no satisfying solutions. Either states forgo the advantage of secrecy of cyber surveillance, notify the non-citizens that they are being spied, and so make the legal basis of surveillance accessible to them, and meanwhile try not to reveal too much detail that would defeat the purpose of the whole surveillance operation; or, the reciprocal relationship between the sovereign and people needs to be reconceptualised in the cyberspace: the accessibility of a state's domestic law becomes universal and the publication of a state's legislation creates an obligation of everyone in the cyberspace to know about that legislation. Except the case where two countries could achieve certain kinds of understanding of mutual espionage (not necessarily using the word espionage or surveillance), the first option is hardly a politically feasible one. And even where two countries agreed on mutual espionage, like Australia and Indonesia did in 2014,[11] there are more questions to be considered, such as the validity of this kind of agreement under international law and the scope of domestic judicial oversight on such mutual espionage. The second option is unreasonable because it would expose individuals to the laws of all countries, and therefore lead to a sheer imbalance between rights and obligations of individuals and states. In short, the territorial limit presumed in the accessibility requirement of national law cannot be reconciled with the extraterritorial human rights limitations imposed through cross-border cyber surveillance programmes.

(b) Legitimate Purposes

The imposition of a lawful restriction on fundamental freedoms must pursue legitimate purposes which are permitted by the human rights treaties. Taking it together with the proportionality requirement discussed in the following subsection, they are subsumed in the test of "democratic necessity". While it

---

[10] *Malone v the United Kingdom* (1984), 10 ECHR (Ser A), 7 EHRR 14, at para.67:

> "[T]he requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conductions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence."

[11] "Julie Bishop hails spying code of conduct with Indonesia", *The Guardian* (28 August 2014), online: <www.theguardian.com/world/2014/aug/28/spying-code-of-conduct>.

has been argued that the context of the measures taken (i.e. the legitimate purpose, and the specific measures, which pertains to their proportionality) cannot be analysed separately,[12] I still divide my discussion into two parts because the two requirements would have some distinct problems posed by transnational cyber surveillance.

The legitimate purposes in the limitation clauses can be grouped into four categories in general: security concerns; health and morals; economic well-being, and the rights of other individuals.[13] The lawfulness of derogations presumes the existence of a state of emergency in which the state has to defend itself, and therefore the purpose of derogation is close to the security concerns among the legitimate purposes of lawful limitations. For the purpose of this paper, I treat these requirements of limitation and derogation together under a general notion of legitimate purpose.

Similar to the requirement of having a legal basis, there is a territorial presumption within the notion of legitimate purpose. Despite various theoretical accounts for this notion,[14] legitimate purpose is still largely a self-judging and self-imposing notion.[15] To be specific, a state or a community determines by itself its own public purposes and takes regulatory measures on its subjects in pursuing the purposes. And the legitimacy of a particular public purpose means the purpose is legitimate to the members of the political community. Currently, international human rights law does not justify or account for a state taking measures vis-à-vis non-citizens outside its own territory for the self-judging public purposes.[16] Such unilateral exercise of sovereign power will be simply against the principle of sovereign equality and non-intervention. The general prohibition of unilateralism sets the territorial limit to the legitimacy of public purpose and the measures pursuing it.

The self-judging and self-imposing character of the notion of legitimate purpose cannot be easily reconciled with states' transnational activities

---

[12] Scott Sheeran, "Reconceptualizing States of Emergency under International Human Rights Law: Theory, Legal Doctrine, and Politics" (2013) 34:3 Mich J Intl L 491.

[13] See e.g ECHR, *supra* note 5 art 8(2).

[14] See e.g. Aileen McHarg, "Reconciling Human Rights and the Public Interest: Conceptual Problems and Doctrinal Uncertainty in the Jurisprudence of the European Court of Human Rights" (1999) 62:5 Mod L Rev 671.

[15] Pedro J. Martinez-Fraga and C. Ryan Reetz, *Public Purpose in International Law: Rethinking Regulatory Sovereignty in the Global Era* (New York: Cambridge University Press, 2015) at 206.

[16] There are some arguments in favour of extraterritorial derogation from human rights treaties, see e.g. Marko Milanovic, "Extraterritorial Derogations from Human Rights Treaties in Armed Conflict" in N Bhuta, ed., *The Frontiers of Human Rights: Extraterritoriality and Its Challenges* (Oxford: Oxford University Press, 2016) 55; Lawrence Hill-Cawthorne, *Detention in Non-International Armed Conflict* (Oxford: Oxford University Press, 2016) at 216. However, the support from case law and state practice is scant. And as I shall argue below, the extraterritorial derogation suffers from a more serious problem of democratic legitimacy.

restricting human rights. The only exception is the case of military occupation, where a special regime of international humanitarian law expressly provides for the obligation of the occupying power to ensure the security of the population in the occupied territory.[17] For transnational cyber surveillance, we need to ask how the public purpose, assuming it is legitimate for one state's own people, can be equally legitimate for citizens of other states who are the targets of surveillance. If the legitimate purpose remains to be an effective requirement, do we need to reconceptualise this notion as referring to, say, public purpose that is legitimate for everyone who may be subject to surveillance? If that was the case, the appreciation of legitimate purpose could no longer be self-judging anymore, because cross-border legitimacy means there needs to be some objective criteria for the determination of legitimate purpose. Accordingly, human rights tribunals may not be able to enjoy the benefit of margin of appreciation as much as they do now.[18] But even with some objective criteria either developed by human rights treaty bodies[19] or recognised by multiple states, there remains a huge leap toward subjecting non-citizens abroad to a state's surveillance which pursues an objectively established legitimate purpose of this state.

The notion of legitimate purpose necessarily limits the territorial scope of human rights restrictions as the purpose and the restrictions need to answer to the "public". It will be a common challenge for any transnational measures limiting fundamental freedoms of individuals. But for bulk cyber surveillance in particular, there is an additional problem for the requirement of public interest. The bulk surveillance, relying on the technology of big data and aiming at pre-emption, fundamentally changes the way of conducting intelligence. Massive amount of data is collected first, and data analysis and pattern recognition are conducted afterwards.[20] And only after the data collection and analysis, it may become clear whether there is a concern of, for example, national security.[21] In other words, in bulk cyber surveillance, human rights are restricted even before a legitimate purpose is identified, which goes against the rationale of permitting

---

[17] See e.g. *Geneva Convention Relative to the Protection of Civilian Persons in Time of War*, 12 August 1949, 75 UNTS 287 art. 49 (entered into force 21 October 1950) [*Fourth Geneva Convention*].

[18] See Sheeran, *supra* note 12.

[19] The European Commission on Human Rights indeed drew on some objective criteria for the determination of state of emergency in the Greek case, *Thlimmenos v. Greece*, see *infra* note 24. However, treaty bodies have been deferring to states' own factual assessment and avoiding the issue by analysing the proportionality of derogatory measures.

[20] Bart van der Sloot, "How to Assess Privacy Violations in the Age of Big Data? Analysing the Three Different Tests Developed by the ECtHR and Adding for a Fourth One" (2015) 24:1 Inf & Comm Tech L 74.

[21] And it may well be the case where the authorities do not know what to do with the massive amount of data simply because there is too much of it. See e.g. Alan Travis & Own Bowcott "'Snooper's Charter' will Cost British Lives, MPs are Warned", *The Guardian* (6 January 2016), online: < www.theguardian.com/world/2016/jan/06/snoopers-charter-will-cost-british-lives-mps-warned > .

limitations on human rights. And as we will see, without identifying a specific legitimate purpose, it will lead to serious problems with the requirement of proportionality.

(c) Proportionality

(i) Proportionality of Surveillance

Proportionality has been a major point of criticisms on states' surveillance measures. To a certain degree, focusing on the issue of proportionality seems to be a smart attempt to escape the highly political debate on the legality of surveillance, because our phrasing of proportionality in terms such as balancing appears to suggest that proportionality assessment can be done simply technically. Such an approach, usually taken by human rights treaty bodies, is severely criticised by Tsakyrakis as "pervert[ing] rather than elucidate[ing] human rights adjudication",[22] because under the guise of balancing, the truly difficult moral judgments of what is right and what is wrong are avoided, and with this guise, we simply forget that sometimes there is no balance to be struck in the first place. If there is no legitimate purpose, a measure cannot be lawful no matter how proportionate it is designed. So even if a transnational cyber surveillance programme is designed to be targeted and smart, there remains the hard question whether surveillance has a legitimate purpose and how international law deems a purpose of surveillance legitimate.

Even when we focus on the proportionality test, it turns out that a neutral and technical proportionality assessment is a myth. Proportionality assessment is full of value judgments, and the severity of an interference largely depends on the importance attached to the right.[23] Besides, proportionality and legitimacy of the purpose of the disputed measure have a more nuanced relation. In a classic assessment of the legality of limitations, the issue of legitimate purpose comes before the assessment of proportionality, as mentioned above. So usually if the disputed measure is not taken for a legitimate purpose, there is no need to proceed on proportionality any more. However, as the ECtHR has held, a disproportionate measure would illegitimize the purpose of the disputed measure.[24] This suggests that proportionality is not only a constituent part for assessing the legality of limitation, but also a check on the alleged legitimate purpose. And for the issue of cyber surveillance, such an interplay warns us that the legitimacy of the purpose of cyber surveillance claimed by the states cannot be taken at face value, because disproportionality could refute the presumption of legitimacy.

---

[22] Stavros Tsakyrakis, "Proportionality: An Assault on Human Rights? " (2009) 7:3 Intl J Constitutional L 468, at 487.

[23] Andrew Legg, *The Margin of Appreciation in International Human Rights Law: Deference and Proportionality* (Oxford: Oxford University Press, 2012), at 184.

[24] *Thlimmenos v. Greece* [GC], No 34369/97, [2000] IV ECHR 263, 31 EHRR 15, para.47.

While state practice remains quite ambiguous,[25] there is a growing consensus at the international level and European regional level on the disproportionality of mass or bulk surveillance programmes.[26] This recognition of disproportionality will incentivise states to design their surveillance programme in a more self-restraining way. But proportionality remains problematic even the state conducting surveillance with sufficient self-restraint. In the following part of this subsection, I shall discuss the quandary of democratic legitimacy of proportionality in its extraterritorial application, which I believe cannot be resolved simply by heightening the scrutiny in its application.

(ii) Extraterritoriality and Democratic Legitimacy

As noted earlier, proportionality is part of the test of "democratic necessity". As the other part of the test, i.e. legitimate purpose, is territorially limited, this territorial limitation naturally applies to the requirement of proportionality. It means that the elements for assessing the proportionality of a regulatory act by the state are inherently confined to a democratic society. This territorial scope of proportionality is supported by the doctrine of margin of appreciation. The close relation between these two doctrines, described by Andrew Legg, is that the margin of appreciation serves as an external factor which is considered along with the internal factor — the nature of the rights — in the assessment of proportionality.[27] The doctrine of margin of appreciation is a judicial construction by the human rights bodies which gives deference to individual states when the judicial body feels incompetent to make a decision. The feeling of incompetence of the judicial body may come from the perception that a state's decision enjoys democratic legitimacy,[28] the recognition of the plurality of state practice or the expertise of states pertaining to a disputed issue.[29] The metaphor of "margin", taken literally, suggests the spatial scope within which the state can exercise regulatory sovereignty.

A quick overview of the current jurisprudence of human rights bodies shows that the test of proportionality has so far been considered largely in cases of domestic limitations or derogations. Its use in dealing with extraterritorial matters has been limited,[30] with only the exceptional situations of extraterritorial

---

[25] Even some states which are usually believed as human rights model countries, such as Netherlands, Denmark, France, Switzerland, have either adopted or been considering about the adoption of laws authorizing bulk interception of communications.

[26] *OHCHR*, *supra* note 1; *Schrems v Data Protection Commissioner*, C-362/14, [2015], online: .

[27] Legg, *supra* note 23, at 198.

[28] But it will be an ironic if an international tribunal defers to a state due to the consideration of democratic legitimacy when the state does not have such democratic legitimacy to take measures on non-citizens abroad.

[29] Legg, *supra* note 23, at 70-174.

[30] It is especially so at the ECtHR. Several reasons contributed to the limited consideration on the issue of proportionality. Firstly, a great amount of attention was paid to the

use of force[31] and military occupation.[32] In both these situations, discussions have largely been focused on the relation, and indeed the reconciliation, between international human rights law (IHRL) and international humanitarian law (IHL). And it has been argued convincingly by Aeyal Gross that a reconciliation between the two branches of law would conflate two different proportionality requirements.[33] Proportionality under IHRL and IHL has completely different applications. The reason lies in their distinctive rationales: for IHRL, balance (or calculation) is conducted by assuming individuals as equal subjects of the state; such equal footing does not exist for IHL which explicitly characterizes people, properties and objects into different categories and differs the protection accordingly.[34] Local people living in the occupied territory are "protected persons" while settlers of the occupying power are not.[35] The protection of settlers of the occupying power will not come into play in the calculation of proportionality of measures, for example, destroying the properties of "protected persons" under IHL.[36] The result of applying proportionality test in IHRL to an occupation scenario is that the protected persons in the occupied territory are considered to be on an equal footing with people of the occupying power (both

problem of jurisdiction, and the merits were less discussed. Secondly, sometimes, proportionality was avoided by the Court finding that a limitation imposed by a state did not have a legitimate aim. See e.g. *Catan and Others v. The Republic of Moldova and Russia* [GC], Nos 43370/04, 8252/05 and 18454/06, [2012] V ECHR 309, 57 EHRR 4. Thirdly, in some cases concerning armed conflicts, the Court was applying the necessity and proportionality tests in IHL. See e.g. *Al-Jedda v. The United Kingdom* [GC], No 27021/08 [2011] IV ECHR 305, 53 EHRR 23. Fourthly, the violation of human rights in extraterritorial settings was claimed and found with respect to a state's positive obligation such as the obligation to investigate the killing of an individual. So the proportionality of a limitation imposed by a state, which pertains to a state's negative obligation, was not litigated. See e.g. *Jaloud v. The Netherlands*, No 47708/08 [2014] ECHR 1292.

31 Use of lethal force, see *Pisari v The Republic of Moldova and Russia*, No 42139/12 [2015] ECHR 403. The ECtHR found that there was available alternative means to stop the car without recourse to lethal force, and so the killing of Pisari was not absolutely necessary for the purpose of effecting a lawful arrest.

32 See e.g. *Beit Sourik Village Council v. The Government of Israel [et al.]* (2004), HCJ 2056/04 (Israel); *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, [2004] ICJ Rep 136.

33 Aeyal M. Gross, "Human Proportions: Are Human Rights the Emperor's New Clothes of the International Law of Occupation?" (2007) 18:1 Eur J Intl L 1; Martti Koskenniemi, "Occupied Zone - 'A Zone of Reasonableness'?" (2008) 41 Israel LR 13.

34 Gross, *supra* note 33 at 5.

35 *Fourth Geneva Convention*, *supra* note 17 arts 4, 49(5).

36 Typical proportionality test in IHL to be applied to occupied territories includes "absolutely necessary" for the security of the detaining power in article 42 of the *Fourth Geneva Convention*, "absolutely necessary by military operations" in article 53 of the *Fourth Geneva Convention*, "necessary for imperative reasons of security" in article 78 of the *Fourth Geneva Convention*: *supra* note 17.

living within the territory of the occupying power and settling in the occupied territories). And the rights of the protected persons, which IHL exactly seeks to protect, become vulnerable to the trade-off for the rights of non-protected persons.[37] By conducting such a proportionality test, the military commander acts as if he was a proper sovereign. Ironically, a well-intentioned IHRL talk of proportionality has rather perpetuated and institutionalised the unlawful occupation.

This kind of worry is not absent in our case of transnational cyber espionage. In peacetime, although there is no category similar to "protected person" in IHL, treating foreigners abroad as subjects of a state's managerial power on an equal plane with people within the state's own territory will encounter difficulties. Two propositions seem to justify such equal footing. First is the principle of non-discrimination in human rights law.[38] Citizenship is one of the prohibited grounds of discrimination in most human rights treaties.[39] However, I argue that this principle ensures same treatment to everyone within the formal jurisdiction of a state. As a matter of fact, for people living in a state's extraterritorial jurisdiction, different treatment is rather accepted. In the occupation cases discussed above, treatment will be indeed discriminatory in the sense that "protected persons" need to be especially taken care of under IHL, and this discriminatory treatment is an outright recognition of the lack of democratic legitimacy of the occupying power. In other situations of extraterritorial jurisdiction, states' obligations are also differentiated based on the actual power and the legitimacy of the power. For example, when a state, through its control of a transnational corporation, owes human rights obligations towards local people of another state, the scope of the negative and positive obligations of the state depends on the extent of its power which will affect the local people.[40] The difference between the extraterritorial power and domestic sovereign authority means that the obligations owed by the state towards people within and without its territory are materially different. It means that even the case is not occupation where "protected persons" need special protection, there lacks a theoretical basis to treat people within a state's territory and non-citizens abroad as equal parties and equal subjects of the regulatory power of a sovereign state. Furthermore, even if the principle of non-discrimination requires factually equal treatment, such a requirement would be based precisely on a recognition that the formal statuses of nationals and foreigners are different. It is this recognition that

---

[37] Gross, *supra* note 33; Koskenniemi, *supra* note 33.

[38] Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age" (2015) 56:1 Harv Intl LJ 81, at 98.

[39] UN Human Rights Committee, *General Comment No.31: Nature of the General Legal Obligation on States Parties to the Covenant*, UN Doc CCPR/C/21/Rev.1/Add.13, May 26 2004 at para.10.

[40] Robert McGorquodale & Penelope Simons, "Responsibility beyond Borders: State Responsibility for Extraterritorial Violations by Corporations of International Human Rights Law" (2007) 70:4 Mod L Rev 598.

leads to a restriction on what can legally be done to foreigners by the sovereign state,[41] and it leads to categories such as "national treatment", "the most favourable nation treatment", etc. In short, the principle of non-discrimination does not result in the equal formal status between citizens and non-citizens within and without the state's territory. And it means that non-citizens outside a state's territory cannot be legitimately presumed as its subjects when a state conducts the proportionality test.

The other propositions supporting equal footings of people within a state and foreigners abroad will be the idea that states are joint trustees of humanity.[42] Such a cosmopolitan view considers states exercising extraterritorial jurisdiction as surrogate trustees of the local people, and it requires that everyone who is factually subject to the regulatory power of a state should be protected equally. And this claim also supports the obligation of a state toward foreigners is context-based.[43] This claim of joint trustees of humanity indeed provides a useful account for states undertaking extraterritorial human rights obligations. But such an abstract and indeed aspirational account does not necessarily lead to equal status between nationals and foreigners. The occupying power would be a proper "surrogate trustee", and the relation with the "protected persons" in the occupied territories is fundamentally different from its relation with its own people. More importantly, this account of joint trustees of humanity, as well as the non-discrimination proposition, needs to be aware that blurring the formal distinction of people may sanction the expansion of the regulatory power of a state to those non-citizens who see the restrictions on their human rights have no legitimacy in the first place.

That being said, one of the difficulties in applying the proportionality test extraterritorially is that we do not have a satisfying theoretical basis for treating the non-citizens abroad and the people within the state's own territory as equal subjects of the unilateral regulatory power of a sovereign state.

II. CONCLUSIONS

In the above sections, I have identified the problems in applying the tests for lawful limitation on fundamental freedoms to transnational cyber surveillance. The core of those problems is that the territoriality of sovereign state is not only geographical. Territoriality has significant legal and political implications in the sense that the democratic legitimacy of a state's regulatory power is always

---

[41] How to treat foreigners can be seen as "justice sensitive externalities", a term used by Mattias Kumm, which sovereign states have no legitimate authority to address unilaterally: Mattias Kumm, "The Cosmopolitan Turn in Constitutionalism: An Integrated Conception of Public Law" (2013) 20:2 Ind J Global Leg Stud 605.

[42] Evan J. Criddle & Evan Fox-Decent, *Fiduciaries of Humanity: How International Law Constitutes Authority* (New York: Oxford University Press, 2016); Eyal Benvenisti, "Sovereigns as Trustees of Humanity: On the Accountability of States to Foreign Stakeholders" (2013) 107:2 AJIL 295.

[43] Criddle & Fox-Decent, *supra* note 42 at 192-198.

territorially limited. For transnational cyber surveillance, I argue that any call for extraterritorial application of human rights law needs to be aware of the territorial limit of democratic legitimacy as currently understood. A territorial perspective of my argument may appear to be outdated since focusing on territoriality is just the remnant of the old fashioned Westphalia dogma and appears to be antithetical to the universalist vision of human rights.[44] It is my opinion that as long as sovereign state remains to be the default political form, territories and borders necessarily have certain political and moral implications on individuals' relation with states. To be sure, the human rights of individuals are beyond territories of sovereign states. However, the substance of the rights, which are affected by how states can legitimately exercise regulatory sovereign power, is territorially contingent.

While it is not my intention to be against extraterritorial application of human rights treaties, I understand that a possible criticism on my argument would be that I am using my assessment on the substantive requirements against the idea of extraterritorial application. So this possible criticism may argue that I confound the merits and applicability issues. I wish to respond to this potential criticism in the final conclusion.

The claim that my argument tends to confound the merits and applicability issues presumes that the two issues can be clearly separated conceptually. And so, logically, the merits issues only come after the admission that human rights law indeed applies extraterritorially to states' foreign cyber surveillance. The applicability-merits separation also implies that the two issues would address different problems. So, for the applicability of human rights law outside a state's territory, a major assessment is when a state has reached sufficient degree of control to trigger its jurisdiction under human rights law, whereas how such control interferes with or violates what human rights are issues of merits.

This separation, which appears to be valid in judicial reasoning, does not necessarily mean that applicability is free from the impact of the problems in the merits issue. As discussed above, democratic legitimacy is a major problem in the substantive requirements of limitation on fundamental freedom in transnational cyber surveillance. If we understood democratic legitimacy from a traditional territorial perspective, there is no satisfying explanation for a state unilaterally exercising regulatory sovereign power on non-citizens outside its territory, whether in claiming legitimate public purposes, or conducting the proportionality assessment, or expanding the accessibility of its domestic law universally. Without a re-conceptualization of democratic legitimacy, merely accepting the extraterritorial application of human rights law can be politically unappealing. Especially in peacetime cyber surveillance between effective sovereigns, the state which is surveilled may also object the argument of extraterritorial application of human rights law because the argument opens the door to unilateralism and may lead to an ironic justification for the violation of

---

[44] Marko Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (New York: Oxford University Press, 2011) at 80.

the sovereignty of the state being surveilled. In this sense, to argue for extraterritorial application of human rights law not only tends to avoid the hard question that whether cyber surveillance is lawful under international law, but could also create a situation which regulates and institutionalizes potential violation of sovereign equality by cyber surveillance.

More importantly, I argue that the claim about the applicability of the law cannot be made without understanding how the law is going to be applied. When we speak about extraterritorial application of human rights law, we mean the whole body of human rights law, not only the negative obligations of states. So to expand the application of human rights law means also to expand states' regulatory power outside their borders. Sovereign states still enjoy a great deal of leeway in the interpretation of human rights law, and especially for those non-absolute rights which are highly relevant in cyber surveillance. Just like the doctrines of proportionality and margin of appreciation, which are judicial constructions not necessarily resulting in more protection of human rights, extraterritorial application of human rights treaties is not a promise for more protection either. So the claim for extraterritorial application of human rights law, should it have any normative significance as we hope, need to be combined with the understanding of merits issues. Otherwise, the claim of extraterritorial application of human rights law could become a rhetoric game of states, each paying lip services and accepting the claim without good faith. It will undermine the integrity of the human rights regime, despite our good intention in arguing for the expansion of the application of human rights law. Therefore, I believe that a holistic approach is more desirable.

Do They Want to Regulate Online Profiling?

Laura Garcia Vargas[*]

"Bottom line: More personal information, more money. It is a valid business model, the one that gives us, in return, access to Internet largely free of monetary charges. But it is a tricky one: personal information becomes not only a currency but the currency. The entire business model rests upon the amount and precision of personal information collected."[1]

Abstract

Online profiling or behavioural tracking is the process by which private companies track and gather data about users' activities in online platforms. The data collected by all the companies is aggregated with the purpose of creating a comprehensive profile about users. Since at least 15 years ago, there have been several attempts to regulate online profiling in order to reduce its privacy implications. In general, these regulations have tried to limit the way the information is used, the type of data that is collected, and impose or suggest the security standards that the companies should take to protect it.

This article will demonstrate that the proposed regulations do not reduce online profiling's privacy repercussions. In addition, it will argue that in order to reduce privacy repercussions it is necessary to regulate the aggregation and commercialization of the data. However, governments, industries, and users may not have enough incentives to find alternative methods or effective regulations to address the problems raised by online profiling.

INTRODUCTION

The tracking of individuals' activities is an old practice. Even before the digital era, companies tracked their customers to understand and analyze their behaviour in order to design better marketing campaigns. With the invention of the computer, and later the internet, it became easier to track customers, to keep a record of the tracking, and to analyze the data. Moreover, it became possible and easy to share the data with other companies in order to understand better the behaviour of a particular individual.

Due to new technologies, an old practice used by companies to improve their marketing campaigns, now is the one of the major sources of personal data collection and creation of databases. As technology advances, not only does the

---

[*] PhD Candidate at the Faculty of Law, University of Ottawa

[1] Office of the Privacy Commissioner of Canada, "Speech: Online Behavioural Advertising – Putting a Normative Framework Around a Business Model – January 21, 2014" (10 March 2014), online: < www.priv.gc.ca/media/sp-d/2014/sp-d_20140121_cb_e.asp >.

tracking become easier, but the information collected by companies becomes more precise and more revealing of the private life of the tracked customer.

Right now there is an industry around personal information. There are hundreds of companies making profits from the personal information of online platforms users. For some of the companies the business is to track users across different platforms, for others is to facilitate the aggregation, and for others is to gain some type of advantage by using that information. The tracking of the online behaviour of the users of online platforms is called online profiling or behavioural tracking.[2]

This paper will explain the practice of online profiling by dividing it in five stages: (1) installation of the technology, (2) tracking of the users, (3) collection of the data in private databases, (4) aggregation of the data, and (5) use of the profiles created after the aggregation of the data. Graphic 1 illustrates these stages and highlights some of the problems that arise in each of them.

Graphic 1. Online Profiling Process

Online profiling arise several privacy implications for the personal information of the online platform users. Policy makers in the United States, Canada, and the European Union have attempted to regulate this practice to reduce the threat to privacy that it represents. Nevertheless, these attempts of regulation have not been successful. The main problem that policy makers have identified is the lack of transparency and users' knowledge with which this practice occurs. Consequently, most of the proposed regulations have focused in making the practice more transparent, informing the users, and asking for the users' consent. Nevertheless, the biggest threat to privacy and the real value of the practice is in the aggregation of the data. Nonetheless, policy makers have not defined the aggregation as the focus of the problem, and the solutions proposed do not affect this stage.

This article will argue two main points. First, in order to reduce the privacy repercussion created by online profiling it is necessary to directly regulate the aggregation and commercialization of the data. Second, the data collected and aggregated represent important benefits to all stakeholders, for this reason there are no incentives to regulate online profiling in order to reduce its real threat to privacy.

This paper will have four sections. Section I will expose the stakeholders involved, and the benefits of the practice. Section II will explain each of the five

---

[2] For the purpose of this paper, online platforms refer to computer browsers, smartphones, tablets, or any device used to connect to the internet.

stages of online profiling, the problems that arise in each of them and the solution proposed to regulate those problem. Section III will argue that to really protect the online platforms users' from privacy threats it is necessary to redefine what is the problem of online profiling. Section IV will analyze if the government, the industry and the users have any incentive to regulate the online profiling practice.

I. ONLINE PROFILING: HOW IT WORKS

By monitoring online behaviour over time, companies collect enough information about an individual (or a specific device) to create a unique digital profile. The creation of comprehensive personal profiles is the main justification of online profiling. In this process, some actors gather the data, others aggregate it, and finally someone buys it mainly for marketing. As Deibert argues: "companies of all shapes and sizes systematically pick through our digital droppings, collating them, passing them around, inspecting them, and feeding them back to us. And this market shows no sign of slowing."[3] This section will analyze who are the main stakeholders and what are the benefits of online profiling.

In the online environment, there are different technologies that enable a communication between the users' devices and tracking companies. Due to this communication first- and third-party companies can follow the user within and between online platforms and/or different physical locations. Depending on the technology used, the company is able to gather different types of information about a user or device.[4] This information might be associated to a specific device or to the identity of an individual. The data that each of the technologies gathers alone may not represent a big threat to privacy, however the information from several of these technologies creates the possibility of producing a very comprehensive profile.

Different organizations participate in the tracking, collection, aggregation and use of the users' information. Based on the interaction with the users, it is possible to divide them in two categories: first and third party.[5] The first-party organizations interact directly with users, because they own the apps and service that the user accesses (e.g. retail and content sites, search engines, third-party payment services, social networks, and weather apps). They have a contractual

---

[3] Ronald J Deibert, *Black Code. Surveillance, Privacy, and the Dark Side of the Internet*, Trade paperback ed. (Toronto, Ontario: McClelland & Steward, 2013) at 56.

[4] See e.g. Officer of the Privacy Commissioner of Canada, "Report on the 2010 Office of the Privacy Commissioner of Canada's Consultation on Online Tracking, Profiling and Targeting, and Cloud Computing", (May 2011), online: < www.priv.gc.ca/media/1961/report_201105_e.pdf > at 12.

[5] See e.g. Tracy A. Steindel, "Path toward User Control of Online Profiling" (2011) 17:2 Mich Telecomm & Tech L Rev 459 at 465.

relation with the user based on the Terms of Use and the Privacy Policy of the company.[6]

On the other hand, the third-party organizations lack a consumer interface, however they have access to the users' online data. Some of these companies track the users; others aggregate, analyze, sell, or buy the users' data (e.g. agency trading desks, data suppliers, ad networks, banks, governments, law enforcement, and lawyers).[7]

Online profiling has benefits for users and companies.[8] For example, targeting advertising supports "free" (or low monetary cost) access to online services and content.[9] In addition, the tracking and the information collected help to improve the commercial relation between users and companies. For instance, it improves the user experience by making the experience more personalized by showing relevant search results based on the web history of the user, and displaying advertising based on frequently visited sites and geo-location;[10] improves the quality of the services of the company and helps with developing new products; [11] secures and protects the users' personal accounts, by letting the company know if someone different from the account owner tries to access the account.[12]

Furthermore, it has marketing benefits for the companies as it enables companies to classify the individuals into groups based on specific characteristics. This classification is useful because it allows audience targeting which facilitates specific and more efficient marketing actions. [13]

---

6 The Privacy Policy stipulates how the company will manage the information they collect from the user. For example, what information they collect and why they collect it, how they use that information, and how to access and update the personal information. See for example Google, "Google Privacy Policy", (20 December 2013), *Google Policies & Principles*, online: < www.google.ca/intl/en/policies/privacy/ > .

7 See e.g. Julia Angwin, "The Web's New Gold Mine: Your Secrets", *Wall Street Journal* (30 July 2010), online: < www.wsj.com/news/articles/SB10001424052748703940904575395073512989404 > .

8 Recent events as the Snowden revelations show that it might have some benefits for the government as well.

9 See e.g. Grand Gross, "Survey: Internet users like targeted ads, free content", *Computerworld* (19 April 2013), online: < www.computerworld.com/s/article/9238549/Survey_Internet_users_like_targeted_ads_free_content?pageNumber = 1 > .

10 See for example Google, "Ads You'll Finda Most Useful", online: < www.google.com/intl/en/policies/privacy/example/ads-youll-find-most-useful.html > .

11 See e.g. Google, "Develop New Ones", online: < www.google.com/intl/en/policies/privacy/example/develop-new-ones.html > .

12 See for example "Cookies, Pixels & Similar Technologies", online: < www.facebook.-com/help/cookies/?ref = sitefooter > ; See also Google, "Protect Google and Our Users", online: < www.google.com/intl/en/policies/privacy/example/protect-google-and-our-users.html > .

13 See e.g. Daniel J Solove, "Privacy and Power: Computer Databases and Metaphors for Information Privacy" (2001) 53:6 Stan L Rev 1393 at 1405.

II. STAGES, PROBLEMS, AND PROPOSED SOLUTIONS

As shown in *Graphic 1* at the beginning of this paper, the online profiling process is divided in five stages. This section will briefly explain each of the stages. Then it will highlight some of the problems that arise in each of them. Finally, it will expose some of the solutions proposed by policy makers in order to mitigate the threat to privacy.[14] Specifically, this section will focus on three concerns: the knowledge and consent of the user, the type of information collected, and the security measures to store and share the data. The aim of this section is to give a general panorama; it does not aim to give an extensive report about current problems and proposed solutions.

(a) Installation of the Technology

In this stage, companies install one or several of the available tracking technologies in the user's device.[15] The moment when this occurs varies; it can be as soon as the person opens a website, when the app is installed or when the device is fabricated (e.g. cookies, web beacons, and GPS).

Other technologies such as IP address, Unique Device Identifier, or browsing fingerprinting do not need previous installation. In these cases, the architecture of the online platform or the device allows the tracking of the user without installing an extra technology on the device.[16] For example, every time a computer is connected to a website its IP address is retrieved.[17] In this stage, the two main problems regarding privacy are: the user does not about the existence, installation, and use of the technologies; and the lack and/or the validity of the consent given by the user regarding the installation of those technologies.

Three of the main proposed solutions are: (1) companies must inform the users about the installation and use of technologies and ask for their consent; (2) companies must give the user an option to opt-out; and (3) the creation of a Do Not Track mechanism. The main problem of those solutions is that even if companies are transparent and inform the user about the use of the technologies and the collection of the data, the user will never have the knowledge and tools necessary to make an informed decision.[18]

---

[14] This includes mainly policy makers from United States, Canada, and the European Union. The paper will not focus on any specific proposal as the different jurisdictions have approach the problem with the same or similar solutions.

[15] Device includes web browsers, computer hard drives, smartphones, tablets, etc.

[16] Here architecture is use Lessig's definition: "The software and hardware that make cyberspace what it is constitute a set of constraints on how you can behave. . .. They constrain some behavior by making other behavior possible or impossible. The code embeds certain values or makes certain values impossible." Lawrence Lessig, *Code 2.0* (New York, United States of America: Basic Books) at 124–125.

[17] See e.g. Mozilla, "Privacy on the Internet", online: <www.mozilla.org/projects/security/pki/psm/help_21/privacy_help.html>.

[18] Moreover, when the companies are transparent they only inform the user about a small part of the technologies: cookies, web beacons, and GPS.

Due to the aggregation of the data that companies do, the user will not be able to foresee what the data collected by that particular company would truly reveal. The data collected often has other uses besides the initial uses described by the Privacy Policy. This data might have secondary uses by first-party organization, or by third-party organizations (or individuals). [19] Even if some of the potential uses are explain to the user, not all are foreseeable by the user when he is giving his consent. In other words, when the user is giving his consent, he cannot really valorize what he is giving away or what he is authorizing. [20]

(b) Tracking

In this stage, companies follow the user's online activities and keep a record of that data. As previously explained, the data that companies can collect include: what did the user see, for how long, her search queries, information provided to the website, and her geo-location, among others. In this stage, the main concerns are: the places where these technologies can follow the users, and that the type of information collected constitutes personally identifiable information (PII).[21]

Technologies can follow the user through different online sites and physical places. Regarding online sites, the user is followed within each website he or she visits, and through different website he or she browses. Apropos the physical places, with the invention of GPS technology, and its installation in personal devices such as mobile phones, automobiles, and cameras, it became easier to collect data regarding the actual geo-location of the user.[22]

The main solution regarding the type of information collected has been to limit the collection of data only to non-PII.[23] The first problem of this solution is the definition of what is personal information. The question about what information to protect against a privacy invasion does not have a unique answer.[24] Therefore, achieving a consensus about this category is the first challenge.

---

[19] In addition, only first party organizations can inform and ask for the user's consent. Third party organizations do not have a direct interaction with the user, then how are they going to inform the user and ask for his consent?

[20] See e.g. Solove, *supra* note 13 at 1452.

[21] With the concept of PII it is also included the concepts "sensitive information" and "personal information".

[22] Other technologies that help determine the geolocation of the user are Base Station Data and WIFI. See Article 29 Data Protection Working Party, *Opinion 13/2011 on Geolocation Services on Smart Mobile Devices*, 811/11/EN WP 185 (2011).

[23] See e.g. Paul M Schwartz & Daniel J Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86 NYUL Rev 1814 at 1816:

> PII is one of the most central concepts in privacy regulation. It defines the scope and boundaries of a large range of privacy statutes and regulations . . . These laws all share the same basic assumption-that in the absence of PII, there is no privacy harm. Thus, privacy regulation focuses on the collection, use, and disclosure of PII, and leaves non-PII unregulated.

[24] For example there is not one clear definition of what personal information is. According

The second problem, and the main reason why this solution is not enough to protect privacy, is that technology has made it possible to combine data to reveal more information. In other words, "[t]he line between PII and non-PII is not fixed, but depends upon technology."[25] Several studies have shown how information that is classified as non-PII in combination with more data allows the identification and disclosure of non-public information of the data subject. For example, the combination of ZIP, birth date, and sex can uniquely identify 87% of the U.S. population;[26] an analysis of the movie viewing history and movie ratings of a person, can reveal non-public sensitive information such as religion, sexual preferences and political views;[27] and the possibility to predict the Social Security Number of a person base on his birth date and birth location.[28]

(c) Collection in Databases

In this stage, the companies collect the data gathered during the tracking in private databases. These databases contain individual files about the users of the online platforms. Those individual files might be associated to a specific device, or to the identity of a person (user name or real name). Current technology makes it possible and inexpensive to store vast amounts of data for an indefinite period. This is problematic from a privacy perspective because it creates the possibility to have more comprehensive and unforgettable personal profiles. With this in mind, the main concerns of this stage are the time the data is stored and the access to the database records.

To reduce the privacy threat of the information collected, it has been established that the data must be de-identified before it is stored and shared.[29] Thus, companies use different anonymization techniques to protect the privacy of the users.[30] This is not an accurate solution to privacy because, due to

---

to Schwartz & Solove, there are three different approaches: "tautological", "non-public", and "specific-types". See *Ibid* at 1828.

[25] *Supra* note 23 at 1846.

[26] See Latanya Sweeney, "Policy and Law: Identifiability of De-identified Data", *Research Accomplishements of Latanya Sweeney,* online: <www.latanyasweeney.org/work/identifiability.html>.

[27] See A. Narayanan & V. Shmatikov, *Robust De-anonymization of Large Sparse Datasets* (2008), online: <www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf>

[28] See Alessandro Acquisti, Ralph Gross & Stephen E. Fienberg, "Predicting Social Security Numbers from Public Data" 106:27 Proceedings of the National Academy of Sciences of the United States of America 10975 (2009), online: <www.pnas.org/content/106/27/10975.full.pdf>

[29] See e.g. US, Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers* (2012) at 22, online: <www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers>

[30] "Anonymization is a process by which information in a database is manipulated to make it difficult to identify data subjects." Paul Ohm, "Broken Promises of Privacy:

technological advances and the proliferation of personal information stored in online and offline databases, the re-identification process is possible and easy to perform.[31]

(d) Aggregation of the Data: Creation of a Comprehensive Profile

In this stage, companies exchange the data collected in their private database with other companies in order to aggregate and transform it into a comprehensive profile. For instance, if company A has a dataset regarding the shopping preferences of the IP 12.345.678.90 and company B has a dataset of the movie preferences associate to that same IP, in this stage those datasets are aggregated to create a more comprehensive profile of the IP 12.345.678.90.[32]

The datasets are exchanged by two processes: shared between subsidiaries of the same company, or traded for money in different data marketplaces.[33] The problems that arise from this stage are the commercialization of the data and the creation of comprehensive profiles. Until now, none of these problems has been part of the regulatory discussion around online profiling.

The commercialization of the data is a problem because it leads to the devaluation of the privacy into companies' assets. If privacy is transformed into companies' assets, and that transformation is accepted, this will affect how the courts will interpret and protect privacy in the future. This is also a problem about the values that society and courts should preserve and protect, or in the words of Lessig, this is a question of "how should changes in technology be accommodated to preserve values from an earlier context in a new context?"[34]

Look at the following example: two strangers (X and Y) follow one person around the city every day. X follows the individual in the zone around his work and Y in the zone around his home. Both X and Y take notes, pictures and videos of the individual's activities, then they sell those records to a third person — C. This situation is stalking and constitutes an invasion of privacy. It is problematic not only because the person is being followed, but also because X and Y are keeping a record of his activities (personal life), and making a profit from that invasion to privacy. As this situation takes place in the real world, society will likely oppose this action and courts will protect the individual's privacy from this type of action.

Responding to the Surprising Failure of Anonymization" (2010) 57 UCLA L Rev 1703 at 1707.

31 See e.g. Schwartz & Solove, *supra* note 23 at 1846. See also Ohm, *ibid* at 1705.

32 See Dan Wallach, "The Technological Landscape of Comprehensive Data Collection" (2012) The Big Picture Comprehensive Online Data Collection Transcript 15 at 33, online: <www.ftc.gov/sites/default/files/documents/public_events/The%20Big%20-Picture%3A%20Comprehensive%20Online%20Data%20Collection/bigpicture_transcript_21206ftc.pdf>

33 See for example: BlueKai, "BlueKai Intro Video", online: <http://bluekai.com/video/>. See also Angwin, *supra* note 7.

34 Lessig, *supra* note 16 at 191.

Online profiling practice is not different from the previous example. It is then necessary to think what consequences does the acceptance of the commercialization of data collected online by private companies have in the concept of privacy in the physical world, and in the social (and legal) values around privacy.

The other problem that arises in this stage is the creation of comprehensive profiles. This represents an invasion to privacy because online platform users lose the control over their personal information.[35] Assuming that the consent given by the user to a company is valid, in this stage the information that the user agreed to share with one company, is shared with others companies. This means that one company not only gathers the information that the user wanted to "share", but much more.

In addition, the creation of comprehensive profiles is a constant threat to privacy because the profiles contain enough information to individualize a person; to know daily patterns about that person, and to make predictions about that person. As Solove states, "[t]he data collected [by corporations] extends beyond information about consumer's view of the product to information about the consumer herself, often including lifestyle details and even a full-scale psychological profile."[36]

Therefore, it is a constant threat because those profiles are stored and available to anyone who can gain access to it (whether authorized or unauthorized). This is problematic because not only could anyone access those files and learn almost everything about a person, but also because the potential uses that those profiles could have.

(e) Use of the Data: Profile Application

In this stage, different organizations use the comprehensive profiles for different purposes, such as online advertising; target marketing; background checking; law enforcement investigation; price targeting; personalized promotions; statistical purposes, and in predictive profiling systems. The comprehensive profiles contain enough information and characteristics to make inferences about a person (or device), for example, she likes movies, understands French, reads newspapers from Middle East countries, buys coffee at Starbucks, and lives in Toronto.

The division of the profiles by group is a useful tool for organizations in order to deliver marketing campaigns that are more precise. It is worth highlighting that the content that the user accesses online is selected by the company that provides it, as this content is chosen depending on the preferences of the user, and the user will only see what the company thinks is more

---

[35] In this regard Steindel affirms, "online profiling is a harmful practice precisely because it is contrary to traditional concepts of privacy and user expectations, which both reflect the belief that privacy includes some measure of control over personal information." Steindel, *supra* note 5 at 468.

[36] Solove, *supra* note 13 at 1404.

appropriate for his profile. Consequently, the classification by group limits the options of the user .[37]

Another possible set of groups are people with homosexual preferences; people with Islam interests; people with interest in arms and bombs, and pregnant women. This set of groups might also be useful for marketing purposes. Nevertheless, depending on the purpose that the organization wants to achieve, it can also be used for discriminatory practices based on sexual preferences and religious beliefs, in unfair treatment due to pregnancy, or to profile possible terrorists.[38]

The problems that arise from this stage are the classification of people in specific groups, and the uses of the profiles. As with the aggregation stage, policy makers have not discussed these problems as the discussion has mainly focused on the targeting advertising industry. The online profiling problem has been defined as if the information gathered is only used by this industry.

Nevertheless, scholars have examined the problems of online profiling beyond the advertising industry. Some of them have made some propositions to limit the potential uses that the comprehensive profiles might have. For example, Solove proposed to establish "meaningful limits on how data can be used — limits that are clear rather that ambiguous and amorphous."[39]

The main problem of this solution is that today's technology makes it possible, and easy, to access the databases where the profiles are stored by different actors (internal and external to the companies).[40] Even if there is a regulation that prohibits certain uses, it will not persuade actors like hackers. Therefore, it will not prevent the access and unauthorized use of the profiles. Moreover, this type of regulation probably will not apply to government agencies that have their own regulation, such as the NSA that, as it will be discuss later, also have interests in these profiles.

---

[37] See Steindel, *supra* note 5 at 469.

[38] For example See Ian Kerr, "Prediction, Preemption, Presumption: The Path of Law after the Computational Turn" in *Privacy, Due Process and the Computational Turn: The Philosophy of Law Meets the Philosophy of Technology* (New York: Routledge, 2013) at 8. See also Ronald Leenes, "Do They Know Me? Deconstructing Identifiability" (2007) 4:1&2 UOLTJ 135 at 158.

[39] Solove, *supra* note 13 at 1461.

[40] Examples of those breaches include the breach to the smartphone app Snapchat on January 1, 2014, where the hacker accessed the list of usernames and phone numbers, and the breach to Boxee.tv forum accounts on April 2, 2014, where the information accessed by the hackers included email addresses, birth dates, IP addresses, message histories, and password changes. See Privacy Rights Clearinghouse, "Chronology of Data Breaches", online: < www.privacyrights.org/data-breach/new > . See also Dino Grandoni, "4.6 Million Snapchat Accounts Leaked After Startup Brushed Off Security Concern", *The Huffington Post* (1 January 2014), online: < www.huffingtonpost.com/2014/01/01/snapchat-leak_n_4528573.html > .

III. RETHINKING THE PROBLEM

This paper has exposed that the online profiling practice creates a constant threat to the privacy of online platform users. Even if the user gives his consent for the collection of the information, the commercialization of the data, the aggregation process and the security vulnerabilities of the databases where all the data is stored, poses a threat to the privacy of the person. All of these justify the need for a regulatory intervention of the online profiling practice.

This section will argue that the way the problem has been defined by policy makers is not accurate to protect the privacy of the users. Therefore, it is necessary to redefine the problem in order to design regulations that effectively reduce the privacy concerns of online profiling.

The objective of the current approach is to reduce the threat to privacy created by online profiling by regulating the first three stages of the process. For instance, inform the user about tracking technologies and the collection of information; ask for consent; limit the type of information that is gathered, and guarantee that the data collected is not associated to an indefinable person.

This approach has proven to be ideal to ensure the delivering of the benefits described at the beginning of this paper to all stakeholders, including technological commodities to users. Nevertheless, for the reasons developed in the previous section, these regulations do not reduce the constant threat to privacy that online profiling creates.

Re-identification methods, proliferation of personal information online and offline, and the possibility of identifying people from non-PII data, are examples of technological factors that policy makers must take into consideration in the design of regulations. In addition, it is also important that they take into account the main objective of online profiling; this is the creation of comprehensive personal profiles. [41]

According to Ohm, "the utility and privacy of data are linked, and so long as data is useful, even in the slightest, then it is also potentially re-identifiable . . . [a]s the utility of data increases even a little, the privacy plummets."[42] Thus, as the data collected in the process of online profiling must be useful as to create comprehensive profiles, the data collected will always be a threat to privacy. Consequently, regulating online profiling by concentrating in the type of the data collected, will never lead to the abolition of the creation of comprehensive profiles.

Taking into account the technological factors and the online profiling justification, no matter how the first three stages are regulated, the result is going to be the same: the aggregation process will be performed, the comprehensives profiles will be created, and they will be available for someone to use. In other words, the threat to privacy will persist.

---

[41] See e.g. Solove, *supra* note 13 at 1407: "[t]he effectiveness and profitability of targeted marketing depends upon data, and the challenge is to obtain as much of it as possible."

[42] Ohm, *supra* note 30 at 1751.

As explained in the previous section, a regulation limiting the uses of the profiles is not an efficient solution to reduce the threat to privacy. A more accurate approach is to understand that the constant threat to privacy exists due to (1) the aggregation and commercialization of the data, (2) the creation of comprehensive profiles, (3) the storage of those profiles in databases, and (4) the application of those profiles. Therefore, the new regulatory proposals should center in the aggregation stage and the storage of the information.

However, if the goal is to eliminate the threat to privacy created by online profiling, regulating some of the stages of the practice will not be enough. As long as companies keep tracking and aggregating the data, the threat to privacy will persist. Therefore, there should be more efforts to find alternative business methods to achieve a real balance between privacy, innovation and economical growth. In order words, to eliminate the negative implications, it is necessary to rethink the industry and business model of online profiling in order to find new alternatives.

Lessig argues that four constraints act as regulators: law, social norms, market, and architecture.[43] Lessig's proposals are an example that there are ways to regulate online profiling besides regulations. Nevertheless, it is necessary that the relevant stakeholders have incentives in order to find alternative methods or effective regulations to address the problems raised by online profiling and implement them.

IV. ARE THERE INCENTIVES TO REGULATE?

The four constraints exposed by Lessig also indicates that the government is not the only actor who can regulate an issue; the private sector and the users also have the power to regulate. Therefore, in order to regulate online profiling, it is necessary for the intervention of the industry and, more importantly, of the users. An additional question to ask is whether those actors have incentives to intervene and regulate this practice. This section will analyze what are the incentives, if any, that these groups may have to regulate the online profiling practice to change or affect the creation of databases with comprehensive profiles.

(a) Government

The existence of the databases created by the online profiling practice by private sector companies is a gold mine for law enforcement and intelligence agents. Under national security, crime prevention or crime investigation, governments from around the globe want to have access to those databases, and they have found the way in.[44] Governments use data mining techniques to

---

[43] See Lessig, *supra* note 16, c. 7.

[44] Deibert argues, "[a]s more and more data is entrusted by users to third parties like Google, governments are side-stepping transparent and accountable judicial processes to police that data." See Deibert, *supra* note 3 at 115.

extract intelligence from vast stores of digital information.[45] The existence of the databases created through the online profiling process benefits these techniques. As Rubinstein explains, data mining "can be viewed as a 'back end' use of personal data that is already collected and resident in public and private sector databases."[46]

Furthermore, the recent Snowden revelations is proof of the interest that government agencies have to gather information of people (online platforms users) and that the databases created by companies through online profiling are the perfect source to find that personal information, e.g. NSA Prism program that tapped into user data of Apple, Google, and others.[47]

As those databases are of great utility for crime investigations, crime prevention and national security, governments do not have incentives to regulate. On the contrary, governments have incentives not to regulate and to maintain and preserve the practice of online profiling as it is today. The creations of the databases are a benefit for them.

(b) Industry

The personal information of online platform users is a big business. In this business, online profiling is one of the practices used by private companies to collect the information. This process involves the participation of many companies.[48] The collection of users' information began as a method to facilitate and improve commerce by improving the effectiveness of targeted marketing. This business method helped to shape the actual architecture of the market. Being so, the industry has the power and tools to regulate the practice; invent new technologies; change the architecture of the technologies used in order to make those technologies less invasive to privacy, or define a new business method that does not depend on the collection of data and the creation of comprehensive profiles.

Nevertheless, various industries benefit from the existence of this business model based on online profiling practices, and these industries are growing every day.[49] Besides the benefits exposed at the beginning of this document, online profiling represents a huge economical benefit for these companies.[50]

---

[45] See Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches" (2008) 75:01 U Chicago L R 261.

[46] *Ibid* at 280.

[47] Varton Gellman & Ashkan Soltani, "NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say", online: *The Washington Post* < www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html >.

[48] See e.g Solove, *supra* note 13 at 1407.

[49] For example, in 2010 a newspaper article report, "Tracking activity is exploding. Researchers at AT&T Labs and Worcester Polytechnic Institute last fall found tracking

Due to the fact that a great number of companies are involved in the online profiling process and all of them benefit from it, industry also does not have the incentives to regulate or change the actual practice of online profiling.

(c) Users

Online profiling jeopardizes the privacy of the users. Consequently, users have a huge incentive to regulate this practice. Based on the regulators proposed by Lessig, users could use privacy tools to make tracking harder, e.g. Ghostery; use tools that improve privacy and security over the internet to make the data collected less accurate, e.g. TOR; or change some browser habits to reduce the amount of personal information available online, e.g. private information posted in social networks.

Nevertheless, two facts demonstrate that for the majority of the users, privacy is not enough incentive to do something regarding online profiling. The first fact is that online profiling has been a public practice for a long time. For instance, in 1999, The New York Times published an article talking about the tracking of consumers, the collection of personal data, and the sharing of that data between companies. [51] This newspaper article is a good example of two things.

First, The New York Times article demonstrates that online profiling is not a practice developed in the dark. One thing is the companies' lack of transparency with the user at the moment of the "contractual" agreement; another is the fact that the practice has been public for a long time, and the majority of the users have not changed their behaviour online.

Second, the article also argues that consumers "are willing to part with personal information as long as they get something in return."[52] The companies gather personal information and give something in return, e.g. free content, promotions, and technological commodities). This statement remains true nowadays, and helps explain why users have not done anything.

The second fact is the Snowden revelations. As noted previously, these revelations demonstrated that, by accessing the databases of private companies, government gathered tons of personal information about people. Nevertheless,

---

technology on 80% of 1,000 popular sites, up from 40% of those sites in 2005.": see Angwin, *supra* note 7.

[50] MarketingCharts staff, "B2B Media and Info Industry Revenues Up 3.4% in 2012", (24 May 2013), online: <www.marketingcharts.com/wp/traditional/b2b-media-and-info-industry-revenues-up-3-4-in-2012-29788/>. See also MarketingCharts staff, "Online Ad Revenues Up 18% Y-O-Y in H1; Mobile's Share Doubles to 15%", (10 October 2013), online: <www.marketingcharts.com/wp/online/online-ad-revenues-up-18-y-o-y-in-h1-mobiles-share-doubles-to-15-37306/>. See also Deibert, *supra* note 3 at 57.

[51] Katie Hafner, "Do You Know Who's Watching You? Do You Care?, *The New York Times* (11 November 1999), online: <www.nytimes.com/1999/11/11/technology/do-you-know-who-s-watching-you-do-you-care.html>.

[52] *Ibid.*

people do not seem to make the connection of the privacy threat between government agencies, spying citizens, and private companies gathering and storing files of personal information about their users.

All the previous information demonstrates that it might be some kind of technological somnambulism around online profiling.[53] Companies improve technologies to give the user more innovation, and users accept that innovation without really questioning (or understanding) what are the true consequences of these new technologies. Then, even when privacy is a big incentive to regulate online profiling, for now it seems to be not big enough for the users to do something about it.

V. CONCLUSIONS

We are being stalked around the web, and our data collected has become a profit asset for private companies and a gold mine for everyone who needs or wants to get personal information about us. This paper has argued that in order to reduce the privacy repercussion created by online profiling, it is necessary to regulate the aggregation and commercialization of the all the data collected by private companies using tracking technologies.

Second, based on the benefits that private companies and government gain from the aggregation of the data, these stakeholders do not have any incentives to regulate. The other relevant stakeholder are the users, taking into account that online profiling threats the privacy that affects directly the life of users, this group should have enough incentives to regulate online profiling. However, there has not been any significant regulation coming from this group after at least 15 years of the existence of the practice.

The absence of regulation can be for two reasons. First, users enjoy the benefits they receive in exchange of their information so much that they are willing to give up their privacy. Second, users do not understand the implications or the magnitude of what they are giving away. The most probable is the second reason, then the only thing needed is a big event that helps users connect the dots, for example between events such as the Snowden revelation and the authorization they give to companies to track them through online platforms.

Finally, today we are allowing first and third parties to track our "online habits" but as technology evolves information gatherers will be able to track other information more closely related to our personal life. For this reason, the ideal objective is to eliminate the threat to privacy created by online profiling. To achieve this goal, regulating some of the stages of the practice will not be enough. It is necessary to replace the actual business models by practices that do not

---

[53] See Langdon Winner, *The Whale and the Reactor: A Search for Limits in an Age of High Technology* (The University of Chicago Press, 1989) at 10: "A more revealing notion, in my view, is that of technological somnambulism. For the interesting puzzle in our times is that we so willingly sleepwalk through the process of reconstituting the conditions of human existence".

require or depend on the gathering, aggregating and storing of personal data. If it is not possible to find any alternatives, then as a society we must ask if the economical profit gained by some private companies and the technological innovation that online profiling practice promises to achieve are more valuable than our privacy.