OHCHR: The Right to Privacy in the Digital Age

Written submission by The Human Rights, Big Data and Technology Project
University of Essex

Introduction

1. This submission is made by the Human Rights, Big Data and Technology Project ('HRBDT'),[1] based at the University of Essex's Human Rights Centre. Funded by the Economic and Social Research Council, HRBDT analyses the challenges and opportunities of big data and associated technologies from a human rights perspective. Drawing on expertise from interdisciplinary researchers and partner organisations, it researches whether fundamental human rights concepts and approaches need adaptation to meet rapidly evolving technological landscapes and assesses existing regulatory responses and their suitability for effective human rights protection.

2. HRBDT welcomes the opportunity to participate in the Office of the United Nations High Commissioner for Human Rights (OHCHR)'s consultation on 'human rights challenges relating to the right to privacy in the digital age' in preparation for the report of the High Commissioner on the right to privacy in the digital age.[2]

3. Despite the far-reaching impact of big data and new technologies on human rights, public debate and policy discussions regularly fail to recognise the full implications for all human rights. The protections offered by the existing and well-established international human rights law (IHRL) framework are also often overlooked or claimed inadequate in pursuit of 'new' solutions. The forthcoming report is therefore timely in affirming the relevance of IHRL to addressing the risks posed to human rights and underscoring the responsibilities on states and businesses to meet their obligations in this area. In HRBDT's view, the challenge is not whether new frameworks are required, but rather how to ensure effective implementation of the existing framework to ensure that human rights, including privacy, are promoted and protected in the digital age.

4. For reasons of space, this submission focuses on: the seriousness of the violation of the right to privacy, both in and of itself, and in the exercise and enjoyment of other rights; and on challenges in the implementation of obligations to establish procedural safeguards, effective oversight and remedies for state and businesses' practices in the digital age (item 7 in the consultation).

[1] The Human Rights, Big Data and Technology Project, available at <http://www.hrbdt.ac.uk>.
[2] A/HRC/RES/34/7, 7 April 2017, OP 10.

A. THE NATURE OF HARM

5. Since OHCHR's 2014 ground-breaking report on the right to privacy in the digital age, the risks to human rights posed by big data and new technologies, including artificial intelligence, have become even clearer. However, in public discourse, the risks to privacy are often minimised by narratives such as having 'nothing to hide' and an underplaying of the seriousness and full implications of unlawful or arbitrary interferences with the right to privacy.

6. Big data and new technologies enable a much more intricate picture of a person's life, interactions, thoughts, and preferences than even a search of a person's home.[3] This interference not only affects privacy but can impact on the exercise and enjoyment of all other rights.[4] Interference with the right to privacy can also have a disproportionate impact on marginalised individuals and/or groups in positions of vulnerability, thus widening inequality and exacerbating discrimination. For example, social networks and other digital platforms have created new spaces for lesbian, gay, bisexual, transgender and intersex (LGBTI) persons to interact, organise, and shape discourse. However, the use of their personal information by states and business enterprises may not only interfere with their right to privacy but can result in targeting by state and non-state actors, detention and threats to their lives.[5]

7. Where the right to privacy is breached, the effect is difficult to undo and may result in ongoing consequences and further human rights implications. The ease of retaining, sharing, repurposing, and fusing data and profiles influences the permanence of digital data, meaning an individual may face new and ongoing risks to their rights into the future.

8. OHCHR's forthcoming report can play a central role in reframing understandings of the nature of the harm posed by interferences with the right to privacy in policy debates and public discourse. This would include a restatement that the right to privacy is essential not only in and of itself, due to the serious

[3] In *Riley v. California*, 573 U.S. _ (2014) the U.S. Supreme Court affirmed that 'cell phone search… would typically expose far more than most exhaustive search of house…'.
[4] Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression, A/HRC/35/22, 30 March 2017, para 78; *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, ECtHR, No. 39315/06, 22 November 2012, para 88.
[5] See for e.g. Access Now, 'In Egypt, expressing your sexuality online makes you a target for human rights abuse. That has to stop.', 9 November 2017, available at <https://www.accessnow.org/egypt-expressing-sexuality-online-makes-target-human-rights-abuse-stop/>; ILGA-Europe, Annual Review of the Human Rights Situation of Lesbian, Gay, Bisexual, Trans and Intersex People, May 2017.

implications of a breach, but also as a gatekeeper to the full exercise and enjoyment of all other human rights.[6]

B. IMPLEMENTATION OF PROCEDURAL SAFEGUARDS, EFFECTIVE OVERSIGHT AND REMEDIES

9. Within HRBDT's research, including empirical research and engagement with those at the cutting edge of regulatory and oversight practices, a recurring theme is that national frameworks either do not exist or fail to adequately reflect the requirements of IHRL on safeguards, oversight and remedies in the digital age.

10. While OHCHR's 2014 report set out the relevant IHRL on procedural safeguards, oversight and remedies,[7] HRBDT is of the view that greater articulation of these standards in the forthcoming report would strengthen national implementation efforts. Within this submission, we highlight key areas on safeguards, oversight and remedies, that would benefit from detailed treatment by OHCHR, as they reflect shortcomings in some national contexts.

(1) Overarching Framework of Procedural Safeguards and Effective Oversight

11. No legislation exists regulating surveillance practices or providing for procedural safeguards and effective oversight in many states.[8] In others, oversight practices may not meet IHRL standards and/or may not be comprehensive. Ineffective regulation and/or oversight may arise in at least three ways.

12. First, frameworks may not fully cover businesses and states' collection, fusion and matching, retention and erasure, repurposing, access to and sharing of data (in the private sphere and also open-sourced data); data management and information security; automated decision-making; and activities such as profiling and analysis of individuals and groups.

13. Second, frameworks may not comprehensively cover the different interactions and sharing of information between businesses; between business and state; and from state to state.

14. Third, oversight frameworks may only focus on one moment in time, for example, the point of data collection, rather than requiring new authorisation and

[6] Report of the Office of the United Nations High Commissioner for Human Rights, The right to privacy in the digital age, A/HRC/27/37, 30 June 2014, para 13; A/HRC/RES/34/7, PP 13.
[7] A/HRC/27/37, paras 37 – 41.
[8] A/HRC/27/37, para 50.

oversight at each point at which the data is shared either within a state (i.e. between departments of government) or with other entities.

15. These limitations reflect a significant implementation gap in the requirements of IHRL and the need for reiteration that IHRL requires procedural safeguards and effective oversight of states and businesses in all contexts. These measures should be built in from the start and not applied retrospectively after collection.

(2) Appropriate legal and oversight frameworks for state surveillance activities

16. In addressing the current implementation gap, a detailed articulation of IHRL requirements would be instructive in order to provide guidance to states regarding the establishment of oversight bodies or the IHRL-compliance of existing oversight processes. This section highlights key aspects of IHRL that merit re-articulation in relation to state surveillance practices.

17. Where oversight bodies exist at the national level, they assume different forms.[9] These include parliamentary oversight committees, independent judicial or quasi-judicial bodies, and dedicated courts. For example, respectively, the PKGr/Parlamentarisches Kontrollgremium (Parliamentary Control Panel) (Germany), the Investigatory Powers Commissioner's Office (IPCO) (UK) and Foreign Intelligence Surveillance (FISA) court (US).

18. Each model has distinct advantages and disadvantages. For example, given their focus on warrant approvals, FISA courts in the USA have been criticised for having limited oversight powers. UK and German judicial oversight bodies have attracted criticism over limited separation of approval and oversight processes. While a diversity of models may be appropriate – and will inevitably depend upon particular domestic legal settings[10] – it is essential that they comply with the core requirements of IHRL.

19. In this respect, states must promulgate a legal basis regulating all surveillance-related activities.[11] This legislation must be consistent with IHRL and establish the grounds on which interference with rights would be lawful. This must cover state requests to businesses (such as Internet intermediaries) as there is a danger that state agencies may make informal 'requests', in lieu of adopting more formal, independently authorised procedures. It must also cover situations in which

[9] For an overview of the situation in the European Union, see EU Fundamental Rights Agency, 'Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU, Volume II: field perspectives and legal updates', October 2017.
[10] *ibid*, p. 63.
[11] See, for example, *Szabo and Vissy v. Hungary*, Judgment, ECtHR, Application No. 37138/14, 12 January 2016, para. 54.

states seek to access information held extraterritorially or share information with other states.

20. States must also demonstrate that an interference pursues a legitimate aim and is necessary or strictly necessary in a democratic society.[12] This raises key questions in relation to the type of offences or activities for which surveillance powers may be deployed, whether these powers may be deployed in a large-scale (bulk) or targeted manner,[13] and how retention periods and access to data are governed.

21. Independent authorisation and oversight is essential.[14] An oversight body should (1) be empowered to independently approve or reject decisions of the executive regarding surveillance warrants, (2) be authorised to proactively investigate and monitor the activities of those who conduct surveillance and who have access to the product of surveillance, (3) conduct periodic reviews of surveillance capabilities and technological developments, and (4) be equipped with appropriate and adequate expertise, competencies, and resources.[15] These processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight body must be subject to appeal or independent review.

22. Oversight frameworks should span each point of the process for surveillance and communications interception or other forms of processing of personal data. Oversight frameworks may integrate a combination of administrative, judicial and/or parliamentary oversight.[16] Exposing oversight bodies to divergent points of view is particularly important in the absence of an adversarial process: it is essential that 'points of friction' – continual challenge to approaches and understandings – be built in. Adopting a multi-stakeholder approach is appropriate in this regard.

---

[12] The precise threshold depends on the nature of the powers in question. See, for instance, *Szabo and Vissy v. Hungary*, para 73; *Tele2 Sverige AB v Post-och telestyrelsen* and *Secretary of State for the Home Department v. Watson and others*, Judgment, Grand Chamber, CJEU, Cases C-203/15, C-698/15, 21 December 2016, paras 109, 110.

[13] i.e. what is the degree of intrusion beyond those connected to a suspected act or offence.

[14] See, *Zakharov v. Russia*, Judgment, ECtHR, Application No. 47173/06, 4 December 2015, para 233.

[15] Report of the Special Rapporteur on the right to privacy, A/HRC/34/60, 24 February 2017, para 37; Report of the Special Rapporteur on the right to privacy, A/HRC/31/64, 24 November 2016, para 48; Council of Europe, Convention for the protection of individuals with regard to automatic processing of personal data, CETS No. 108, 28 January 1981; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC; Privacy International, Guide to International Law and Surveillance, August 2017.

[16] Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, A/HRC/14/46, 17 May 2010, paras 13-15; A/HRC/31/64, para 50.

23. These elements are critical because they (1) embed objectivity and prevent conflicts of interest, (2) provide the oversight body with opportunities to monitor operational activities comprehensively and gain fuller understanding of operational practices, which is important for identifying where and how controls may be strengthened, and (3) enable the oversight body to carry out its mandate effectively and efficiently. Technical expertise and capacity to evaluate and investigate practices is critical to effective regulation of surveillance and communications interception and other forms of processing personal data.

24. Beyond their core mandate of evaluating operational practices, oversight bodies should also engage in public information about the existing laws, policies and practices in surveillance and communications interception and other forms of processing of personal data.

25. Many challenges highlighted above can be addressed by ensuring oversight bodies are compliant with IHRL requirements. Although certain difficulties do arise – particularly in relation to national security concerns – IHRL has established guidance in this regard, and lessons may be drawn from existing practice, including in related contexts where appropriate.

(3) Procedural safeguards and effective oversight of business enterprises

26. Beyond the surveillance practices of states, the centrality of businesses in the collection, fusion, retention and sharing of data and the profiling of individual users of their products and services also has serious implications for the effective exercise and enjoyment of human rights and therefore also requires procedural safeguards and effective oversight. This is an area which has received relatively little attention, to date, beyond changes required in regions such as Europe due to the General Data Protection Regulation (GDPR). While welcome, the GDPR does not address the full extent of human rights concerns associated with data collection and use. This also extends beyond existing approaches towards regulation and self-regulation to generate mechanisms to ensure IHRL compliance.

27. The UN Guiding Principles on Business and Human Rights set out obligations on states and businesses in relation to the role of businesses on human rights. Aside from states' obligations in relation to private actors, the Principles also requires that businesses themselves respect human rights, which includes preventing or mitigating adverse human rights impact and providing a means of access to justice where human rights violations are alleged and remedies where they are

found to be breached. [17] The state duty to protect against business-related human rights abuses includes an oversight role. Failures to assess and implement the Principles and ensure that an effective oversight process is in place reflects a further implementation gap.

(4) Remedies

28. In relation to both state surveillance and business activities, very little attention has been paid to the obligation on states and business enterprises to provide effective access to justice and to the nature and forms of remedies required, where a violation(s) of IHRL is found.[18] It is therefore critical for remedies to feature centrally in policies and practices in the digital age, and on the agenda of states and business enterprises.[19]

29. Given that the effects of surveillance and communications interception or other forms of processing of personal data are not necessarily restricted to territorial borders, the right to a remedy applies irrespective of borders.[20]

30. Realising the right to a remedy is distinct from technical rectification of system-level faults. It encompasses three key elements – prevention, redress, and deterrence, and is not limited to retrospective measures after a violation might have occurred.[21]

31. In the context of surveillance and communications interception or other forms of processing of personal data, there are distinct challenges that potentially impede securing of effective remedies.

32. First, an individual or group can only bring a claim when on notice of a potential rights' violation. Unlike in other areas, an individual or group may be unaware that their privacy and/or other human rights have been interfered with, for example, through data-sharing or where states can access the information held by

[17] Report of The Special Representative of The Secretary-General on The Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, A/HRC/17/31, 21 March 2011, principle 13, 25.
[18] A/HRC/35/22, para 74; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/32/38, 11 May 2016, para 68; Amnesty International and the Business & Human Rights Resource Centre, Creating a paradigm shift: Legal solutions to improve access to remedy for corporate human rights abuse, 4 September 2017.
[19] A/HRC/35/22, para 73.
[20] A/HRC/34/60, para 34.
[21] Guiding Principles on Business and Human Rights; Report of the Working Group on the issue of human rights and transnational corporations and other business enterprises, A/72/162, 18 July 2017, paras 38, 40, 57.

businesses and other states directly. Where government data requests come with non-disclosure agreements or 'gag' orders, the entity (typically a business) providing the data is legally prohibited from notifying the individual(s) whose data is affected. This heightens the restriction on the individual's access to remedy, as they may not have the opportunity to challenge the data request particularly if they do not receive notice in advance and cannot challenge such requests.[22] Further, businesses and states may use and share data and technologies to build profiles of individuals or make inferences and predictions about them. However, as the recent Facebook/Cambridge Analytica incident demonstrates, an individual may be unaware of these practices until revealed. This challenge underscores the critical role played by an appropriate legal framework, transparency, oversight and notification as a condition precedent to the exercise of the right of access to an effective remedy. It also underscores the importance of embedding notification into oversight mechanisms and the relationship between oversight mechanisms and access to justice.

33. Second, the widespread use of algorithms to support decision-making raises critical issues for the exercise of an effective remedy. Where algorithms are used in decision-making, the right to an effective remedy may be compromised where individuals are not able to access the input data, challenge the findings reached by the algorithm or challenge how the findings of the algorithm were used in the eventual decision reached.[23] Transparency, explainability and understandability are key issues in this regard.

Professor Lorna McGregor
Professor Pete Fussey
Dr Daragh Murray
Vivian Ng
HRBDT
Human Rights Centre
University of Essex

[22] Electronic Frontier Foundation, Who Has Your Back? 2017: Seventh Annual Report on Online Service Providers' Privacy and Transparency Practices Regarding Government Access to User Data, July 2017.

[23] This submission draws on research produced in a draft paper, Lorna McGregor, Daragh Murray & Vivian Ng on algorithmic accountability.