Response to the call for inputs for a report on "the right to privacy in the digital age" by United Nations Office of the High Commissioner for Human Rights

IT for Change
April 2018

1. Introduction: Why the right to privacy assumes a new dimension in digital times

Technology was once thought to aid surveillance, but now surveillance is seen as an essential and coveted by-product of technology. The appetite for data through which pervasive surveillance takes place is the driving force of the digital society today. Governments have traditionally used data collected through statistical systems to inform policies. However, with the digital revolution, data acquires the status of knowledge upon which policy is predicated. Further, with Big Data methodologies, causation is exchanged for correlation, and we see algorithms increasingly replacing human mediation and decision-making. As digital technologies are written into our daily lives, they have allowed those who control the technology (state and corporation) and the data collected, to observe individuals microscopically.[1]

Privacy is no longer about protecting one in the sanctity of one's home from outside interference, or limited to conventional relationships of confidentiality, such as with a doctor or a bank. The fact that we leave digital traces in our public and private transactions has meant the need for privacy to be extended to all such transactions that have a digital footprint. Cross-pollination across digital databases, public as well as private, allows for the enmeshing of myriad fixed and variable markers of individuals to give unprecedented insight into an individual's life and social relationships,[2] as well as the practices of communities. For instance, the Indraprastha Institute of Information Technology, Delhi, developed OCEAN,[3] a 'people search engine', which works by cross-linking various publicly available government databases and social media information to demonstrate the amount of private data that is publicly available and easily recoverable.[4] Data may not only be collected from individuals without their knowledge, but individual data revealed in a particular context may also be taken out of and deployed without consent in completely new contexts.

1 David Watts and Vanessa Teague, Big Data and Open Data - Appendix 4 http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx
2 Helen Nissenbaum, Protecting Privacy in an Information Age: The Problem of Privacy in Public, https://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf
3 OCEAN Open-source Collation of eGovernment data And Networks http://precog.iiitd.edu.in/research/ocean/search/
4 Srishti Gupta, Mayank Gupta and Ponnurangam Kumaraguru, OCEAN: Open source Collation of eGovernment data and Networks, http://precog.iiitd.edu.in/research/ocean/OCEAN.pdf

2. Implications of algorithmic sorting and grouping on privacy

Merely obfuscating direct identifiers like the name or address does not make individuals unidentifiable[5]. For instance, from an IP address or search query, it does not take much to pinpoint the individual. Digital corporations who undertake online advertising, which is usually one-to-one or targeted, work on this logic. They not only narrow down on an individual; they are also able draw up profiles of them from data sourced and collected on their own.[6]

Considering the current state of affairs, it has been argued that de-anonymisation is but a feel-good bromide. Moreover, what is considered to be anonymous is also deeply flawed. Companies claim to have de-identified data sets by wiping out direct identifiers, but replace them with other unique or sufficiently unique identifiers.[7]

State-created unique identifiers such as the biometric based identification – *Aadhaar* – in India, for example, have greatly enhanced cross-linking of databases, without the need for direct identifiers. In fact, these identifiers are more distinct and accurate than names or addresses in finding the needle in the haystack, so to speak. Because welfare entitlements have been made contingent upon the production of *Aadhaar*, enrollment for it is high.[8] This has also attracted private sector co-option, with the production of *Aadhaar* becoming a pre-requisite even to avail private sector services[9], whether banking, Internet services or enrollment in schools, hospitals or for jobs.

Even without a single unique identifier to marry databases, states and corporations collect such copious amounts of data that some data reference points are bound to recur across databases, so that even if you are not identifiable, your identity will be known and a reasonably unique individual profile will be built. These identity points, which were previously hidden or revealed only through certain relationships, allow for seemingly disparate individuals to be grouped together.[10] Gillespie refers to the algorithmic sorting and grouping of individuals, often without any disclosure of why they are being grouped in a particular way, as ‘calculated publics’. This process he cautions may make subtle or not so subtle correlations that entrench biases. Android Market, for example, suggested downloading a ‘sex offender location app’ to anyone who downloaded the dating app

5 Paul M. Shwatz and Daniel J. Solove, The PII Problem: Privacy and a New Concept of Personally Identifiable Information, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1909366

6 Ibid

7 Solon Barocas and Helen Nissenbaum , Big Data's End Run around Anonymity and Consent http://wpressutexas.net/cs378h/images/b/b3/LaneEtAlPrivacyBigDataAndThePublicGood.pdf

8 Anumeha Yadav and Menaka Rao,The government wants pregnant women to enroll in Aadhaar to get their social scheme benefits, The Scroll, March 2017, https://scroll.in/pulse/831175/the-government-wants-pregnant-women-to-enroll-in-aadhaar-to-get-their-social-scheme-benefits, Aadhaar covers over 89% population: Alphons, The Times of India, March 2018, https://timesofindia.indiatimes.com/business/india-business/aadhaar-covers-over-89-population-alphons/articleshow/63202223.cms

9 M Rajshekhar, How private companies are using Aadhaar to try to deliver better services (but there's a catch), The Scroll, December 2016, https://scroll.in/article/823274/how-private-companies-are-using-aadhaar-to-deliver-better-services-but-theres-a-catch

10 Solon Barocas and Helen Nissenbaum , Big Data's End Run around Anonymity and Consent http://wpressutexas.net/cs378h/images/b/b3/LaneEtAlPrivacyBigDataAndThePublicGood.pdf

Grindr meant for gay men, making the underhanded connection 'between homosexuality and predatory behavior'.[11]

Uncovering identities can also regurgitate biases that were thought to have been weeded out by socio-legal reform. Redlining and reverse red-lining can be easily carried out by Fin-tech companies based on racial identity. This information may not be gathered by them directly (which may well be illegal), but by picking it up and piecing it together from other data sources like information shared on social media, friends on contact bases, location of residence, where one shops at etc.[12] Allocating group identifiers without investigating the social impact of such an action can have adverse effects on the group. The *Bhoomi* project by the state of Karnataka that created a central repository of land records by digitising them is an excellent case study of actionising identity adversely. *Bhoomi* identified parcels of degraded land and dry-land that were occupied for decades by poor *dalit* farmers and small farmers, who however did not own these lands. Because these records were digitised and centralised, it proved to be a convenient way for vested interests to locate and oust vulnerable farmers from their land. [13]

For harm to occur, the revealed identity need not even be actually operationalised for particular purposes. The LGBTQ community felt a deep sense of betrayal when BuzzFeed broke the news that Grindr disclosed the HIV status of its users to two other companies.[14] Not only is the potential for misuse in this case immense, the outing of something that is so deeply personal and socially stigmatised also instills a sense of fear in the community. Much like how hate speech based on social identity like gender can chill the participation of that group in society.[15]

Evidently, the protection of privacy must address the social exclusion, discrimination, exploitation and harm caused through algorithmic segmentations that create 'calculated publics' or reinforce and perpetuate preexisting social marginalisation of certain groups.

3. The 'social value' of privacy

Philosophical and legal discussions about privacy have traditionally centered around the individual. The right to be let alone was justified as an individualistic right to protect one from the prying eyes of the other. From this starting point, the individual is deemed to be vested with sufficient rights to negotiate with the state and private entities as to how data that emanates from her will be governed. However, given the hegemony of digital corporations and the huge information asymmetry, it would be flawed to adopt a legal

11 Tarleton Gillespie, The Relevance of Algorithms, http://www.tarletongillespie.org/essays/Gillespie%20-%20The%20Relevance%20of%20Algorithms.pdf

12 Knowledge@wharton, The Surprising Ways that Social Media Can Be Used for Credit Scoring, http://knowledge.wharton.upenn.edu/article/using-social-media-for-credit-scoring/

13 Solomon Benjamin, R Bhuvaneswari, P. Rajan and Manjunatha. Bhoomi: 'E-Governance' , Or, An Anti-Politics Machine Necessary to Globalize Bangalore? https://casumm.files.wordpress.com/2008/09/bhoomi-e-governance.pdf

14 Azeen Ghorayshi and Sri Ray, Grindr Is Letting Other Companies See User HIV Status And Location Data, BuzzFeed News, April 2018, https://www.buzzfeed.com/azeenghorayshi/grindr-hiv-status-privacy?utm_term=.kv22Kmxmmd#.ffygb0D00R

15 Kylie Weston- Scheuber, Gender and the prohibition of hate speech, https://lr.law.qut.edu.au/article/download/504/494/

approach that attributes power and knowledge to the individual for negotiating an informed deal on privacy.[16] Individuals are constantly asked to trade their privacy for other benefits like security, entitlement and efficiency. In the tussle between an individual's right to privacy and the variable 'greater good' as touted by the state and the corporation, the social value of privacy is forgotten.

Priscilla M. Regan recognises three dimensions to a social value of privacy[17]:

Firstly, privacy has a 'common value'. That is, an individual's interest in privacy is to some extent shared by other individuals in a community/society. The essence of this concept is reflected in laws that use the term 'reasonable expectation of privacy'. For instance, in India, the law on voyeurism uses this term in reference to 'private areas' of the body, and to being video-graphed at certain venues like changing rooms.[18] A common value or agreement about privateness has thus been developed in relation to parts of the body referred as well as locations where one may be surreptitiously filmed.

Secondly, Regan posits, privacy has a public value which fortifies democratic political systems. This is a means to an end argument, where privacy is seen as facilitating other rights, like free speech and expression, and checking the powers of the state and the corporation, essential to a robust democracy. Hannah Arendt, takes this one step further, and places an inherent value on privacy for democracy. She argues that the private sphere helps citizens develop affinities through common understandings and shared values, which in turn upholds the public sphere. Because unabated state surveillance can result in chilling free speech, profiling and exiting of marginalised communities from the public sphere, the public value of privacy is a strong counter to arbitrary state surveillance that corrodes the public sphere. The Supreme Court in Canada, for instance, recognised in relation to warrantless surveillance that the question was not only whether criminals should be subject to such surveillance, but also whether society should be subjected to it.[19]

Finally, privacy has a 'collective value'. Under this conception, privacy is thought to exhibit the characteristics of 'collective good', which are indivisibility and non-excludability, and thus is an unsuitable market good[20]. In the networked world, wherein social media architectures have normalised an 'access for data' regime, by default, data becomes a market good. This dominant rule erodes the collective value of privacy, transferring the regulation of privacy to the individual.

4. Recognition of group interests and the right to freedom from harm

Regan's submission on the social value of privacy goes back to 1995. Her exhortation that a democratically debated right in this regard be developed needs to be re-imagined for the

16 Paul M. Schwartz, Internet Privacy and the State, https://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1765&context=facpubs
17 Priscilla M. Regan, Legislating Privacy : Technology, Social Values, and Public Policy, https://books.google.co.in/books/about/Legislating_Privacy.html?id=zFDBqMbAOIgC&redir_esc=y
18 See Section 66A of the information Technology Act and Section 254C of the Indian Penal Code
19 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1031964
20 Priscilla M. Regan, Legislating Privacy : Technology, Social Values, and Public Policy, https://books.google.co.in/books/about/Legislating_Privacy.html?id=zFDBqMbAOIgC&redir_esc=y

digital age not only with respect to individual freedoms, but also the rights of collectives or groups. While legislative frameworks like the EU GDPR have sought to protect and promote the right to privacy using an expanded definition that accounts not only for 'identified', but also personally 'identifiable', information, researchers have argued that it still falls short of what is necessary for the Big Data age.As discussed, a group may be discriminated against based on the knowledge of a single piece of information like race, which may be acted upon without any knowledge of the specific identity of the individuals who make up the group.[21]

The Committee of Experts, constituted to draw up a data protection framework for India, observed that, "new technologies pose considerable challenges" as to what is or is not personally identifiable information", suggesting that, "this standard may have to be backed up by codes of practice and guidance notes indicating the boundaries of personal information having regard to the state of technology."[22] Graham Greenleaf opines that a 'code of practice' may not be sufficient and suggests expanding the ambit of data protection law to any information that can affect the interests of individuals based on their personal characteristics.[23] This focus on interests rather than identity provides a sound conceptual modeling for the recognition of the right to privacy.

Another conceptual inroad could be harm based data protection frameworks. Harm based frameworks are based on un-divestable rights in data. While consent may have its place, it may be rendered an inadequate condition when data collection and processing or allied activities can potentially infringe upon the rights of the individual or the group. These include the right against discrimination, right to data security, right against the disclosure of sensitive data etc, which must be seen as inalienable.[24] The South Korean data protection law's modus for collective redress - 'Data Protection Collective Suit' in case of violation of a group's privacy[25] - may be useful to look at, in this regard.

5. Need for an international instrument on private use of data

David Watts who has authored a thematic report on Big Data and Open Data for the Special Rapporteur on Privacy has noted that "An innovative information economy would probably achieve greater community support if there was observable adherence by governments and corporations to strong regulation around the acquisition, sharing and control of people's data."[26] As the Special Rapporteur notes,

---

21 Ibid
22 White paper of the committee of experts on data protection framework for india, http://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf
23 Graham Greenleaf, Data Protection: A Necessary Part of India's Fundamental Inalienable Right of Privacy – Submission on the White Paper of the Committee of Experts on a Data Protection Framework for India, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102810
24 Rahul Matthan, Beyond consent: A new paradigm for data protection, http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf
25 Graham Greenleaf, Asian Data Privacy Laws: Trade and Human Rights Perspectives, https://books.google.co.in/books?id=3yfSBAAAQBAJ&printsec=frontcover#v=onepage&q&f=false
26 David Watts and Vanessa Teague, Big Data and Open Data - Annex 4 http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

over a third of the member-states of the UN have no legislations recognising the right to privacy.[27] Although it looks like countries like India are inching towards a comprehensive data protection policy, for now, it seems like citizens are stuck with arrangements that are no better than private contracts which may not even be governed by domestic laws.[28] Importantly, the Special Rapporteur also drafted a legal instrument which is to act as a blueprint for an international understanding (binding or non-binding) on Government-led surveillance and privacy.[29] It is important to bear in mind that private entities have also invested heavily in trailing users. The Cambridge Analytica episode[30] epitomises what is now christened 'surveillance capitalism'- that is, the no-holds-barred data extraction, analysis, experimentation and customisation that digital corporations routinely engage in 'for the purposes of knowing, controlling, and modifying behavior to produce new varieties of commodification, monetisation, and control'[31]

We hope that the Office of the High Commissioner for Human Rights will also develop the blueprint of an international instrument on private use of data. As argued above, acknowledging the social value of privacy as overarching, and safeguarding group privacy in such an instrument is as important as the recognition of individual privacy.

Scholars engaging with the idea of a community's right to data[32] caution us against putting all the eggs in the privacy basket. They have proposed models wherein the state (national to the municipal level) acts in trusteeship of all citizen data, owned in common by citizens, by allowing private access to this data only under certain conditions, which could include monetary compensation. In certain cases, such as for research by non-commercial entities or for public interest, these conditions could be relaxed. We may then need to think of models which 'combine data protection with a proactive economic and democratic agenda that will seek to ensure that citizens do not lose control over the precious resource (data).'[33]

27 Paper presented at Expert workshop on the right to privacy in the digital age Annex, http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

28 Prashant Reddy T., Cambridge Analytica and Facebook – Is Anybody Actually Liable Under Indian Law?, April 2018, https://thewire.in/law/cambridge-analytica-facebook-liability-indian-law

29 Draft Legal Instrument on Government-led Surveillance and Privacy Including the Explanatory Memorandum- Annex 7, http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx

30 Patrick Greenfield, The Cambridge Analytica files: the story so far, The Guardian, March 2018, https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far

31 Shoshana Zuboff, Big other: surveillance capitalism and the prospects of an information civilization, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754

32 Parminder Jeet Singh, The non-politics of outrage, The Hindu, March 2018, http://www.thehindu.com/todays-paper/tp-opinion/the-non-politics-of-outrage/article23359148.ece

33 Evgeny Morozov, After the Facebook scandal it's time to base the digital economy on public v private ownership of data, The Guardian, April 2018, https://www.theguardian.com/technology/2018/mar/31/big-data-lie-exposed-simply-blaming-facebook-wont-fix-reclaim-private-information