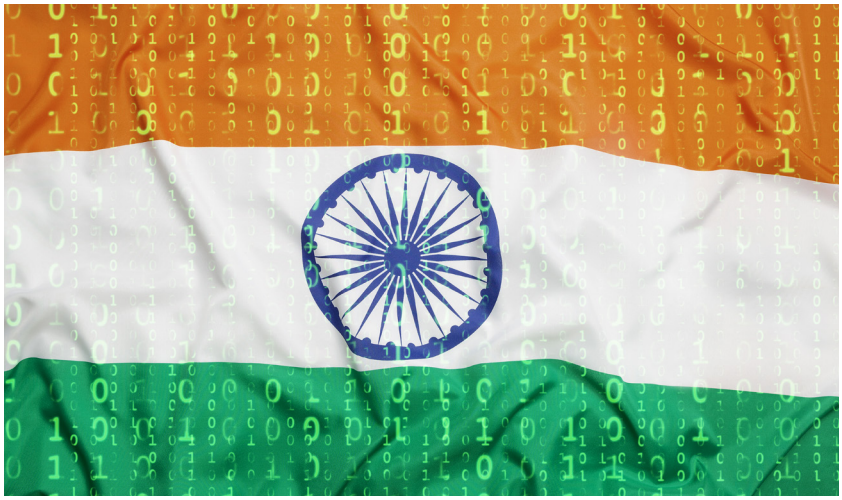
Notes de l'Ifri
Asie.Visions 96

Working with "Last Mile" Data Protection in India



Arun SUKUMAR

November 2017

ifri Center for Asian Studies

The Institut français des relations internationales (Ifri) is a research center and a forum for debate on major international political and economic issues. Headed by Thierry de Montbrial since its founding in 1979, Ifri is a non-governmental, non-profit organization.

As an independent think tank, Ifri sets its own research agenda, publishing its findings regularly for a global audience. Taking an interdisciplinary approach, Ifri brings together political and economic decision-makers, researchers and internationally renowned experts to animate its debate and research activities.

ISBN: 978-2-36567-792-9

How to quote this document:

Arun Sukumar, "Working with 'Last Mile' Data Protection in India", *Asie.Visions*, No. 96, Ifri, November 2017.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tel.: +33 (0)1 40 61 60 00 – Fax: +33 (0)1 40 61 60 60

Email: accueil@ifri.org

Website: Ifri.org

Author

Arun Mohan Sukumar heads the Observer Research Foundation's Cyber Initiative and is the Co-Chair of CyFy: The India Conference on Technology, Security and Society (on sabbatical). He is a PhD candidate at The Fletcher School of Law and Diplomacy, Tufts University. He was until recently the elected Vice Chair of the Asia-Pacific Regional Internet Governance Forum (2015-17). Arun has served as an independent legal expert to the United Nations General Assembly's First Committee on disarmament and international security and the 2016-17 UN Group of Governmental Experts, the forum tasked with conceiving cyber norms. He was also the non-governmental representative in India's official delegation to the 2016 Tallinn Manual consultations to articulate laws of armed conflict in cyberspace. He is a member of the National Security Council Secretariat's study group created to recommend a policy for India on negotiating and developing cyber norms. Arun is a member of the World Economic Forum's Global Future Council on the Digital Economy and Society. He is a lawyer by training.

Executive Summary

India's digital economy is characterized by "last mile" data protection, with privacy norms and data collection/ sharing standards being set at the level of the application ("app"), operating system (OS) and the device. This practice lends itself to multiple, often crisscrossing rules maintained by smartphone manufacturers, mobile operating system vendors and application developers. The user is caught in a maze of privacy policies that bear on important questions: what data is collected, where it is stored, who it is shared with, and legal recourse in the face of policy violations or unauthorized use of data by third parties.

Contributing to the confusion is the lack of statutory or regulatory clarity on data protection. India's own data protection rules offer wide latitude to technology companies to determine their own practices, which encourage irregular and poorly enforced privacy policies. If regulatory ambiguity has opened the door for conflicting data protection guidelines, the problem is compounded by India's heavy reliance on foreign devices and applications, many of which transfer data of Indian users outside India's borders and base their privacy policies on their home jurisdictions. This system of "last mile" data protection significantly diminishes the state's ability to protect the privacy of its citizens, a right that was recently confirmed as "inalienable" by the Supreme Court of India.

This paper highlights "last mile" protection through an analysis of policies at the app, OS and device layer — using the examples of the Google Play Developer Distribution Agreement, Google Developer Policy, the India-specific privacy policies of smartphone manufacturers Huawei, Vivo and Xiaomi, as well as the privacy policy of WhatsApp. While acknowledging that such policies are here to stay and that it may not be feasible to craft statutory guidelines that comprehensively address every dimension of data sharing and collection, given the diversity in technological platforms, the paper makes the case for a self-regulating, autonomous and multi-stakeholder agency for protecting the integrity of user data.

Table of Contents

Introduction

In August 2017, the Supreme Court of India delivered a far-reaching verdict on the "right to privacy" of the country's citizens.[1] The Court's unanimous conclusion — that there indeed existed a "fundamental", inalienable right to privacy, ring-fencing the individual's freedom to be "left alone"[2] — radically transforms how digital platforms collect and share data in India. The case and its hearing by the Supreme Court bear closely on the legality of the massive, nationwide biometric identity program ("Aadhaar")[3] launched by the government of India in 2009. Assailed by its critics as a vehicle for government surveillance and hailed by its proponents as an effective delivery mechanism for public and private services, the Aadhaar project is the fulcrum around which India's privacy laws could evolve in the future.[4] But Aadhaar is only one — albeit significant — among many data-collection platforms in India. Privacy in digital spaces is joined at the hip with the general ability of mobile devices and applications to protect data from unlawful or unwarranted access by third parties, making the enjoyment of such a right contingent on the state's ability to ensure compliance with data protection norms. More so, given that Indians today access the internet through their mobile phones more than any other electronic device.[5]

Concurrently, the Indian Supreme Court has been hearing arguments on the validity of WhatsApp's privacy policy, and in particular, its sharing of user data with its parent company, Facebook.[6] During this hearing, the Indian government declared that it would "come out with regulations on data protection", as the data of users is "connected to their personality",

1. "Is Privacy a Fundamental Right? Supreme Court Refers Matter to 9-Judge Bench", *Hindustan Times*, July 19, 2017, www.hindustantimes.com [Last accessed August 1, 2017].
2. Justice K.S. Puttuswamy & Anr v. Union of India & Ors W.P (Civil) No. 494 of 2012, https://indiankanoon.org.
3. "Aadhaar" refers to the Unique Identification (UID) numbers provided to Indian citizens enrolled in the program: these 12-digit numbers are matched usually with their fingerprints and iris scans. The database and program is managed by the Unique Identification Authority of India, which was established in 2009 and vested with statutory status and powers in 2016.
4. "Why Privacy Clause in Aadhaar Law If It's Not Fundamental Right: SC Grills UIDAI", *Hindustan Times*, July 28, 2017, www.hindustantimes.com [Last accessed August 1, 2017].
5. "India amongst World Leaders in Use of Mobile to Surf the Internet – StatCounter", BusinessWire, March 28, 2017, www.businesswire.com [Last accessed August 12, 2017].
6. "WhatsApp Privacy: Supreme Court Constitution Bench To Hear On Monday", NDTV.com, May 13, 2017, www.ndtv.com [Last accessed August 1, 2017].

and thus an integral part of their "right to life".[7] The regulatory capacity of the state to protect data will be tested against its ability to prevent and investigate security breaches, and unauthorized use or sharing of personally identifiable information. This capacity is arguably stronger with respect to a government-owned project like Aadhaar, although Aadhaar data breaches may occur during its handling both by public or private agencies.[8] The writ of the Indian state does not, however, run over the lion's share of user data in India that is harvested and stored abroad through private devices and applications.[9]

Indeed, the digital ecosystem in India is marked by a heavy reliance on imported products and services, and with them, on imported standards of data protection. Five of the top-selling smartphone vendors — Samsung, Xiaomi, Vivo, Oppo and Lenovo — are based in China and South Korea, and there is no Indian product among the most popular "apps" (WhatsApp, TrueCaller, ShareIt, MXPlayer or UC Browser, to name a few) used on these devices.[10] Imports are expected to meet 75% of the domestic demand for electronics in India by 2020. Electronic imports even managed to surpass, in 2016-2017, the total imports of gold to the country.[11] In fact, the capture in market share by Chinese smartphone manufacturers have come at the cost of their Indian counterparts, reducing the latter's national presence in just three years from 52% to 14%.[12] Compounding this concern is the "export" of data harvested through these devices and services to jurisdictions outside India. Save for government data[13], and information collected through government services, there exist no data localization requirement in Indian laws, which not only hampers the ability of law enforcement agencies to collect electronic evidence but also weakens the implementation of a data protection regime.[14]

7. "Centre Tells Supreme Court It Will Frame Regulations to Protect User Data", *Scroll*, July 22, 2017, https://scroll.in [Last accessed August 1, 2017].
8. "Aadhaar eKYC Mandatory for Mobile Connections: Here's How It Applies to You", *The Indian Express*, March 27, 2017, http://indianexpress.com [Last accessed August 1, 2017].
9. Vinit Goenka's Blog, "IT Sovereignty in India – The Data Centre Dimension", https://vinitgoenka.wordpress.com [Last accessed August 1, 2017].
10. "Chinese Firms Shipped 51% Smartphones to India in March Quarter: IDC Report", *Livemint*, May 17, 2017, www.livemint.com [Last accessed July 15, 2017]; "10 Most-Popular Android Apps in India", GadgetsNow, June 2, 2017, www.gadgetsnow.com [Last accessed July 15, 2017].
11. "Are Electronic Imports the New Gold for the Indian Economy?", *Livemint*, May 18, 2017, www.livemint.com [Last accessed July 15, 2017].
12. "Mary Meeker's Focus on India: The Key Highlights", *Recode*, May 31, 2017, www.recode.net [Last accessed July 15, 2017].
13. "Government Data on Cloud Must Be Stored in India: Ministry of Electronics and IT", *Economic Times*, April 20, 2017, https://economictimes.indiatimes.com [Last accessed July 15, 2017].
14. ITI Data Localization Snapshot, January 19, 2017, www.itic.org [Last accessed July 20, 2017].

This paper highlights how policies or terms of engagement between a series of actors — the mobile operating system, the device manufacturer, the app, and the user — are creating a complex and somewhat incongruous mesh of legal and technical standards for India's digital economy. These "last mile" policies erode the capacity of the Indian state to protect the data of its citizens, even as it has belatedly begun the pursuit of this goal through judicial pronouncement. To throw these incongruities into relief, this paper looks at five different policies of major technology players who currently operate in the Indian market:

- the Developer Distribution Agreement between Google Play and app developers;
- Google Play Developer Policy and the Core App Standards for Android Devices;
- the Mobile Application Distribution Agreement between Android and device manufacturers;
- the privacy policies of Chinese mobile manufacturers Huawei, Vivo and Xiaomi;
- WhatsApp's Privacy Policy.

Following an assessment of these policies and standards, the paper then compares them to the Indian government's extant guidelines on data protection. It shows that these national guidelines offer considerable autonomy to app developers and mobile software, thus limiting the state's own ability to safeguard the data of its citizens. The paper then makes the case for a self-regulating, autonomous and multi-stakeholder agency for protecting the integrity of user data.

An Incongruous Mesh of Privacy Standards: Five Policies of Major Technology Players Operating in India

This section shows that the complexity of India's digital economy comes from the fact that there are multiple layers of data protection rules set by major technology players. One layer, for instance, is between the operating system and the Apps, another one between the operating system and the mobile manufacturers, and a third one between the mobile manufacturers and the users. This section also looks at the 2016 litigation against WhatsApp to highlight India's weak regulatory capacity to protect data.

Google Play Developer Distribution Agreement

All developers who seek to make their applications available through Google Play — the "app store" for the company's Android operating system — are required to sign a Developer Distribution Agreement (DDA) with the store. The DDA has several provisions for data protection. According to the agreement, Google Play reserves the right to publish and remove applications based on the conduct and "good standing" of the developer.[15] Although there is no accepted or formal definition of such a term — save in the context of corporate or labor laws — in US statutes, or even in Google Play's own policies, there exists a number of "dos and don'ts" that would presumably burnish the credentials of a developer. The DDA states that developers are required to provide "legally adequate privacy notice and protection"[16] for those users from whom their app has collected login or personal information. However, the Agreement also makes it clear that "if the user has opted into a separate agreement with [the developer] to store or use personal or sensitive information directly related to [the app] then

15. Clause 2, Google Play Developer Distribution Agreement, https://play.google.com [Last accessed on August 2, 2017].
16. *Ibid.*, Clause 4.3.

the terms of that separate agreement will govern your use of such information".[17]

The DDA also requires developers not to[18]:

- Create products that "interfere with, disrupt, damage, or access in an unauthorized manner the devices, servers, networks, or other properties or services of any third party".
- Facilitate, through their apps, the "hacking of hardware and software" or the "circumventing of security provisions".
- Embed app elements that "seriously harm" user devices or data.

In most instances of violation, the DDA vests Google Play with discretion to remove or suspend the availability of apps in its store.

Google Developer Policy and Android Core App Standards

The Google Developer Policy — a broader set of guidelines that go beyond Google Play's distribution agreement — also contains similar data protection norms. Apps are required, according to the Policy, to "comprehensively disclose how [the] app collects, uses and shares user data, including the types of parties with whom it's shared."[19] It also requires "affirmative consent" from the user to collect and transmit data that is "unrelated to the functionality" of the app.[20]

The Google Play Developer Distribution Agreement and the Google Developer Policy's legal standards are augmented by technical criteria introduced by Google through its "core app quality" metric for Android. Android app developers are expected to meet a series of requirements to satisfy security and functionality conditions. For instance[21]:

- All private data should be "stored in the app's internal storage".
- All "external data" should be "verified before being accessed".
- Apps should only request "the absolute minimum permissions" required to support core functionality.

17. *Ibid.*
18. *Ibid.*, Clause 4.4
19. "Privacy and Security", Google Developer Policy Centre, https://play.google.com [Last accessed on August 2, 2017].
20. *Ibid.*
21. "Android Developers: Core App Quality", https://developer.android.com [Last accessed on August 2, 2017].

- The app does not seek permission to access "sensitive data" unless required for a "core capability". In other words, unless sensitive data is absolutely critical to the functioning of the app, it should not be collected.
- Application components that "share content with other apps" are required to "define and enforce appropriate permissions".

Android's compatibility requirements also limit the right of developers to use the device's audio and camera functionalities.[22] Developers also have to conform to the set of technical standards known as "app permissions" if they wish to make their apps available on Android. Permissions are classified as "normal", "signature" and "dangerous" based on the type of access they seek.[23]

- Normal permissions allow applications "access to isolated application-level features, with minimal risk to other applications, the system, or the user".
- "Dangerous" permissions, in contrast, offer "access to private user data or control over the device that can negatively impact the user". These may require the affirmative consent before the user.
- "Signature" permissions have to be requested by an app with the same digital certificate as the "app that declared it".

The protection level required for an app to access fingerprint hardware in Android phones for example is "normal".[24] On the other hand, the ability by apps to send SMSes, access user location, answer phone calls and track body metrics like heart rate require "dangerous permissions".[25] Finally, developers also have to ensure that some properties of their apps are out of bounds for third-party applications, such as rebooting an OS, or capturing audio and video. [26]

Taken together, these three agreements/ policies – Google Play DDA, Google Developer Policy and Android Core App Standards – incubate the guidelines and standards that ought to be maintained by app developers on Android platforms. There is no evidence yet to suggest that Google set such

22. *Ibid.*
23. "App Manifest: Android Developers", https://developer.android.com [Last accessed on August 2, 2017].
24. "Normal Permissions: Android Developers", https://developer.android.com [Last accessed on August 2, 2017].
25. "Requesting Permissions: Android Developers", https://developer.android.com [Last accessed on August 2, 2017].
26. "Manifest Permission: Android Developers", https://developer.android.com [Last accessed on August 2, 2017].

standards in consultation with national governments (Android is merely offered as an illustrative example, and other operating systems too follow similar guidelines). This means that, in India, where a staggering 97% of smartphones run Android software, both the state and the user are, at best, passive absorbers of data protection standards set by an industry operator.[27]

Mobile Application Distribution Agreements

If the engagement between the Android/Operating System platform and the app developer creates one layer of data protection rules, the relationship between the OS and the device manufacturer creates another on top of it. For instance, the Google Mobile Application Distribution Agreement (MADA), which governs the use and adoption of Google's apps in Android smartphones, have several stringent requirements for the device manufacturers. Not only does the MADA get into granular details like the design and placement of Google apps on a smartphone screen, but it also requires "Google Phone-top Search [to] be set as the default search provider for all Web search access points on the device".[28]

Analysts have argued that the MADA terms, which are rarely disclosed to the public, create anti-competitive effects in favor of Google.[29] But the real impact of such agreements in 'Android-heavy' jurisdictions like India is the absorption of Google applications' data protection guidelines into popular use. What's more, the "controlling law" in most such agreements are foreign jurisdictions like the states of California or New York[30], which limits not only the policy intervention of the Indian state, but the ability of smartphone manufacturers in emerging markets to contest MADA guidelines.

27. "Google's Android captured 97% Indian Smartphone Market Share in Q2 2016: Report", *The Indian Express*, August 6, 2016, http://indianexpress.com [Last Accessed August 12, 2017].
28. "Mobile Application Distribution Agreement (HTC)", www.benedelman.org [Last Accessed August 12, 2017].
29. B. Edelman, "Secret Ties in Google's "Open" Android", February 13, 2017, www.benedelman.org [Last Accessed August 12, 2017].
30. "Samsung MADA with Google", https://fr.scribd.com [Last Accessed August 12, 2017]; "Mobile Application Distribution Agreement between Motorola Inc and Google Inc.", www.sec.gov [Last Accessed August 12, 2017].

Privacy Policies - Huawei, Vivo and Xiaomi

The privacy policies governing the relationship between the smartphone manufacturers and their users add yet another, often confusing layer of data security guidelines. Take the example of three smartphone manufacturers based in China, whose products are popular in India: Huawei, Vivo and Xiaomi.

Huawei's End User Software Licensing Agreement makes it clear that, "all data collected from [the] device may be [transferred] to Huawei and its affiliate/licensors" in foreign jurisdictions.[31] This would include data collected from third party software components used by Huawei under an open software license. The Agreement acknowledges that such jurisdictions may not even have data protection laws. It only states Huawei will ensure a "similar and adequate" level of protection [for data stored abroad] as required by applicable laws and regulations.[32] Huawei's privacy policy for India specifically acknowledges that it receives "third party" data, or in other words, those of smartphone apps.[33] Finally, it declares that Huawei "has no control over the privacy and data protection policies of Third Parties, which are not governed by [the] Policy."[34] In other words, Huawei's End-User License Agreement, which outlines the general terms between users and software on Huawei products, suggests that it will be governed by the laws of the People's Republic of China. [35]

The smartphone manufacturer Vivo on the other hand states that it "will never allow any authorized third party to use [personal information] for any other purpose other than this Privacy Policy".[36] The term "authorized third party" has not been defined in Vivo's smartphone privacy policy, which also declares elsewhere that the "use of the products or services from a third party shall be subject to the provisions of [its] privacy policy/terms of use".[37] Like Huawei, Vivo too concedes that "[smartphone] information may be stored or transmitted to servers outside of the country" of the user's residence.[38] The concern that Vivo phones and other Chinese handheld devices may be transmitting data beyond Indian borders to

31. Clause 6.3, Huawei Device End-User Software Licensing Agreement, http://consumer.huawei.com/ [Last Accessed August 1, 2017].
32. *Ibid.*
33. Clause 1.1.c, "Huawei Privacy Policy", http://consumer.huawei.com [Last Accessed August 1, 2017].
34. *Ibid.* at Clause 7.
35. *Supra* n. 28 at Clause 13.
36. Clause 2, "Vivo Privacy Policy", www.vivo.co.in/PrivacyPolicy [Last Accessed August 1, 2017].
37. *Ibid.* at Clause 5.
38. *Ibid.* at Clause 6.

China – a likely but by no means foregone conclusion without clear information to back such a claim – caused the Indian government recently to seek "detailed written responses" from 28 smartphone manufacturers on their security practices.[39]

Xiaomi, another Chinese smartphone manufacturer, has faced controversy in India on account of its similar provisions on data sharing. In 2014, the Indian Air Force issued an advisory to its employees cautioning against the use of Xiaomi's Red 1s phone, as it was "found that the phone was forwarding carrier name, phone number, IMEI (the device identifier) plus numbers from [the] address book and text messages back to Beijing".[40] MIUI, Xiaomi's operating system, was also criticized for allowing the company's smartphones to automatically share data with its servers in China. This setting has now been changed, and a Xiaomi user has to turn this feature "on" to enable data sharing.[41] Despite such controversies, Xiaomi's products have steadily gained market share in India and look poised to grow further over the next decade. [42]

Privacy policy – WhatsApp

WhatsApp, the popular messaging application run by Facebook, has nearly 200 million users in India. WhatsApp provides a list of information that is both "automatically collected" and provided by the user. The platform states that it does not retain messages in the "ordinary course" of service, but may store content to "improve performance and deliver media messages more effectively".[43] The communication channels on WhatsApp are, notably, end-to-end encrypted. WhatsApp's privacy policy also makes it clear that information collected from a user will be shared with third party services — as well as the Facebook "family of companies" — "whose own terms and privacy policies will govern the use" of such app/ product.[44]

39. "India's Crackdown on Chinese Technology Companies Gathering Pace", *Livemint*, August 24, 2017, www.livemint.com [Last Accessed August 27, 2017].
40. "IAF Asks Personnel Not to Use Xiaomi Phones", *The Economic Times*, October 25, 2014, https://economictimes.indiatimes.com [Last Accessed August 1, 2017].
41. "Is Xiaomi Really Spying on the Your Privacy?", *Deccan Chronicle*, October 23, 2014, www.deccanchronicle.com [Last Accessed August 1, 2017].
42. "The Rise and Rise of China's Xiaomi in India", *Forbes*, September 12, 2017, www.forbes.com [Last Accessed September 20, 2017].
43. "Information We Collect: WhatsApp Legal Info", www.whatsapp.com [Last Accessed August 1, 2017].
44. *Ibid.*

WhatsApp's privacy policy has been the subject of litigation in India's appellate courts as it relates to the app's sharing of user data with Facebook. In 2016, a lawsuit filed in the Delhi High Court sought an "opt out" feature in WhatsApp for the user to not share data with Facebook. It also sought the removal of data of all users who have deleted WhatsApp from their devices. In its judgment, the Court acknowledges that "the terms of service of "WhatsApp" are not traceable to any statute or statutory provisions"[45], and as a result it cannot adjudicate or evaluate its privacy policy on the basis of any constitutional right (the August 2017 Supreme Court ruling has now affirmed the constitutional status of the right to privacy, but still left the regulation of data collection by the private sector to the government). Where users do not wish to share their data with Facebook, the Court ruled, they are free to delete WhatsApp.[46] While upholding its privacy policy, the Delhi High Court nevertheless instructed WhatsApp not to share any user data collected before September 25, 2016 — the effective date of operation for its new privacy policy — with Facebook.[47] Perhaps most significantly, the Court also declared, "it is not open to the users" to compel WhatsApp "to continue the same terms of service".[48] In effect, the Delhi High Court concluded that absent regulatory standards in India, there is nothing to prevent WhatsApp from articulating and implementing its own guidelines on data sharing. The Supreme Court's recent verdict on the "right to privacy" arguably tips the scale in the user's favour, but it is unlikely that appellate courts in India will venture to adjudicate without statutory guidance on the collection and sharing of data by technology companies.

45. ¶18, Karmanya Singh Sareen and Anr v. Union of India and Ors, W.P.(C) 7663/2016 & C.M.No.31553/2016, https://indiankanoon.org [Last Accessed August 1, 2017].
46. *Ibid.* at ¶19.
47. *Ibid.* at ¶20.
48. *Ibid.* at ¶16.

India's Weak Regulatory Capacity on Data Protection

As they stand, national guidelines offer considerable autonomy to app developers and mobile software — even allowing them to determine which data can be shared, and what information merits stronger protection than others. As a result, the Indian state's ability to safeguard the data of its citizens proves very limited. Against this background, there is a case for creating a self-regulating, autonomous and multi-stakeholder agency for protecting the integrity of user data. Such body would be able to hold the private sector accountable for its own security protocols, allow for a "race to the top" for best practices, and potentially harmonize contradictory data policies at the device and app layers.

Data protection as seen by Indian Law

The maze of policies described in the previous section sits awkwardly with the regulatory principles found in the IT Act of 2008 and the rules enacted under it. The IT Act, which defines cyber offences broadly, also confers the government with sweeping powers to tackle them. The legislation levies a hefty penalty (to the tune of 800,000 US dollars) for the failure of companies or persons to protect data through "reasonable security practices and procedures".[49] It lists out a number of offences that bear on the issue of app/ platform security, including:

- Tampering with source code;[50]
- Retaining stolen source code knowingly;[51]
- Falsifying digital certificates;[52]
- Impersonation of apps by third parties.[53]

49. Section 43A, Information Technology Act, 2000. [As Amended by Information technology (Amendment) Act 2008], https://cc.tifrh.res.in/ [Last Accessed August 1, 2017].
50. *Ibid*. at S.65.
51. *Ibid*. at S. 66B.
52. *Ibid*. at S.74.
53. *Ibid*. at S.66D.

In 2011, the Indian government crafted rules to define "reasonable security practices" as stipulated in the parent IT legislation.[54] These rules define "cyber incidents" as those violating "applicable security [policies] resulting in unauthorized access, denial of service or disruption, [or] unauthorized use of a computer resource to store and process data".[55] App developers, app hosts and mobile devices are required by these rules to

1. provide clear and "accessible" privacy policies;
2. inform the user on the type of sensitive personal data that is collected by them;
3. inform the user of the reason behind collecting and using such data and;
4. obtain the consent of the user before sharing sensitive personal data.[56]

The term "sensitive personal data" has been illustratively defined, and apps or devices can collect them if it is in "connection" and "necessary" for their functions.[57] As for technical standards, platforms and devices are required to have a "documented information security program" and "security controls commensurate with the information assets being protected".[58] The IS/ISO/IEC 27001 set of standards on IT security is highlighted by the rules as one such technical standard that meets the criterion of "reasonable security practices".[59]

Working with "last mile" data protection

As the above segments indicate, India's cyber security regime lends itself to "last mile" data protection: maintaining the integrity of data assets and sensitive information is mostly the remit of apps, whose privacy policies are deferred to by device manufacturers, mobile software platforms, and even Indian law. Devices and mobile operating systems, in turn, have created an additional layer of data protection standards. This creates a number of regulatory challenges for the Indian state.

First, as the Delhi High Court observed in its 2016 order on WhatsApp's data sharing policy, the privacy policies of myriad apps in the smartphone ecosystem do not have any statutory or regulatory basis. As a

54. The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, www.wipo.int [Last Accessed August 10, 2017].
55. *Ibid.* at Rule 2(c).
56. *Ibid.* at Rules 4,5.
57. *Ibid.* at Rule 3.
58. *Ibid.* at Rule 8.
59. *Ibid.*

result, law enforcement agencies in India have no guidance to ascertain whether data breaches are, indeed, breaches, and what policies or laws stand violated. Many app developers neither have any office in India nor do they retain the data of users for long, making it difficult for law enforcement agencies to investigate cybercrime and to hold apps accountable for possible cases of unauthorized access by third parties. The same problem holds true for India's courts and tribunals.

Second, Indian law offers considerable autonomy to app developers and mobile software platforms in deciding *what* data to protect. The IT Rules referenced above list information that qualifies as "sensitive personal data", but beyond such a classification, it is entirely for app developers or software platforms to collect data that they deem necessary for their services. In the absence of well-accepted guidelines or principles on the treatment of specific data, regulators will be constrained to identify data leaks, responsible use of data by third party apps, and broad trends in the collection of sensitive data by certain sectors.

Third, "last mile" data protection ensures that technical standards substitute for effective laws or policies. The list of "permissions" that a developer ought to comply with in order to make his/her app available on Google Play, for instance, is a clear example of how security standards create default data protection norms. Policy choices determined by mobile software platforms determine the nature and extent of data breaches. Camera software, public WiFi hotspots, QR codes and firmware patches have all been found to be points of vulnerability in smartphones, but differential levels of security accorded to applications that use them complicate the work of law enforcement agencies in identifying breaches.

Fourth, given the maze of privacy policies, the user is often left in the dark on how his/her data will be shared, transferred or put to use by third-party products. For example, the use of an Android application in a Vivo phone could lead to multiple outcomes for the user's data:

1. Data collected by the app may be shared with Google Play and Android, in conformity with Google's privacy policies.
2. User data may be shared with a third-party, say, another app, in line with the latter's terms of uses.
3. The Vivo phone may collect user data from the said app, according to its own privacy policy.

In each scenario, the user may provide his/her consent to access and continue the app's services, but with little knowledge of the protections available to data stored by third parties (especially using cloud services),

the legal regimes that apply to data stored in multiple geographies, or whether products that share or collect his/her data have similar levels of "permissions" that apply for "sensitive" content.

Fifth, the limited capacity of the Indian state to enforce cyber security at the app level often manifests itself in catch-all regulations on surveillance, targeted often at Internet Service Providers (ISP) based in India. The IT Act allows the Indian government to intercept, monitor or decrypt "any information", a power that is strengthened by the low levels of encryption mandated for ISPs in India.[60] Catch-all regulations leave open the possibility of data leakage, given that ISPs have been acknowledged globally to be vulnerable to security breaches.

And *finally*, on account of this regulatory deficit on data protection, Indian industry and government have also been rendered susceptible to external pressures. The United States and Council of Europe, for instance, have sought India's signing of the Budapest Convention on cybercrime[61] to promote better information sharing and cooperation between their law enforcement agencies. On the back of its own ruling on net neutrality, the US Federal Communications Commission (FCC) wrote to India's Telecom Regulatory Authority (TRAI), expressing hope that the FCC's 'open internet' order "will help our friends around the world".[62] Given that net neutrality regulations in India will bear on the bottom lines of many US companies, the FCC and other American stakeholders will be keenly following pronouncements from TRAI and the government of India. A 2010 "adequacy report" for India commissioned by the EU assessed that "Indian law does not provide adequate protection in relation to the use of personal information". The report also suggested that, "it is unlikely that the data subject can enforce the data protection rights" granted by India's Information Technology Act, 2008, since "Indian law is based on the doctrine of privity of contract".[63] In light of the multitude of privacy policies and 'terms and conditions' that implicate the Indian user, his/her smartphone device and the apps he/she uses, this finding is relevant even today. Ahead of the EU General Data Protection Regulation (GDPR) coming into force on May 25, 2018, Indian technology companies — mostly

60. *Supra* n. 44 at S. 69.
61. The Convention on Cybercrime of the Council of Europe, or the Budapest Convention, serves "as a [binding] framework" to develop national legislation to tackle cyber crimes and "for international cooperation between State Parties". See generally, "Budapest Convention and Related Standards" www.coe.int [Last Accessed August 10, 2017].
62. "Net Neutrality: US FCC Chief Writes to Trai Head", GadgetsNow, June 28, 2016, www.gadgetsnow.com [Last Accessed August 10, 2017].
63. "EU Adequacy Assessment of India", Data Security Council of India, January 7, 2012, p.6, www.dsci.in [Last Accessed August 10, 2017].

unencumbered by domestic regulation — have scrambled to ensure compliance with the directive.

Dealing with "last mile" data protection

The objective of this exercise is not to call into question or wholly debunk the idea of "last mile" data protection. Given that the next generation of internet users in India — expected to add 500 million in 4 years to the country's online population — will largely access digital networks through mobile phones, and given the great diversity in their consumption patterns, it may be impossible for the Indian state to craft legislation that addresses all manners of data breaches through smartphones. But the current data regime is marked by crisscrossing privacy standards adopted by apps or mobile software platforms, the consequences of which are unknown to the ordinary user. A notable empirical assessment of the "data sharing practices" of smartphone apps by researchers at the University of Oxford and the Massachusetts Institute of Technology found, for instance, that the "permissions-based" model of data collection does not necessarily improve a user's understanding of privacy.[64] Beyond barebones requirements for user consent and "sensitive personal data", there are few regulatory signposts in privacy policies on data sharing, data localization for highly sensitive content, or cooperation with law enforcement agencies.

Until such guidelines are created, "last mile" data protection may be managed through an autonomous and multi-stakeholder data protection agency that evaluates user complaints and data breaches, as well as recommends security standards for sensitive information and specific sectors that collect data. The US Federal Trade Commission's regulatory action against the hand-held device manufacturer HTC in 2013 may offer useful lessons. The Federal Trade Commission then investigated and found HTC responsible for:[65]

1. Not providing adequate "permission checks" that limit the access of apps to certain features in its phone without the user's consent.
2. Creating an insecure "custom application" that allowed the downloading and installation of apps "outside of the normal" Android installation process, thereby circumventing security checks that Google's mobile software may have provided.

64. M. Van Kleek, I. Liccardi, R. Binns, *et al.*, "Better the Devil You Know: Exposing the Data Sharing Practices of Smartphone Apps", http://people.csail.mit.edu [Last Accessed August 10, 2017].
65. In the Matter of HTC America, Inc, File No.122 3049, www.ftc.gov [Last Accessed August 10, 2017].

3. Failure to secure communication between logging applications that collected user information.

In this case, the Commission instructed HTC to:[66]

1. Designate employee(s) to be "accountable for security" concerns.
2. Conduct a risk assessment of external and internal vectors of unauthorized access to HTC devices.
3. Deploy "reasonable" safeguards to mitigate such risks.
4. Select and retain service providers "capable of providing appropriate security practices".

The case represents an instance where a regulator held a mobile manufacturer to account for not complying with industry-wide security standards, and the safeguards that were introduced by the mobile operating system software. India does not have the equivalent of the Federal Trade Commission, but a multi-stakeholder agency — comprising representatives from industry, government and civil society — could address some data protection concerns listed here. Such an institution could be statutorily empowered to investigate data breaches, prompt security audits of companies and recommend best practices by sector. The agency may be able to develop common understandings of "sensitive data", "security breaches" and "permission checks" that go beyond legislative definitions. It would also help define commonly used terms with quasi-legal implications, such as "good standing" or app "functionality" within the context of the services collecting data. What's more, they would also create a level playing field between the app developers — often with meager resources — and a mobile software host like Android or iOS, which currently have discretionary power to suspend or remove apps in their ecosystem. A multi-stakeholder agency to monitor and safeguard the "last mile" would lay the ground for a bottom-up approach to crafting data protection norms with teeth that can guide and steer the development of privacy policies of app providers.

66. *Ibid.*

Conclusion

This paper is an attempt to highlight the legal and technological reasons behind India's limited agency over its "cyberspace", and to offer a modest proposal to protect the data of Indian citizens collected by private entities. India's weak regulatory capacity owes its origins to poor legislative design. Its existing data protection guidelines do little to strengthen the security of "apps", which are often points of extreme vulnerability in the digital ecosystem.[67] But the ability of the Indian state to enforce a "right to privacy", recently confirmed by the Supreme Court, is further complicated by a system of "last mile" data protection, which leaves the user's fate at the hands of privacy policies of mobile devices, operating software and apps. Even with a constitutional guarantee of "privacy" or a statutory data protection regime in place, their effectiveness could be undermined by the competing privacy standards and policies by smartphone manufacturers, app developers and mobile operating systems.

In other words, the Indian state's ability to protect data held by the private sector is limited by:

1. The absence of a clear law on data protection, causing regulatory uncertainty over what constitutes a security breach or unlawful access by third party apps.
2. The presence of default "rules of the road" set by mobile operating systems like Android and iOS for securing the content on their platforms.
3. The opaque terms of engagement between smartphone manufacturers and mobile-OS platforms, which provide little guidance to the user about his/her rights, and to regulators about the distribution of legal liabilities and technological/security responsibilities.
4. The prevalence of catch-all data interception and monitoring guidelines to telecom network operators that increase the risk of leakage at the Internet Service Providers' level.

67. See generally, "HPE Security Research: Cyber Risk Report 2016", www.thehaguesecuritydelta.com [Last accessed August 1, 2017].

This is not to say the state should determine security standards for the application or device layers as a whole. "Last mile" data protection is here to stay. Given the range of apps available today on a single mobile device, it would not be feasible for regulators to set function-agnostic data protection standards for each of them. Consequently, this paper has made the case for an autonomous, multistakeholder data protection agency that will evaluate user complaints, perform security audits, lay down best practices and hold companies and developers accountable to sector-specific standards as well as their own policies.

institut français
des relations
internationales