BRIDGING THE TRANSPARENCY GAP

A COMPARATIVE ASSESSMENT OF SURVEILLANCE-RELATED TRANSPARENCY EFFORTS IN THE UNITED STATES AND INDIA

August 2021

NEW AMERICA
OPEN TECHNOLOGY INSTITUTE
ESYA centre

ABOUT THE AUTHORS

Spandana Singh is a Policy Analyst at New America.

Meghna Bal is a lawyer and technology policy researcher based in Delhi.

ABOUT THE ESYA CENTRE

The Esya Centre is a New Delhi based technology policy think tank. The Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. It aims to build institutional capacities for generating ideas that will connect the triad of people, innovation, and value to help reimagine the public policy discourse in India. More details can be found at www.esyacentre.org and on Twitter @EsyaCentre.

ABOUT THE OPEN TECHNOLOGY INSTITUTE

The Open Technology Institute (OTI) works at the intersection of technology and policy to ensure that every community has equitable access to digital technology and its benefits. We promote universal access to communications technologies that are both open and secure, using a multidisciplinary approach that brings together advocates, researchers, organizers, and innovators. To learn more, please visit us online at www.newamerica.org/oti and on Twitter @OTI.

ABOUT NEW AMERICA

New America is dedicated to renewing the promise of America, bringing us closer to our nation's highest ideals. We're a different kind of think tank: one dedicated to public problem solving. Our team of visionary researchers, changemakers, technologists, and storytellers study and seize the opportunities presented by dramatic social and technological change. We search for powerful ideas, wherever they are, and collaborate with civic innovators around the country to develop evidence-based solutions. To learn more, please visit us online at www.newamerica.org or follow us on Twitter @NewAmerica.

Design Credits

Illustrations by *Taniya O'Connor*
Layout by *Khalid Jaleel*

CONTENTS

OVERVIEW

The United States and India both operate sophisticated and extensive government surveillance programs that increasingly involve collecting user data and seeking such data from domestic and international technology companies. As government surveillance efforts become increasingly intertwined with the corporate world, it is imperative that both governments and companies provide meaningful and adequate transparency around their operations and how they intersect with the surveillance ecosystem. This transparency is important as it can enhance accountability and inform ongoing domestic and bilateral public policy conversations as well as discussions around appropriate safeguards for citizens.

INTRODUCTION

In 2013, Edward Snowden, a U.S. government contractor, leaked thousands of classified documents from the U.S. National Security Agency (NSA) which exposed details about the extent of government surveillance in the United States. The Snowden disclosures highlighted how the NSA had been able to acquire mass amounts of data from major internet and telecommunications corporations which had been fulfilling the government's sweeping requests for user information.[1]

The Snowden disclosures also revealed that India was the fifth-most tracked country by the United States with the NSA collecting 6.3 billion units of data on the country.[2] In addition, over the past few years, the Government of India has significantly expanded its surveillance efforts, sparking concerns among civil society and citizens. In 2013, for example, the United Progressive Alliance Government (UPA2), a coalition of center-left political parties in India, announced plans to launch a Central Monitoring System which, when fully implemented, would bring all electronic communications within the country under the government's lens.[3] Further, transparency reports from several U.S.-based internet companies have indicated that government requests for user data in India are at an all-time high. In the first half of 2020, for example, Facebook received 35,560 requests for user data from the Indian government, compared to 26,698 during the second half of 2019.[4]

The Snowden disclosures created a significant trust deficit in the digital space, causing consumers to grow wary of governments and major technology and telecommunications companies.

The Snowden disclosures created a significant trust deficit in the digital space, causing consumers to grow wary of governments and major technology and telecommunications companies.

Since then, governments have come under increased pressure to provide more transparency around the extent of their surveillance programs. In addition, civil society organizations have similarly called on internet and telecommunications companies to provide greater transparency around the scope and scale of government surveillance requests they receive, particularly with regard to user data.[5] The Snowden disclosures also fostered tensions between governments around the world, many of whom began calling for data localization in order to protect their citizens' data privacy and security.[6] These localization mandates would require internet platforms to store all information that they collected, carried, or processed on the country's citizens within their nation's borders.

As this report will outline, the U.S. and India both operate vast surveillance apparatuses. Both nations have also engaged in complex and rather unique domestic debates regarding the scope of government surveillance power, its influence on technology and telecommunications companies, and its impact on the privacy and security of their citizens. Until recently, the surveillance efforts of these two countries were viewed as unrelated to one another. However, a deeper understanding of the surveillance ecosystems

[1] Rachel King, "FBI, NSA Said To Be Secretly Mining Data From Nine U.S. Tech Giants," *ZDNet*, June 6, 2013, https://www.zdnet.com/article/fbi-nsa-said-to-be-secretly-mining-data-from-nine-u-s-tech-giants/.

[2] Jayshree Bajoria, "India's Snooping and Snowden," *India Real Time - Wall Street Journal* (blog), June 5, 2014, https://blogs.wsj.com/indiarealtime/2014/06/05/indias-snooping-and-snowden/.

[3] Rohan Joshi, "India's Central Monitoring System," Discussion Document (Bengaluru: Takshashila Institution, July 2013), http://takshashila.org.in/wp-content/uploads/2013/07/India%E2%80%99s-Central-Monitoring-System-Rohan-Joshi.pdf.

[4] Yuthika Bhargava, "India's request for user data second only to U.S.", *The Hindu*, May 13, 2020. https://www.thehindu.com/news/national/indias-request-for-facebook-user-data-second-only-to-us/article31572505.ece.

"Facebook Transparency Report." Facebook, 2020. https://transparency.facebook.com/government-data-requests/country/IN.

[5] Kevin Bankston, Ross Schulman, and Liz Woolery, *Getting Internet Companies To Do The Right Thing*, February 2017, https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/.

[6] Benjamin Wittes, "Jonah Force Hill: The Growth of Data Localization Post-Snowden (Lawfare Research Paper Series)," *Lawfare*, July 21, 2014, https://www.lawfareblog.com/jonah-force-hill-growth-data-localization-post-snowden-lawfare-research-paper-series.

in both of these nations, and how they overlap, is becoming increasingly important for several reasons.

First, India is a growing and lucrative market for U.S. companies that are acquiring and managing increasing amounts of data on Indian citizens. The number of internet users in the country has boomed over the last 20 years—rising from a mere six million in 2005[7] to a whopping 700 million in 2020.[8] In addition, 2020 figures have indicated that Facebook has 328 million users in India, far more than the company has in the United States.[9] Similarly, India is the largest market for the messaging platform WhatsApp, with over 400 million users.[10] India therefore offers significant market potential to U.S. companies seeking to expand their user base and product offerings.[11] However, as domestic surveillance efforts in India simultaneously expand, these companies are receiving an increased number of government requests for data on Indian citizens. It is therefore important to understand the norms and principles that guide such surveillance efforts from both the American and Indian perspectives.

Over the past decade, India has emerged as a global destination for innovation, startups, and technology

Second, over the past decade, India has emerged as a global destination for innovation, startups, and technology. The country is home to a number of successful technology businesses including e-commerce and digital wallet company Paytm, food-tech company Zomato, and food-delivery startup Swiggy.[12] These companies are rapidly expanding and simultaneously acquiring greater troves of user data, at times on an international scale. As expansion into new markets, including the U.S., becomes a possibility for these companies, they are likely to face greater pressure to institute stronger privacy and security safeguards for their users, both from governments and other entities such as civil society organizations. India's engagement with these public policy and digital rights issues is relatively nascent. As such, existing legal frameworks in India that are applicable to tech companies remain underdeveloped. A greater comparative understanding of the surveillance landscape in both nations, including the laws, policies, and regulations guiding these operations, would provide useful insights into how the United States and India may improve their frameworks to generate beneficial outcomes for their citizens and economies.

Finally, the United States and India are increasingly exploring bilateral partnerships, including in the technology space. In 2018, the U.S. government passed the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which authorizes the United States to enter into "Executive Agreements" with other countries to facilitate foreign governments' access to data held by U.S. tech companies and vice versa.[13] Given the deep involvement of U.S. tech companies in India, the United States and India may soon explore the formation of such an Executive Agreement. However, in order for such a plan to see fruition, India would have to, among other things, establish a minimum threshold for privacy and security of user data—as per CLOUD Act requirements—and the U.S. government would have to certify that the other country (in this case, India) meets specified standards for safeguarding human rights such as privacy. Existing frameworks in India such as the Indian Information Technology Act, 2000 (IT Act) are inadequate in this regard, and therefore the government would have to introduce a new set of standards and mechanisms in order to qualify for the Executive Agreement. The Indian government is currently considering the Personal Data Protection Bill, 2019 (2019 PDP Bill), which would broadly provide a framework for the protection of personal data of individuals, regulate the flow and usage of data by the

[7] Economics Research Unit - Statistics, "Telecom Statistics India - 2017" (Department of Telecommunications, Government of India, 2017), http://dot.gov.in/sites/default/files/Telecom%20Statistics%20India-2017.pdf.

[8] "Number of Internet Users in India from 2015 to 2022" (Statista, July 2017), https://www.statista.com/statistics/255146/number-of-internet-users-in-india/.

[9] Noor F. Wasia, "*Facebook brings its A-game to India*", *Business World,* August 6, 2020. http://www.businessworld.in/article/Facebook-Brings-Its-A-Game-To-India/26-08-2020-313142/ https://www.barrons.com/articles/india-facebook-users-surpass-u-s-is-it-apple-demonetization-14999982716.

[10] Wasia, "*Facebook brings its A-game*" and Gadgets 360 Staff, "WhatsApp Now Has 200 Million Monthly Active Users in India," *Gadgets 360*, February 25, 2017, https://gadgets.ndtv.com/apps/news/whatsapp-now-has-200-million-monthly-active-users-in-india-1663332.

[11] Rajan Anandan, "Google for India: Building Services for Every Indian, In Their Language," *The Keyword* (blog), entry posted August 28, 2018, https://www.blog.google/technology/next-billion-users/google-for-india-2018/.

[12] Durba Ghosh, "2018 Saw A Whole New Breed of Indian Startup Unicorns Emerge," *Quartz India*, December 19, 2018, https://qz.com/india/1499596/indias-byjus-zomato-oyo-swiggy-udaan-became-unicorns-in-2018/.

[13] Clarifying Lawful Overseas Use of Data Act, S. 2383, 115th, 2D. https://www.congress.gov/bill/115th-congress/senate-bill/2383/text.

public and private sectors, and establish a Data Protection Authority of India.[14]

A comparative assessment of surveillance powers, associated transparency mechanisms, and their limitations in both nations can therefore inform discussions on what a potential bilateral partnership between India and the United States would look like. Such an assessment can also inform ongoing efforts to reform surveillance-related standards and mechanisms in both countries.

This report begins by providing an overview of the surveillance landscape in both the United States and India. It then analyzes relevant government and corporate transparency mechanisms in both countries. The report concludes by providing recommendations on how both governments and companies in both countries can promote greater transparency and accountability around their engagements within the surveillance landscape.

***Editorial Disclosure**: This paper discusses policies by Dropbox, Facebook, Google (including YouTube), Microsoft, and Twitter, all of which are funders of work at New America but did not contribute funds directly to the research or writing of this piece. New America is guided by the principles of full transparency, independence, and accessibility in all its activities and partnerships. New America does not engage in research or educational activities directed or influenced in any way by financial supporters. View our full list of donors at www.newamerica.org/our-funding.*

[14] Personal Data Protection Bill, 2019 (India).

THE SURVEILLANCE LANDSCAPE IN THE UNITED STATES

The surveillance landscape in the United States today results from a patchwork of programs and authorities that date back several decades, some of which have expanded over time.

In the 1970s, the U.S. Senate formed the Church Committee to investigate allegations that the U.S. government was spying on its own citizens. The Church Committee Report, published in 1976, revealed a wide range of intelligence community abuses and ultimately led to the enactment of the Foreign Intelligence Surveillance Act of 1978 (FISA).[15] FISA established standards and procedures to govern certain types of U.S. government surveillance.

Several years later, on December 4, 1981, U.S. President Ronald Reagan issued Executive Order 12333, also known as the *United States Intelligence Activities* order. The order was based on the notion that "timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents, is essential to the national security of the United States,"[16] and it set forth the powers and responsibilities of U.S. intelligence agencies. EO 12333 is considered to have established the foundation for the numerous expansive intelligence-operated data collection programs in the United States over the past few decades.[17] During his term, President George W. Bush twice further amended that program, via Executive Order 13355: Strengthened Management of the Intelligence Community in 2004,[18] and Executive Order 13470: Further Amendments to Executive Order 12333, United States Intelligence Activities in 2008.[19] Both amendments to the original Executive Order altered the governance and reporting structures of U.S. intelligence agencies in order to strengthen their operations. As amended, EO 12333 remains the governing authority for most ongoing U.S. intelligence activities, other than those conducted under FISA.

> The authorities for U.S. intelligence activities were further expanded after the September 11 terrorist attacks.

The authorities for U.S. intelligence activities were further expanded after the September 11 terrorist attacks. Shortly after the attacks, President George W. Bush signed an Executive Order which declared a State of National Emergency. This order gave the President the authority to allocate defense funds as he saw fit, expand the size and operations of the military, and broaden the surveillance capacities of the state, among other things.[20] President Barack Obama signed similar orders on an annual basis to continue these practices.[21]

---

[15] Senate Historical Office, "Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities," United States Senate, https://www.senate.gov/artandhistory/history/common/investigations/ChurchCommittee.htm.

[16] Exec. Order No. 12333 Fed. Reg. (Dec. 4, 1981). https://www.archives.gov/federal-register/codification/executive-order/12333.html.

[17] Rainey Reitman, "EFF's Game Plan for Ending Global Mass Surveillance," *Deeplinks* (blog), entry posted January 26, 2015, https://www.eff.org/deeplinks/2015/01/effs-game-plan-ending-global-mass-surveillance.

[18] "Executive Order: Strengthened Management of the Intelligence Community," news release, August 27, 2004, https://georgewbush-whitehouse.archives.gov/news/releases/2004/08/20040827-6.html.

[19] Chris Strohm, "Bush Orders Intelligence Overhaul," Nuclear Threat Initiative, last modified August 1, 2008, https://www.nti.org/gsn/article/bush-orders-intelligence-overhaul/.

[20] Zac Copeland, "The National Emergency Under Executive Order 13224 Moves into Year 16," *Lawfare Blog*, entry posted November 3, 2016, https://www.lawfareblog.com/national-emergency-under-executive-order-13224-moves-year-16.

[21] Ned Resnikoff, "Obama Quietly Extends Post-9/11 State of National Emergency," *MSNBC*, September 25, 2013, http://www.msnbc.com/all/obama-quietly-extends-post-911-state.

Further, in October 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) was signed into law with the aim of strengthening national security.[22] Title II of the Act, focused on enhancing surveillance procedures, amended FISA and the Electronic Communications Privacy Act (ECPA). It enhanced the powers for government agencies to gather foreign intelligence information from both citizens of the United States as well as foreigners. Title II also expanded the scope and availability of wiretapping, surveillance orders, and search warrants.[23]

Several provisions of the PATRIOT Act are subject to "sunset" dates, forcing Congress to reconsider and reauthorize them. The two most recent extensions of expiring PATRIOT Act provisions were in May 2011 when President Barack Obama signed a four-year extension of certain provisions of the USA PATRIOT Act under the PATRIOT Sunsets Extension Act of 2011,24 and in June 2015, one day after three provisions of the USA PATRIOT Act expired. On June 2, 2015, Congress enacted the USA FREEDOM Act, which reauthorized all three expiring provisions of the USA PATRIOT Act until December 15, 2019.25 However, the USA FREEDOM Act significantly amended Section 215, which enables the government to obtain an order from the secret FISA court to require third parties to turn over tangible things such as business records. Section 215 has been interpreted to permit the collection of "telephony metadata" (call-log information such as the date, time, and duration of calls to and from a phone number)26 in connection with foreign intelligence and counterterrorism investigations.27 However, the USA FREEDOM Act clarified that Section 215 may not be used for bulk collection of such data. The amended Section 215 includes authority to collect call detail records from communications service providers, where records are deemed relevant to international terrorism. The USA FREEDOM Act also instituted a number of additional reforms to the PATRIOT Act.

On March 15, 2020, Section 215 of the PATRIOT Act expired, along with the roving wiretap provision (which allows a Foreign Intelligence Surveillance Court order or electronic surveillance to be applied to numerous cell phone numbers used by the same target)[28] and the lone wolf authority under FISA (which allows the government to obtain surveillance orders under Title I of FISA for specific individuals without having to prove they are connected to a foreign power or organization, but has not been used since it was enacted in 2001).[29] Prior to 2020, U.S. Congress has not allowed PATRIOT surveillance authorities to lapse for more than one day since they were enacted in October 2001. In 2020, both the U.S. House of Representatives and Senate passed editions of the USA FREEDOM Reauthorization Act but did not make efforts to merge the two bills or otherwise address the reauthorization of the three expired provisions. As experts have noted, it is unclear how the expiration of these authorities has influenced intelligence activities, if at all.[30]

For these reasons, U.S. Senators Patrick Leahy (D-VT) and Mike Lee (R-UT) penned a letter in July

---

[22] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001). https://www.govinfo.gov/content/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf.

American Civil Liberties Union, "Surveillance Under the USA/Patriot Act," American Civil Liberties Union, https://www.aclu.org/other/surveillance-under-usapatriot-act.

[23] Electronic Privacy Information Center, "Analysis of Specific USA PATRIOT Act Provisions: Pen Registers, the Internet and Carnivore," Electronic Privacy Information Center, https://www.epic.org/privacy/terrorism/usapatriot/.

[24] Jim Abrams, "Patriot Act Extension Signed By Obama," *Huffington Post*, December 6, 2017, https://www.huffingtonpost.com/2011/05/27/patriot-act-extension-signed-obama-autopen_n_867851.html.

[25] Cindy Cohn and Rainey Reitman, "USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here," Electronic Frontier Foundation, last modified June 2, 2015, https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here.

[26] Scott F. Mann, "Fact Sheet: Section 215 of the USA PATRIOT Act," Center for Strategic & International Studies, last modified February 27, 2014, https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act.

[27] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM Act) Act of 2015, https://www.congress.gov/114/plaws/publ23/PLAW-114publ23.pdf.

[28] "FISA Reauthorization," Senate Republican Policy Committee, last modified February 25, 2020, https://www.rpc.senate.gov/policy-papers/fisa-reauthorization.

[29] "FISA Reauthorization," Senate Republican Policy Committee.

[30] Sharon Bradford Franklin, "Statement on Behalf of OTI to the Privacy and Civil Liberties Oversight Board on Exercise of Authorities Under the Foreign Intelligence Surveillance Act," address presented at Privacy and Civil Liberties Oversight Board Hearing, Washington, DC, USA, August 31, 2020, New America's Open Technology Institute, last modified August 31, 2020, https://www.newamerica.org/oti/testimonies/statement-behalf-oti-privacy-and-civil-liberties-oversight-board-exercise-authorities-under-foreign-intelligence-surveillance-act/.

2020 to then Attorney General Barr and the Director of National Intelligence raising concerns that intelligence agencies may be inappropriately relying on Executive Order 12333 or other surveillance powers to fill gaps created by the expired authorities. Such concerns from both civil society and lawmakers underscore the need for fundamental surveillance reform in the United States and demonstrate the need for the intelligence community to provide greater transparency around how the recent expiration of the three surveillance authorities has influenced their operations. Such transparency could also contribute to more informed policymaking, especially related to future surveillance reforms.

FISA has been repeatedly amended since the September 11 attacks, with the intention of expanding the government's surveillance capabilities and making it easier to obtain surveillance warrants.

In addition to Executive Order 12333, FISA also provides significant authority for surveillance for foreign intelligence purposes. As noted above, it was enacted after, and in direct response to, surveillance abuse scandals that arose in the 1970s around illegal spying on U.S. citizens by the U.S. government.[31] FISA is a federal law which outlines procedures for physical and electronic surveillance and the collection of foreign intelligence information regarding foreign powers and agents of foreign powers. The Act established the Foreign Intelligence Surveillance Court (FISC) to oversee and manage requests for surveillance warrants under FISA by law enforcement and intelligence agencies. FISA has been repeatedly amended since the September 11 attacks, with the intention of expanding the government's surveillance capabilities and making it easier to obtain surveillance warrants.[32]

The principal statutes that govern the U.S. government's efforts to acquire information for law enforcement purposes from or with the assistance of domestic entities in the United States are FISA (which permits for domestic information collection for foreign intelligence purposes), the Wiretap Act, and ECPA. The Fourth Amendment of the U.S. Constitution provides safeguards limiting all U.S. surveillance of U.S. persons—citizens and legal permanent residents—and of people inside the United States. The Fourth Amendment also limits collection under FISA and EO 12333, to the extent that the collection under FISA is targeted at, or any of these collections are reasonably anticipated to collect information regarding, U.S. persons (these authorities are discussed in detail below).

Despite these safeguards and the improvements made since the Snowden revelations, U.S. surveillance laws remain overbroad and in need of reform. These issues are now complicating U.S. trade with other nations. On July 16, 2020, the Court of Justice of the European Union struck down the Privacy Shield, which had facilitated data transfers between the United States and the EU in Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems (Schrems II). Under the Schrems II case, the Court outlined that U.S. surveillance laws, particularly Section 702 of FISA and Executive Order 12333, do not provide sufficient levels of protection for the personal data of European citizens as are provided under EU law, including the General Data Protection Regulation (GDPR). The court determined that FISA Section 702 and E.O. 12333 did not align with the principle of proportionality under EU law, as it could not be guaranteed that those surveillance programs were only collecting data that is strictly necessary on EU citizens. Further, the court found that EU citizens lacked a sufficient mechanism for judicial redress under those laws.[33] This is further indication that U.S. surveillance programs must be reformed significantly. Such reforms should ensure that surveillance operations are focused on "legitimate and appropriate targets," include strong safeguards for privacy and civil liberties, provide meaningful redress opportunities for all individuals subject to U.S. surveillance, and encourage transparency, among other things.[34]

[31] NCC Staff, "Looking back at the Church Committee," Constitution Daily, https://constitutioncenter.org/blog/looking-back-at-the-church-committee.

[32] Electronic Privacy Information Center, "Foreign Intelligence Surveillance Act (FISA)," Electronic Privacy Information Center, https://epic.org/privacy/surveillance/fisa/.

[33] *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, C-311/18, Court of Justice of the European Union, July 16, 2020, https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN

[34] Sharon Bradford Franklin et al., *Strengthening Surveillance Safeguards After Schrems II: A Roadmap for Reform*, April 7, 2021, https://www.newamerica.org/oti/reports/strengthening-surveillance-safeguards-after-schrems-ii/.

Surveillance Mechanisms in the United States

Currently, the U.S. government employs a number of mechanisms to acquire user information, both domestically and internationally. These are broken down below:

Search Warrants: The Fourth Amendment of the United States Constitution protects against unreasonable searches and seizures. In general, this requires that the government obtain a search warrant based on a showing of probable cause. However, courts have recognized various exceptions to the warrant requirement and have approved statutory procedures in certain types of cases that do not require a probable cause showing.

National Security Letters (NSL): An NSL is a request for information that certain agencies of the U.S. Executive Branch can make when they are conducting national security investigations.[35] Currently, NSLs are authorized under four federal statutes: the Electronic Communications Privacy Act (ECPA) (18 U.S.C. § 2709), the National Security Act (50 U.S.C. § 3162), the Right to Financial Privacy Act (12 U.S.C. § 3414), and the Fair Credit Reporting Act (15 U.S.C. §§ 1681u, v.).[36] Under ECPA 18 U.S.C. Section 2709, NSLs compel companies to disclose "the name, address, length of service, and local and long distance toll billing records" of a subscriber to a wire or electronic communications service.[37] NSLs cannot be used in ordinary criminal, civil, or administrative cases and cannot be used to acquire information on services outside this scope. NSLs can only be used to collect information that is considered to be less sensitive (e.g., not the content of communications), and must only meet a lower standard of proof, such as relevance to an authorized investigation. Although NSLs are a U.S. government procedure, many foreign governments have similar legal processes that allow them to obtain information for the purposes of national security.[38] For example, in India, directions for interception, known as "lawful orders" are permitted under Rule 419A of the Indian Telegraph Rules (Telegraph Rules) and Section 69 of the IT Act. [39]

Foreign Intelligence Surveillance Act (FISA): As explained above, FISA was originally enacted in 1978 to manage how the U.S. government collects certain foreign intelligence information for national security purposes. The Act established the Foreign Intelligence Surveillance Court (FISC), which is comprised of 11 federal district court judges who review government applications for electronic surveillance and other requests for intelligence collection, as well as the Foreign Intelligence Surveillance Court of Review (FISCR), which reviews appeals from the FISC. Both the FISC and FISCR can compel companies to hand over information for foreign intelligence investigations. The original types of surveillance orders authorized by FISA require the government to show probable cause to believe that the target is a foreign power or an agent of a foreign power. The FISA Amendments Act of 2008 expanded FISA by, among other provisions, adding Section 702, which authorizes the U.S. government to target non-Americans located abroad and to collect the content of their communications. Under Section 702 the FISC does not review individual applications regarding particular surveillance targets, but instead approves certifications for certain categories of intelligence information such as counterterrorism and approves targeting and minimization procedures.

The Electronic Communications Privacy Act (ECPA): ECPA was enacted in 1986. It broadened the Federal Wiretap Act of 1968, which until then had focused on providing protections from interception of telephone lines, to also include interceptions of computer and digital and electronic communications. In general, it outlines the standards under which U.S. law enforcement agencies can obtain electronic communications data from tech companies. ECPA has been amended over the past decades, including by the PATRIOT Act.[40] However, it still re-

[35] Electronic Frontier Foundation, "National Security Letters: FAQ," Electronic Frontier Foundation, https://www.eff.org/issues/national-security-letters/faq.

[36] Electronic Frontier Foundation, "National Security," Electronic Frontier Foundation.

[37] Counterintelligence Access to Telephone Toll and Transactional Records, 18 U.S.C. § 2709. https://www.law.cornell.edu/uscode/text/18/2709.

[38] Electronic Frontier Foundation, "National Security," Electronic Frontier Foundation.

[39] Software Freedom Law Center, "Freedom in the Net," Software Freedom Law Center, last modified January 9, 2015, https://sflc.in/indias-surveillance-state-procedural-legal-framework.

[40] U.S. Department of Justice, "Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2510-2523.," Justice Information Sharing, https://it.ojp.gov/privacyliberty/authorities/statutes/1285.

quires further amendments to ensure the statute remains applicable and relevant given the rapid pace of new communications technologies.[41]

One of the most recent amendments to ECPA has been through the CLOUD Act. The CLOUD Act amended the Stored Wire Electronic Communications Act (also known as the Stored Communications Act), which is part of Title II of ECPA. This amendment, made in March 2018, sought to address the question of whether U.S. companies must comply with U.S. law enforcement requests for data access, regardless of where the data is being stored. This debate was brought up by the *Microsoft Corp. v. United States* case, as Microsoft refused to turn over data to U.S. law enforcement agencies based on the reasoning that the data was being stored in Ireland.[42] The passage of the CLOUD Act resolved the dispute between Microsoft and the U.S. government and has now created a more streamlined structure with which U.S. law enforcement agencies can obtain access to data for investigations.[43] The CLOUD Act also enables foreign governments who enter into Executive Agreements with the U.S. government to submit requests for the content of electronic communications directly to U.S. companies, and vice versa. However, as of now no bilateral agreements are in place.

In addition, ECPA enables law enforcement agencies to obtain data from private companies in cases involving the imminent threat of death or serious physical injury to any person. In such cases, law enforcement agencies can submit an Emergency Disclosure Request to companies, which requests the expedited release of basic subscriber or user information to the agency.[44]

ECPA also sets out several different procedures and standards related to government agencies requesting user information from companies. The most common method for making such requests is through the use of a subpoena.[45] Under ECPA, there are some cases in which the courts recognize that the requirements of the Fourth Amendment can be met with lower standards than probable cause. As a result, a warrant based on probable cause is not necessary and rather law enforcement, depending on how intrusive the data request is, can obtain a subpoena or a court order, such as a D-order, instead.[46] D-orders require a higher standard than a subpoena. They are most commonly used to obtain non-content, transactional customer records such as the addresses of websites that an individual has visited and the email addresses of other people the individual has corresponded with.[47]

[41] "Digital Due Process Coalition," Digital Due Process Coalition, https://digitaldueprocess.org/.

[42] Sharon Bradford Franklin, "The Microsoft-Ireland Case: A Supreme Court Preface to the Congressional Debate," *Lawfare*, February 22, 2018, https://www.lawfareblog.com/microsoft-ireland-case-supreme-court-preface-congressional-debate.

[43] Electronic Privacy Information Center, "The CLOUD Act," Electronic Privacy Information Center, https://epic.org/privacy/cloud-act/.

[44] Voluntary Disclosure of Customer Communications or Records, 18 U.S.C. § 2702. https://www.law.cornell.edu/uscode/text/18/2702.

[45] Electronic Privacy Information Center, "Electronic Communications Privacy Act (ECPA)," Electronic Privacy Information Center, https://epic.org/privacy/ecpa/.

[46] Electronic Privacy Information Center, "Electronic Communications," Electronic Privacy Information Center.

[47] Electronic Privacy Information Center, "Electronic Communications," Electronic Privacy Information Center.

THE SURVEILLANCE LANDSCAPE IN INDIA

The surveillance landscape in India and the associated government surveillance powers are a colonial legacy. The Indian Telegraph Act, 1885, (Telegraph Act) which was originally enacted by the British to allow the establishment of telegraph lines on private property,[48] also allowed for authorities to intercept any message or take over any telegraph in cases of public emergency.[49]

After India gained independence, the Telegraph Act was retained by the new government. Over the years, the government's abuse of the surveillance capabilities afforded by the Telegraph Act have come to light numerous times. In 1991, for example, a Central Bureau of Investigation (CBI) investigation founded on a complaint made by Chandra Shekhar, a prominent Indian politician, revealed that the administration of Prime Minister Indira Gandhi had tapped the phones of at least 50 politicians and tampered with physical mail.[50] A few years later, it was revealed that throughout the course of the 1980s, both the Central and State governments had sanctioned the tapping of several politicians' phones.[51] These phone-tapping revelations under both the Indira Gandhi and Rajiv Gandhi regimes prompted the People's Union for Civil Liberties (PUCL), a human rights organization, to file a writ petition in the Supreme Court of India challenging the constitutionality of Section 5(2) of the Telegraph Act.[52] The petition also called for the creation of procedural safeguards to prevent the arbitrary tapping of telephones.[53]

In *PUCL vs. Union of India*, the Indian Supreme Court noted that Section 5(1) of the Telegraph Act empowers the Central or State government to temporarily take over any communication medium in the event of a public emergency or the emergence of a threat to public safety.[54] The Court also observed that Section 5(2) allows the Central or State government to authorize the interception or prevent the dissemination of any message or class of messages only if it is necessitated by matters related to the country's sovereignty and security, maintaining public order or friendly foreign relations, and the prevention of criminal activity.[55]

Ruling on the issue, the Court noted that the power accorded to the government under Section 5(2) to intercept any communication could only be exercised if there was a public emergency or a threat to public safety, as provided by Section 5(1) of the Telegraph Act.[56] Further, the Court stated that the interception power under 5(2) must be qualified by procedural provisions that ensure that its application is just and reasonable.[57] The Court then laid out a set of procedural guidelines to be followed by any government that deemed it necessary to exercise its surveillance powers under Section 5 of the Telegraph Act.[58] The guidelines were subsequently incorporated into the Telegraph Rules.[59]

---

[48] "Act No. XXXIV of 1854 for Regulating the Establishment and Management of Electric Telegraphs in India" (1854), https://wipolex.wipo.int/en/text/389822.

[49] "Indian Telegraph Act" (1885), http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf.

[50] Prabhu Chawla, "Secret Report by CBI Contains Shocking Details of Phone Tapping Ordered by Congress(I) Govts," *India Today*, February 28, 1991, https://www.indiatoday.in/magazine/special-report/story/19910228-secret-report-by-cbi-contains-shocking-details-of-phone-tapping-ordered-by-congressi-govts-814118-1991-02-28.

[51] Chawla, "Secret Report by CBI Contains Shocking Details of Phone Tapping".

[52] The Supreme Court of India, *People's Union for Civil Liberties v. The Union of India and Another*, December 18, 1996, https://indiankanoon.org/doc/31276692/.

[53] The Supreme Court of India, *People's Union for Civil Liberties v. The Union of India.*

[54] The Supreme Court of India, *People's Union for Civil Liberties v. The Union of India.*

[55] The Supreme Court of India, *People's Union for Civil Liberties v. The Union of India.*

[56] The Supreme Court of India, *People's Union for Civil Liberties v. The Union of India.*

[57] The Supreme Court of India, *People's Union for Civil Liberties v. The Union of India.*

[58] The Supreme Court of India, *People's Union for Civil Liberties v. The Union of India.*

[59] "The Indian Telegraph Rules, 1951," § 419A (2014), http://www.dot.gov.in/sites/default/files/358%20GI-2014%20dated%208.2.2014_6.pdf?download=1.

The Indian government has had far reaching powers which have enabled it to carry out widespread surveillance for decades. However, the government only began developing the infrastructure necessary to enable the use of powers to their broadest extent in 2007.

As demonstrated, the Indian government has had far-reaching powers which have enabled it to carry out widespread surveillance for decades. However, the government only began developing the infrastructure necessary to enable the use of these powers to their broadest extent in 2007. The 2007-2008 Annual Report from the Department of Telecommunications (DoT) outlined that after extensive discussions with several security agencies, specifications for a Central Monitoring System (CMS) had been finalized by the Telecommunications Engineering Centre, an agency operating under the aegis of the DoT.[60] The CMS would be used to monitor communications on mobile phones, landlines, as well as on the internet in India,[61] and would enable government agencies to access a target directly and avoid manual interference by Telecom Service Providers.[62] After the CMS project was formally approved in 2011, the Centre for Development of Telematics, a government institution dedicated to communications research and development, was charged with executing the CMS project.[63] Once the CMS was operational, its daily operations would be handled by the Telecom Enforcement Resource and Monitoring Cells.[64]

Despite the fact that the CMS offers the government far-reaching surveillance capabilities, there is very little information available on the CMS in the public domain. A news report from 2016 indicated that the CMS is already operational in some Indian cities such as Mumbai and Delhi.[65] The CMS potentially enables the government to secretly but continuously monitor communications within the country in real-time, without any external oversight over how such activity is being targeted.[66]

As internet and telecommunications companies grow and acquire more user data, they will also increasingly receive requests for this data from governments around the world. Presently, Indian law enforcement authorities rely on the Mutual Legal Assistance Treaty (MLAT) process to acquire data from companies in other countries, primarily in the United States. The MLAT is a formal framework for information exchange between two countries, in this case the United States and India, to aid law enforcement in criminal cases. However, the MLAT process is time-consuming and cumbersome. According to one report, it can take anywhere between 3-6 months for law enforcement to obtain the data it requires through the MLAT process.[67] This has largely prompted the Indian government to push for data localization provisions, which would require international companies to store the personal data of Indian citizens processed in India within the country's borders.[68] In 2018, the Srikrishna Committee, convened to formulate a data protection framework for the country, drafted the 2018 PDP Bill. The Committee also compiled a report calling for data mirroring and localization, citing several reasons for why data must be housed locally in India, including concerns related to national security and the cumbersome nature of

[60] "Annual Report 2007-2008" (Department of Telecommunications, Ministry of Communications and Information Technology, 2008), http://dot.gov.in/sites/default/files/English%20annual%20report%202007-08_0.pdf as cited by Jaideep Reddy, "The Central Monitoring System and Privacy: Analysing What We Know so Far," Indian Journal of Law and Technology 10 (2014): 41–62.

[61] "Centralised System to Monitor Communications" (Press Information Bureau, India, November 26, 2009), http://pib.nic.in/newsite/erelease.aspx?relid=54679 as cited by Jaideep Reddy, "The Central Monitoring System and Privacy: Analysing What We Know so Far," *Indian Journal of Law and Technology* 10 (2014): 41–62.

[62] Jaideep Reddy, "The Central Monitoring System and Privacy: Analysing What We Know so Far," *Indian Journal of Law and Technology* 10 (2014): 41–62.

[63] Reddy, Central Monitoring System.

[64] Reddy, Central Monitoring System.

[65] Sneha Johari, "Govt's Central Monitoring System Already Live in Delhi & Mumbai," *MediaNama*, May 11, 2016, https://www.medianama.com/2016/05/223-india-central-monitoring-system-live-in-delhi-mumbai/.

[66] Johari, Central Monitoring System Already Live in Delhi & Mumbai.

[67] Bedavyasa Mohanty and Madhulika Srikumar, "Hitting Refresh: Making India-US Data Sharing Work," Special Report (New Delhi: Observer Research Foundation, August 2017), https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf.

[68] "Report by the Committee of Experts under the Chairmanship of Justice B.N. Srikrishna" (New Delhi: Justice B.N. Srikrishna Committee, July 2018), http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

the cross-border data acquisition process offered through MLATs.[69]

The 2018 PDP Bill proposed the institution of data mirroring, which would require a copy of personal data related to Indian citizens to be stored in India and the localization of certain types of personal data.[70] In addition, according to the Bill, cross-border transfers of personal data were contingent on approvals from the Data Protection Authority and the government. Only categories of sensitive personal data approved by the government could be transferred outside the country whereas the transfer of critical personal data was barred. Sensitive personal data included financial data, passwords, health data, data related to a person's sexual preference and orientation, and any data that pertains to religious affiliation. Critical personal data was not defined in the Bill. Rather, the Bill empowered the Central government to decide which categories of personal data qualified as critical.

The calls for mirroring and localization in the 2018 PDP Bill were problematic. Experts noted that if the goal of the Bill was to provide better privacy to citizens in India, the push for localization and mirroring made little sense because the Bill did not provide any relevant protections in this regard.[71] Moreover, as the following section will outline, Indian authorities enjoy access to broad surveillance powers with virtually no external oversight. Mandating the localization and mirroring of data without establishing a set of safeguards around how that data is accessed by law enforcement and other government agencies raises further concerns about potential abuses of power.

In December 2019, a new version of the PDP Bill was tabled before the Indian Parliament. It was subsequently referred to a Joint Committee on the Personal Data Protection Bill, which is preparing a report on the merits of the new draft.[72] Localization requirements in the 2019 iteration of the PDP Bill are slightly more liberal than the 2018 version. For example, the 2019 PDP Bill does not have a mirroring requirement.[73] However, sensitive personal data must still be stored in India and may only be transferred outside the country subject to conditions similar to those placed on the cross-border transfer of personal data under the 2018 PDP Bill.[74] In addition, the Bill states that critical personal data may only be processed in India.[75]

However, the 2019 PDP Bill fails to give the Data Protection Authority adequate autonomy from the Central government.[76] For instance, Section 86 provides that the government may direct the Data Protection Authority to do anything the former deems necessary in cases related to matters of national security, sovereignty, and diplomacy, and the Data Protection Authority must comply. Further, the 2019 Bill also grants law enforcement agencies broad exemptions from data protection obligations when personal data is processed to investigate, detect, prosecute, or even prevent a criminal or illegal act.[77]

The 2019 PDP Bill grants law enforcement agencies broad freedoms and fails to provide adequate safeguards to check the abuse of these powers. Section 91 of the 2019 Bill empowers the Central government to direct data fiduciaries to provide non-personal data to support targeted state subsidy facilities or formulate evidence-based policies.[78] The use of the term non-personal data is contentious, however, as it is vaguely defined as "any data other than personal data" which would include anonymized personal data.[79] This creates further opportunity for the misuse of data by agencies.

In addition, the legitimacy of demands for data localization and mirroring must be questioned in light of the passage of the CLOUD Act in the United

---

[69] B.N. Srikrishna Committee Report.

[70] Government of India, *Personal Data Protection Bill,* 2018, S. 40, https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf

[71] Rishabh Bailey, "The issues around data localisation", The Hindu,

[72] "Press Release: Joint Committee on the Personal Data Protection Bill, 2019." Parliament of India, January 27, 2020. http://loksabhaph.nic.in/Committee/CommitteeInformation.aspx?comm_code=73&tab=1.

[73] The Personal Data Protection Bill, 2019, Chapter VII https://www.prsindia.org/sites/default/files/bill_files/Personal%20Data%20Protection%20Bill%2C%202019.pdf.

[74] The entity facilitating the transfer of personal data outside the country must obtain explicit consent being given by the person whose data it is for doing so. Further the transfer must be made pursuant to a contract or intra-group scheme approved by the Data Protection Authority.

[75] *The Personal Data Protection Bill,* 2019, § 33.

[76] *The Personal Data Protection Bil*l, 2019, § 86.

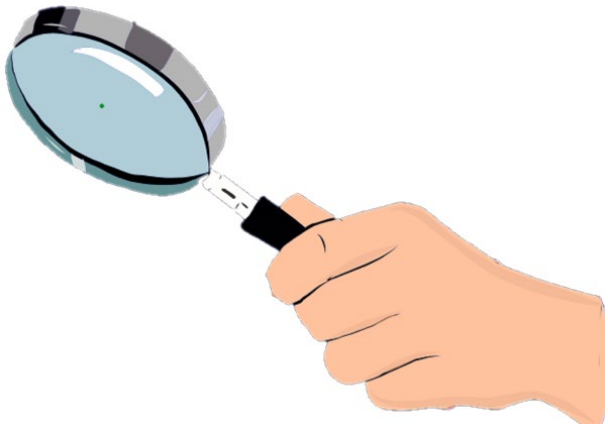
[77] *The Personal Data Protection Bil*l, 2019, § 36.

[78] *The Personal Data Protection Bil*l, 2019, § 91.

[79] The Personal Data Protection Bill, 2019, § 91

States. As previously discussed, the CLOUD Act could allow the United States and India to enter into a bilateral agreement through which the latter's law enforcement agencies could directly approach private U.S. tech companies for user information, without having to go through U.S. courts.[80] An agreement under the CLOUD Act would likely provide law enforcement agencies with a more efficient alternative to the MLAT process, thus negating the need for localization.

The 2020 Draft E-Commerce Policy also includes proposals for data localization. According to the online Indian news portal *Medianama*, a leaked copy of the draft stated that "an unspecified authority can restrict the cross-border flow of potentially commercial data" relating to national security, health, genome, and biometrics.[81] Under this bill, the government would define the categories of data that require localization.[82]



[80] Sreenidhi Srinivasan et al., India-US Data Sharing for Law Enforcement: Blueprint for Reforms, January 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.

[81] Agrawal, Aditi. "India's New Draft e-Commerce Policy Focuses on Data, Competition, Counterfeiting, Consumer Protection." MEDIANAMA, July 3, 2020. https://www.medianama.com/2020/07/223-second-draft-ecommerce-policy-india/.

[82] Agarwal, India's New Draft e-commerce Policy.

Surveillance Mechanisms in India

Currently, Indian authorities employ several mechanisms to acquire user data from both U.S. and Indian entities.

Mechanisms Used to Acquire User Data from U.S. Entities:

Direct Requests: According to Section 91 of the Code of Criminal Procedure (CrPC), any officer or court may issue summons to any entity or individual in possession of a document or anything else that is necessary for aiding a trial. As a result, Indian authorities may directly submit requests for "non-content data" from private international corporations without having to navigate U.S. legal procedures.[83] ECPA, as discussed above, prohibits U.S. companies from sharing any communications content without an appropriate court order. However, it does not expressly forbid voluntarily sharing data such as a user's identity or location with foreign governments.[84] Provided that requests are deemed appropriate and in line with their policies, U.S. entities generally share this information voluntarily with Indian law enforcement authorities.

Emergency Requests: In cases of emergency, such as the death of an individual, Indian law enforcement authorities can request user data from U.S.-based entities.[85] The responses to emergency requests are generally quick, "often within hours" provided that the law enforcement agencies are able to establish a case for exigency.[86]

Letters Rogatory: Letters of request, also known as letters rogatory, are sent by a competent court in India to a competent court in the United States, where the former asks the latter to assist in the production of evidence relevant to an investigation.[87] Under Section 166-A of the CrPC, the investigating officer must submit an application to their superior, stating that the evidence may be located outside the country.[88] The superior officer, after consulting with the Ministry of Home Affairs (MHA), brings the application for a letter of request before the competent court in India.

Mutual Legal Assistance Treaty (MLAT): As previously outlined, an MLAT is an agreement generally used by two or more countries for cooperation in criminal investigations. The US-India MLAT in Criminal Matters was signed in 2001 and entered into force in 2005.[89] In instances where data is stored in the United States, India can request support from the U.S. government in obtaining evidence from entities in the United States, including technology and telecommunications companies. If the request is approved by the U.S. government, a company would be required to comply with it. The U.S. government can similarly use the MLAT process to access data stored in India . However, as previously outlined, the MLAT process is known for being cumbersome and can therefore hinder ongoing investigations.[90] In India, requests for user information under the MLAT follow a similar procedure as requests submitted using letters rogatory. However, in the case of an MLAT request for non-communications content such as meta-data (call time, duration, etc.), the investigating officer does not need to go through a competent court and may present their application to the MHA directly.[91] In instances where a foreign government is seeking to gain access to communications content from U.S. companies, its request would need to go through a U.S. court.

---

[83] Bedavyasa Mohanty and Madhulika Srikumar, "Hitting Refresh: Making India-US Data Sharing Work," Special Report (New Delhi: Observer Research Foundation, August 2017), https://www.orfonline.org/wp-content/uploads/2017/08/MLAT-Book.pdf.

[84] Bedavyasa Mohanty, Hitting Refresh.

[85] "Guidelines for Indian Law Enforcement Agencies" (Ministry of External Affairs, India, August 2015), http://mea.gov.in/Images/pdf1/Extradition_Guidelines.pdf.

[86] Bedavyasa Mohanty, Hitting Refresh.

[87] "Comprehensive Guidelines for Investigation Abroad and Issue of Letters Rogatory (LR)" (Ministry of Home Affairs, Government of India, December 31, 2007), https://mha.gov.in/sites/default/files/LR-170709.pdf.

[88] "Code of Criminal Procedure," § 166-A (1973).

[89] Office of Treaty Affairs,"*India (05-1003) – Treaty on Mutual Legal Assistance in Criminal Matters*", U.S. Department of State, https://www.state.gov/05-1003.

[90] Access Now, "Mutual Legal Assistance Treaties," Mutual Legal Assistance Treaties, https://www.mlat.info/faq.

[91] "Comprehensive Guidelines Regarding Service of Summons/Notices/Judicial Process in Criminal Matters on the Persons Residing Abroad" (Ministry of Home Affairs. Government of India, February 2009), https://mha.gov.in/sites/default/files/ISIIMX-M452N_20190222_22022019.pdf.

Mechanisms to Acquire Data from Indian Entities:

The Indian Information Technology Act, 2000 (IT Act): Section 69 of the IT Act grants competent authorities the power to issue directions for the interception, decryption, or monitoring of digital information in certain cases. These include cases that are relevant to the defense of the country, national sovereignty or integrity, national security, maintaining friendly foreign relations and public order, preventing the commission of a cognizable crime, and investigating any offence. Section 69B further allows the Central government to authorize any government agency to monitor and collect data to enhance the country's cybersecurity and to contain the spread of malware.[92] Section 79 of the IT Act and the Rules published thereunder also enables government agencies to send information requests to intermediaries.[93]

The Indian Telegraph Act (Telegraph Act): As previously discussed, Section 5(1) of the Telegraph Act enables the Central or State governments to take "temporary possession" of any "telegraph"[94] in the event of a public emergency or in the interest of public safety, for as long as the public emergency or threat to public safety exists. Section 3(1) of the Telegraph Act defines a telegraph as "any appliance, instrument, material or apparatus used or capable of use for transmission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, visual or other electro-magnetic emissions, radio waves or Hertzian waves, galvanic, electric or magnetic means".[95] Thus, any electronic communications device or infrastructure could technically qualify as a telegraph today. Section 5(2) of the Telegraph Act allows the Central or State governments to authorize the interception or prevention of the dissemination of any message or class of messages in cases related to the country's sovereignty and security, maintaining public order or friendly foreign relations, and the prevention of criminal activity.[96]

The Indian Telegraph (Amendment) Rules, 2007 (Telegraph Rules): Rule 419A of the 2007 Indian Telegraph (Amendment) Rules states that only the Secretary of the Home Ministry may call for the interception of messages or any class of messages.[97] Rule 419A was brought in to codify the guidelines set forth by the Supreme Court in the matter of *PUCL vs Union of India* to bridge the absence of a defined procedure for government surveillance. However, in the event of "unavoidable circumstances" a Joint Secretary may also issue orders for interception if they have received authorization from either the Union or the State Home Secretary. Additionally, in exigent situations, where it is not feasible to obtain prior orders for the interception of communications, the senior most or second most senior officers from authorized security agencies at the Central or the State level may also issue orders to intercept communications.[98]

Indian Post Office Act, 1898 (IPO Act): Section 26 of the IPO Act grants Central or State governments the power to seize any postal articles in the event of a public emergency or in the interest of ensuring public safety or tranquility.[99]

Code of Criminal Procedure, 1973 (CrPC): Under Section 91 of the CrPC, any Indian court or officer in charge of a police station may summon an individual to produce information or evidence that may be relevant for the purpose of an investigation, trial, inquiry, or any other criminal proceeding.[100]

---

[92] Government of India, "*The Information Technology Act, 2000*" (2000).

[93] The Information Technology Act, 2000 and The Information Technology (Intermediaries Guidelines) Rules, 2011 (2011), r3(7).

[94] " The Indian Telegraph Act, 1885" (1885), http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf.

[95] The Indian Telegraph Act, 1885.

[96] "The Indian Telegraph Act, 1885" (1885), http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf.

[97] "The Indian Telegraph (1st Amendment of 2014) Rules, 2014," § 419A (2014), http://www.dot.gov.in/sites/default/files/358%20GI-2014%20dated%208.2.2014_6.pdf?download=1.

[98] The Indian Telegraph Rules, Rule 419A.

[99] Government of India, "T*he Indian Post Office Act*," § 26 (1898), https://www.indiapost.gov.in/VAS/DOP_RTI/TheIndianPostOfficeAct1898.pdf.

[100] Government of India, "T*he Code of Criminal Procedure*," § 91 (1973).

Telecom Licenses: In order to offer their services in India, internet service providers (ISPs) and telecom service providers (TSPs) must establish and comply with license agreements with the Department of Telecommunications.[101] These agreements have a wide range of requirements which facilitate government surveillance.[102] Some of these are explained below.

- **TSP License Agreement:** TSPs are required to comply with two separate license agreements—the Cellular Mobile Telephone Service License Agreement (CMTS Agreement) and the License Agreement for the Provision of Basic Telephone Services (BTS Agreement). The CMTS Agreement applies to cell phone communication services while the BTS Agreement applies to fixed-line communication services.

  The CMTS Agreement requires TSPs to provide facilities for the simultaneous monitoring of calls by government security agencies.[i] TSPs must also provide designated authorities within the Central and State governments with "necessary facilities" that would enable the government to monitor information passing through the TSPs' networks.[i] The BTS Agreement outlines that the government has the right to monitor communications at any point within a TSP's network.[i]

- **ISP License Agreements:** ISPs in India must comply with the License Agreement for Provision of Internet Services (LAPIS). LAPIS requires ISPs to provide tracing facilities to government authorities so that the government can track and block obscene, unauthorized, or infringing content on the ISP's network.[i] ISPs are also required to share a list of their subscriber bases with government agencies and maintain a monitoring centre at their own expenses.[i]

- **License Agreement for Unified Access Service (UASL):** Both ISPs and TSPs are required to comply with the UASL. Under the UASL, ISPs and TSPs must facilitate the interception requests made under Section 5 of the Telegraph Act as directed by the Licensor.[i] Paradoxically, although the UASL prohibits ISPs and TSPs from deploying bulk encryption on their networks, it also tasks them with the responsibility of securing subscriber privacy and preventing unlawful interception of communications.[i]

- **Unified License Agreement (UL):** The UL includes provisions related to monitoring and interception for both ISPs and TSPs that are similar to those in the UASL. However, the provisions in the UL are more granular in scope. For instance, clause 41.16 requires ISPs and TSPs to ensure there are backups in place in monitoring systems to prevent glitches.[i]

[101] The Government of India is currently mooting a proposal to consider whether certain communications over-the-top platforms such as Whatsapp and Facebook Messenger should adhere to the conditions stipulated in Telecom Licences and regulations. If such a regulation is passed, these entities might have to conform with some of the surveillance requirements applicable to telecom service providers and internet service providers.

[102] For an exhaustive overview of stipulations within Telecom Licenses that facilitate surveillance please see, "State of Cyber Security and Surveillance in India: A Review of the Legal Landscape" (Center for Internet and Society, India), https://cis-india.org/internet-governance/blog/state-of-cyber-security-and-surveillance-in-india.pdf.

GOVERNMENT TRANSPARENCY EFFORTS IN THE UNITED STATES AND INDIA

Although both the United States and India operate broad surveillance programs, both countries fail to provide adequate transparency to the public about these operations. However, because the United States currently has greater protections related to digital and consumer rights than India, its efforts to provide transparency around its surveillance are more established and comprehensive.

In the United States, there are a number of methods for providing transparency around surveillance efforts at the federal level. Some of these reporting mechanisms are required by law and are based on clear guidelines that detail which entities are required to prepare and publish these reports and what information must be included in the reports. Other reporting mechanisms, however, are not based on legal frameworks and may aim to provide more information on surveillance efforts than is legally required. Currently, the primary methods of providing transparency around surveillance operations at the federal level are:

1. The Office of the Director of National Intelligence's (ODNI) Office of Civil Liberties, Privacy, and Transparency releases an annual Statistical Transparency Report Regarding Use of National Security Authorities. The report includes data on FISA probable cause court orders and targets; FISA Section 702-related orders, targets, and U.S. person queries; FISA use in criminal proceedings; the use of pen register and trap and trace devices; orders, targets, and unique identifiers collected related to business records, and National Security Letters.[1]

2. The Administrative Office of the U.S. Courts produces an annual wiretap report which includes information related to federal and state applications for orders for wire, oral, or electronic communications. The report does not include data on information collected under FISA.[1]

3. The Administrative Office of the U.S. Courts produces a separate annual report covering the operations of the Foreign Intelligence Surveillance Court (FISC).[1]

4. The U.S. Department of Justice produces an annual report with data on applications to use pen registers and/or trap and trace devices under FISA.[1]

5. The U.S. Department of Justice also produces an annual report which covers:[1]

    a. All final, filed applications by the government for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes under the Act

    b. All final, filed applications by the government made for obtaining access to certain business records

    c. Certain requests made by the FBI related to NSL authorities

The U.S. government can promote greater transparency around its surveillance operations by increasing the amount of this information that is available to the public.

Although these transparency reporting mechanisms are valuable and important, there is room for improvement. For example, under FISA, methods for promoting transparency exist, but these reports are only delivered to Congress, rather than the general public. The reporting of this classified and sensitive information enables further oversight. However, it does not promote greater transparency and accountability around oversight procedures for the public. Going forward, the U.S. government can promote greater transparency around its surveillance operations by increasing the amount of this information that is available to the public.

In addition, greater transparency is needed around how the government collects data on U.S. persons under FISA. These efforts should be carried out and overseen by the Privacy and Civil Liberties Oversight Board (PCLOB), an independent agency that was established by Congress in 2004 to oversee issues related to privacy and civil liberties in the United States, particularly related to policies and practices on terrorism.[103] In particular, the PCLOB should introduce and encourage measures which promote greater transparency and accountability around FISA activities to the public. These efforts should include information that enhances public understanding and awareness around how the intelligence community has used Section 702 of FISA to collect information on U.S. persons. Although there is some contention around what measures and metrics would be most accurate, such information around the scope and scale of these surveillance efforts are critical.

Specifically, the PCLOB should encourage the intelligence community to disclose greater information on the impact FISA surveillance activities have had on members of racial minorities and other protected groups or on First Amendment-protected activities such as protests. FISA does not include specific prohibitions on targeting individuals based on their race, religion, gender, ethnicity, or other protected class status and there are no public guidelines around this issue. FISA prohibits the targeting of surveillance that is "solely" based on First Amendment-protected activities, but there are questions around whether this offers adequate safeguards for First Amendment activities. It is therefore vital that the government provide greater transparency around how it targets individuals for surveillance based on their membership in a protected class or based on whether they are exercising their First Amendment rights, and what the impact of these surveillance efforts is. Both the House and Senate editions of the USA FREEDOM Reauthorization Act of 2020 included guidance that the PCLOB should prepare a public report examining these issues (though those bills never made it into law, as explained earlier). PCLOB should move forward and produce such a report even without a congressional mandate, as it would provide vital transparency to the public and could help inform future policymaking in this space.

When compared to government efforts to promote transparency around surveillance operations in the United States, government efforts to provide transparency around surveillance efforts in India are limited. The 2019 PDP Bill demonstrates the Indian government's continuous pattern of extending the remit of surveillance without enacting any concomitant safeguards or transparency measures to check any abuse of power. Currently, the Indian government does not have any mandated or voluntary reporting structures that disclose qualitative or quantitative data related to its surveillance efforts. Going forward, the Indian government should publish granular data on surveillance-related requests made under the Telegraph Rules, Telecom Licenses, and the IT Act. At a minimum, this data should include aggregate quantitative statistics on the number of government requests for user data it has submitted to private companies. This data should be broken down by industry in order to outline which industries are being approached for access to user data the most and to demonstrate what kinds of user data law enforcement authorities are obtaining access to the most. This data can also inform much needed public policy conversations between advocates, companies, and the government on how to improve surveillance-related transparency efforts, as well as safeguards and consumer protections.

Going forward, any extension of surveillance powers in India must be accompanied with adequate safeguards that protect user rights. The International Principles on the Application of Human Rights to

[103] "History and Mission," U.S. Privacy and Civil Liberties Oversight Board, https://www.pclob.gov/About/HistoryMission.

Communications Surveillance (Necessary and Proportionate Principles), which are the culmination of a two-year effort by 40 of the world's leading experts on privacy and security, are a valuable starting point for such transparency efforts.[104] The Principles state that interception provisions should be balanced against human rights considerations, as these rights will be threatened if surveillance powers are abused.[105] In addition, the Necessary and Proportionate Principles outline a framework of checks and balances to ensure that surveillance efforts are restricted to a narrow remit and adhere to established norms of procedural fairness.[106] Overall, the Principles call for comprehensive transparency around the scope and scale of government surveillance efforts being carried out and call on governments to disclose information related to these efforts.[107] Introducing transparency-related safeguards and requirements would especially help provide greater insight into governmental surveillance programs such as the CMS.

Concerningly, over the last year, the Indian government introduced changes to the Right to Information Act, 2005 (RTI Act), thereby undermining the principles of transparency and accountability with relation to the surveillance landscape. The RTI Act was introduced in 2005 to provide greater transparency and accountability around the operations of public authorities.[108] Under the Act, Indian citizens can investigate how a government agency performs its duties by requesting information from the agency.[109] Agencies that receive requests are required to provide the requesting citizen with the information requested except for certain items which are delineated under Section 8 of the RTI Act.

For instance, the government is not obligated to share any information that would prejudice the sovereignty of India or any key strategic matter for the state.

The RTI Act encompasses a tripartite enforcement structure. Public authorities—any authority, body, institution, or self-government established by or under the Constitution, Parliamentary legislation, State legislation, or government notification such as public sector companies and regulators—are required to appoint Public Information Officers and Assistant Public Information Officers at the Central and State level, depending on the scope of the public authority's office.[110] Citizen requests for information first go to the Central/State Assistant Public Information Officers who are then required to forward the requests to the Central/State Public Information officers. As stated above, the Public Information Officers are required to issue a response within 30 days of the receipt of the request. Appeals from these determinations go to an Appellate Authority. An appeal from the Appellate Authority's decision then goes to the Central or State Information Commission. These bodies consist of a Chief Information Commissioner plus 10 other Information Commissioners.[111]

In July 2019, the government amended the RTI Act.[112] The 2019 changes impact the terms and conditions of service of the Chief Information Commissioner as well as the Information Commissioners at the Central and State levels. Initially the tenure of Central/State Chief Information Commissioner and other Information Commissioner was fixed by the legislation for a period of five years. However, as a result of the amendment to the RTI Act, the Central

[104] "International Principles on the Application of Human Rights to Communications Surveillance." Electronic Frontier Foundation, July 10, 2013. https://www.eff.org/files/necessaryandproportionatefinal.pdf.

[105] International Principles on the Application of Human Rights to Communications Surveillance.

[106] International Principles on the Application of Human Rights to Communications Surveillance.

[107] Meghna Bal and Ananth Padmanabhan, "*Response to OTT Consultation Paper*" (New Delhi: Center for Policy Research,2019), http://cprindia.org/research/reports/trai-consultation-paper-regulating-over-top-communication-services-response-1.

[108] Government of India, "*The Right to Information Act*", Long Title (2005). https://rti.gov.in/rti-act.pdf.

[109] The Act also encourages the government to publish as much information as it can, within the contours of the Act, so that citizens only have to seek it out as a last resort. Citizens can make requests for information either by post or electronically and public authorities are expected to respond to requests within 30 days. If the citizen is not satisfied with the response, such as when the request for information is refused, they may appeal the decision.

[110] The Right to Information Act, § 5.

[111] The Right to Information Act, § 12(2).

[112] Prior to this amendment the PDP Bill, 2018 also called for an amendment of the RTI Act. Specifically, it called for Section 8 of the RTI Act to be amended, so that it forbade any disclosure of information relating to an *individual's personal data that could harm that individual*, if the extent of harm outweighs the benefit of ensuring *transparency and accountability* in the operations of a public authority.# Such an amendment would allow the State to block citizens' attempts to investigate how the government processes citizen's data.# It would, therefore, severely circumscribe citizen agency within the Indian democracy, as it would directly hinder a citizen's ability to check the state of governance in the country. The PDP Bill, 2019 removed the amendment to Section 8 of the RTI Act.

government now has the power to determine the duration of Commissioners' tenures.[113] In addition, previously, the remuneration payable to the Commissioners was determined by the RTI Act so that they were on par with the salaries given to senior level government officers.[114] However, due to the amendment to the RTI Act, the Central government has the discretion to determine these officers' salaries.[115] Given that the very institution the Commissions are supposed to supply information about now determines the salaries and tenures of their officers, these changes could significantly erode the independence of the Information Commissions. This could have serious repercussions for the state of transparency and accountability around government operations in India, including around government surveillance efforts.[116] Since its passage the amendment has garnered heavy criticism from civil society and opposition leaders, as it was passed with very little public debate and hardly any parliamentary scrutiny.[117] The RTI Amendment was challenged by a member of the central Indian legislative arm, the Parliament, before the Supreme Court.[118] However, a judgment is yet to be passed in the matter[119]

Regardless of the outcome of the challenge to the amendment, however, the government should consider publishing statistics related to surveillance requests in a manner that does not jeopardize any strategic or national security interests. Such an effort would go a long way in instilling trust and confidence amongst citizens in the digital space in India. In the past, the government has responded to Right to Information requests regarding lawful orders for surveillance issued under the Telegraph Act. For example, the Software Freedom Law Centre, a non-governmental organization that focuses on issues of digital freedoms and rights, filed a Right to Information request with the Ministry of Home Affairs in 2014, asking for information on the number of orders issued under Rule 419A of the Telegraph Rules and a breakdown of the quantum of orders issued under this Rule by each agency authorized to do so.[120] While the government declined to respond to the latter portion of the request due to security reasons, it disclosed that the government issued 7,500-9,000 phone interception orders per month. The 2019 amendment to the RTI may frustrate transparency efforts further in the future by creating an environment that discourages independent decision-making by information commissioners, thereby making them less inclined to disclose such figures.

Additionally, as previously outlined given the paltry state of safeguards surrounding surveillance in India, the government must consider the introduction of broader reforms such as the creation of a statute based on the International Principles on the Application of Human Rights to Communications Surveillance to ensure that there are no abuses of surveillance powers.

In a positive development, however, the government issued the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 which prescribe due diligence standards for online intermediaries. These require online intermediaries with over five million users to publish monthly compliance reports which detail the content takedown requests received and the actions undertaken for redressal.[121]

---

[113] Sinha, Roshni. "Explainer: The Right to Information (Amendment) Bill, 2019." PRS Legislative Research, July 19, 2019. https://www.prsindia.org/theprsblog/explainer-right-information-amendment-bill-2019.

[114]Singh, Explainer: The Right to Information Amendment.

[115] Singh, Explainer: The Right to Information Amendment.

[116] Singh, Explainer: The Right to Information Amendment.

[117] Ray, Kalyan. "Parliament Passes Controversial RTI Amendment Bill." The Deccan Herald, July 25, 2019. https://www.deccanherald.com/national/national-politics/parliament-passes-controversial-rti-amendment-bill-749591.html.

[118] "SC Issues Notice to Centre on Jairam Ramesh's PIL Challenging RTI Act Amendment." The Tribune, January 31, 2020. https://www.tribuneindia.com/news/nation/sc-issues-notice-to-centre-on-jairam-rameshs-pil-challenging-rti-act-amendment-34060.

[119] Jairam Ramesh vs. Union of India & Ors., No. W.P. (C) No. 1473 of 2019 (Supreme Court Pending). https://main.sci.gov.in/php/case_status/case_status_process.php?d_no=45158&d_yr=2019.

[120] "Information on India's Surveillance Practices," April 9, 2014. https://sflc.in/information-received-under-rti-for-surveillance#:~:text=In%20March%202014%2C%20SFLC.in,such%20orders%20under%20the%20Rule.

[121] Government of India, "Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, R. 4(1)(d), (2021), https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf.

CORPORATE TRANSPARENCY EFFORTS IN THE UNITED STATES AND INDIA

Private companies also play an important role in promoting transparency around government surveillance efforts. As previously discussed, both the United States and India are home to rapidly growing internet and telecommunications companies that are expanding their global reaches and processing increasing amounts of user data. As a result, the likelihood of data collected by these companies being collected or shared for government surveillance purposes is increasing.

For example, according to Google's bi-annual transparency report on government requests for user information, in the second half of 2019, the company received a record number of user data disclosure requests (10,891) for India, which specified a record number of users or accounts (25,896).[122] The number of requests for user data, as well as the number of users and accounts specified in these requests, has grown markedly over the years.[123] For reference, during the same period in 2011 Google received only 2,207 requests, which specified 3,427 accounts. Because governments are increasingly seeking access to user data collected by companies, it is vital that these companies implement meaningful transparency measures.[124]

Although companies based in the United States face some restrictions around the surveillance-related data they can disclose, these companies have greater leeway to share such data compared to companies based in India.

In the United States, ECPA enables companies to report data related to ECPA demands that they have received. In addition, the USA FREEDOM Act allows companies to publish numerical information related to NSLs and FISA orders they receive through four different kinds of banded ranges of numbers. Typically, reporting on smaller band ranges will be less granular and will see longer delays in reporting as a result of the statute. The four categories of bands are:[125]

- Reporting in bands of 1000, semiannually, covering a period of 180 days or more, with a 180-day delay for FISA process. This category enables companies to separately report on the number of requests and the number of customer selectors targeted by NSLs, FISA orders for content, and FISA orders for non-content. Companies can also report the specific number of customer selectors targeted for three FISA non-content requests: pen register and trap and trace orders, orders for the ongoing production of call detail records, and orders for other business records.

- Reporting in bands of 500. This reporting category is similar to the first category, but it does not permit companies to report on customer selectors targeted for the three FISA-non content requests.

- Reporting in bands of 250, semiannually, covering a period of 180 days or more, with no delay. In this category, companies are not permitted to separately report on NSLs, FISA for content, and FISA for non-content. Rather, they can only publish one figure outlining the total number of national-security related requests, and the total of customer selectors targeted by those requests.

- Reporting in bands of 100, annually, covering a period of one year and delayed for at least one year. Similar to the third option, this reporting category only permits companies to report the total number of national security-related requests and the total number of targeted customer selectors.

[122] "Google Transparency Report: Requests for User Information." Google, December 2019. https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:IN;time:Y2011H2&lu=user_requests_report_period.

[123] Google, "Requests for User Information," Transparency Report, last modified 2018, https://transparencyreport.google.com/user-data/overview?hl=en.

[124] Kevin Bankston, Liz Woolery, and Ryan Budish, *The Transparency Reporting Toolkit - Guide and Template*, December 29, 2016, https://www.newamerica.org/oti/policy-papers/transparency-reporting-toolkit-reporting-guide-and-template/.

[125] Bankston, Woolery, and Budish, *The Transparency*.

Although U.S.-based companies are permitted to disclose some information related to government requests for user data that they receive, these arbitrary and wide reporting bands prevent companies from providing more granular and meaningful transparency and accountability around the scope and scale of such demands. Going forward, the U.S. government should eradicate these banded requirements and permit companies to publish more granular and specific data related to national security-related demands.

In the United States, companies issuing transparency reports that outline the scope and scale of government requests for their users' information, under current restrictions, is now considered an industry-wide best practice. Resources such as the Transparency Reporting Toolkit, produced by New America's Open Technology Institute and Harvard University's Berkman Klein Center for Internet & Society, aimed to guide companies on how to best structure and standardize these reports.[126] Many U.S.-based technology and telecommunications companies also have clear, instituted policies and systems for processing government requests for information.[127] Google, for example, outlines its policies and procedures on its website and also provides users with a Frequently Asked Questions section that answers questions such as why a government agency might request user information, what Google does when they receive such a request (including when they challenge requests), and what different legal frameworks can be used to acquire user information.[128] Similarly, Automattic, the parent company of popular content management system WordPress, publishes its legal guidelines online, which outline what user information Automattic has, what the relevant U.S. legal processes the company is subject to are, and the policies and procedures the company follows when it receives a request.[129] These procedures are applied to these companies' operations globally, and therefore Indian users benefit and are safeguarded by these procedures as well.

In India, corporate efforts to provide transparency and accountability around how companies are intertwined with government surveillance operations are limited. Most Indian companies do not have comparable, rights-protecting policies for managing requests for surveillance assistance, including government requests for user data. While the privacy policies of most Indian companies mention that they share data with the government and other agencies, they do not outline this process in detail. For example, India's most popular mobile wallet application Paytm states in its privacy policy that it will share user data with external agencies to enable service provision, through a legally mandated request, or to mitigate fraud. It does not, however, detail under what law such requests could be made or in service of which law they would share data to enable service provision. Paytm's privacy policy also states that the company will never share personal data without the user's consent. However, a sting operation carried out last year by an Indian investigative news agency, *Cobrapost*, revealed that the company had been using its platform to assist the political agenda of the ruling party, the Bharatiya Janata Party (BJP).[130] The *Cobrapost* sting also revealed that Paytm had been sharing personal user data with the Indian Prime Minister's Office, following a case of rioting in the state of Kashmir.[131]

Companies in India should publish clear and accessible information explaining how they manage user data and what their policies for sharing user data with the government are.

Going forward, companies in India such as Paytm should publish clear and accessible information explaining how they manage user data and what their policies for sharing user data with the government are. These policies should explain in detail when a company would share user data with the government, what kind of user data the company can share, what laws the company provides user data under, how the company evaluates requests for user data to

[126] Bankston, Woolery, and Budish, *The Transparency*.

[127] Ranking Digital Rights, *2019 Corporate Accountability Index*, May 2019, https://rankingdigitalrights.org/index2019/assets/static/download/RDRindex2019report.pdf.

[128] Google, "United States Legal Process FAQs," Transparency Report Help Center, https://support.google.com/transparencyreport/answer/9700059.

[129] Automattic, "Legal Guidelines," WordPress, https://wordpress.com/support/report-blogs/legal-guidelines/.

[130] *Operation-136 II, Paytm* (Cobrapost, 2018), https://www.youtube.com/watch?v=lvj8hRD1GY4&t=0s&list=PLtIitJsHQm66Z2Vk7UsYE_Bhyo_eYG_C&index=4.

[131] *Operation-136 II.*

ensure they are appropriate, and when the company pushes back on incomplete requests. These policies should be easy to access on a company's website and should be written in plain language that is digestible for the average user. Transparency reports would also provide greater insight into how companies are managing user data and when they are sharing such data with the Indian, and potentially other, governments.

Corporate transparency reporting, however, is still a relatively uncommon phenomenon, even for the largest Indian technology and telecommunications companies

Corporate transparency reporting, however, is still a relatively uncommon phenomenon, even for the largest Indian technology and telecommunications companies. Currently, the vast majority of data available on government requests for user data in India are published by U.S.-based companies such as Google, Facebook, and Twitter. However, these companies offer differing levels of granularity between countries. According to a report by the Center for Internet and Society in India, Google only discloses information on three types of data requests for India. In comparison, the company provides information on eight different request categories for the United States. These disparities may exist due to legal restrictions on disclosures in India (discussed below). However, Indian companies should, at the very least, begin publishing transparency reports that are in line with the reports published by U.S. companies. Further, both U.S. and Indian companies should aim to publish more granular data in their reports on requests in the Indian context. Such granular reporting is possible under law for companies based in India. For example, disclosures that pertain to requests under Section 91 of the CrPC are legal. As a result, transparency reports could include data on the specific provision of Indian law under which requests were made,[132] where such disclosure is not expressly prohibited such as in the case of Section 91 of the CrPC or Section 79 of the IT Act and its rules.

There are several reasons why corporate transparency reporting is not currently a significant practice in India. These could serve as obstacles for solidifying the practice as an industry wide practice in the future as well.

1. Voluntary disclosures about government requests for user data is prohibited by several Indian laws. Section 5(2) of the Telegraph Act read with Rule 419 (A) of the Telegraph Rules requires TSPs to "maintain extreme secrecy" when dealing with affairs relating to legal interception.[133] Additionally, Rule 25(4) of the Information Technology (Procedure and Safeguards for Interception, Monitoring, and Decryption of Information) Rules, 2009 and Rule 11 of the Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009 mandate the maintenance of absolute confidentiality on orders for decryption, monitoring, collection, or interception of traffic data.[134] Moreover, The UASL and the ISP license agreements also contain confidentiality clauses that require licensees to maintain the confidentiality of any secret information shared with them during the licensing agreement.[135] These restrictions go as far as preventing entities from even divulging the existence of surveillance orders. As such, telecommunications companies and ISPs are prohibited from publishing aggregate data on government requests for user information.

2. There are important legal caveats. There is no bar on reporting requests under Section 91 of the CrPC. However, Section 91 does provide that its provisions are not applicable to any information held by a postal or telegraph authority. The definition of these terms is uncertain and open to judicial scrutiny.136 For instance, telecommunications could be interpreted as a

[132] Sarkar, Torsha, Suhan S, and Gurshabad Grover. "Through the Looking Glass: Analysing Transparency Reports." The Center for Internet and Society, October 31, 2019. https://cis-india.org/internet-governance/files/A%20collation%20and%20analysis%20of%20government%20requests%20for%20user%20data%20%20and%20content%20removal%20from%20non-Indian%20intermediaries%20.pdf.

[133] Indian Telegraph Act, S. 5(2) and Indian Telegraph Rules, Rule 419A.

[134] "Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009," § 25(4) (2009) and "Information Technology (Procedure and Safeguards for Monitoring and Collecting Traffic Data or Information) Rules, 2009," § 11 (2009).

[135] Unified Access Service License and the Internet Service Provider License.

[136] Krishnakumar, Tarun. "Law Enforcement Access to Data in India: Considering the Past, Present, and Future of Section 91 of the Code of Criminal Procedure, 1973." The Indian Journal of Law and Technology 15 (2019): 67–101.

telegraph authority.137 In such a case, Section 92 of the CRPC would apply which gives judicial officers the discretion to decide whether such information is relevant to a case and take the information directly from the relevant postal or telegraph authority.138 Notably, Section 92 does not prohibit disclosure of such requests either, provided that the information may need to be kept a secret while the matter is pending. Further, requests for information made by the government to intermediaries under Section 79 of the IT Act and the IT Rules may also be reported as there is no express prohibition for these either. Now, the IT Rules, 2021 mandate publishing information on content takedown requests under Section 79 of the IT Act.

3. In India, privacy only recently became a prominent public policy concern. Although judicial deliberations on privacy in India date as far back as 1954, significant discursive interest in privacy only arose within the country in 2010.[139] Since then, the privacy movement has slowly garnered momentum. The clarion call for better privacy safeguards possibly rang loudest with the enactment of the Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits, and Services) Act in 2016. The Aadhaar Act was introduced to serve as the legal framework underpinning India's eponymous unique identification program. Aadhaar IDs were meant to serve as facilitators for better, more targeted delivery of government subsidies, benefits, and services. To prevent the creation of fraudulent identities, citizens are required to hand over their biometric information (fingerprints and iris scans) when registering for Aadhaar. These details are linked to a particular Aadhaar number. When that individual comes to claim any service covered by the scheme, the biometric details serve as a point of verification. However, the introduction of the program has raised concerns about the privacy of user data, especially with regard to government monitoring of citizen activities,[140] as well as the security of user data, given the number of breaches and scandals the program has undergone.[141]

   a. The Aadhaar program became quite controversial for several reasons. According to human rights activist Usha Ramanathan, the Unique Identification Authority of India (UIDAI) was coercing individuals to sign up for Aadhaar cards by making the availability of government services contingent on having enrolled for Aadhaar.[142] The Aadhaar Act purportedly granted legal sanction to the UIDAI's alleged actions. In addition, Section 57 of the Aadhaar Act allowed private as well as public entities to use Aadhaar to establish the identity of an individual for "any purpose."[143] As discussed, the verification process under Aadhaar requires an Aadhaar holder to present their Aadhaar ID as well as their biometric information to obtain access to a service, such as a SIM card for their mobile phone. The receiving entity could then seek the authentication of the person's ID by sending the person's Aadhaar ID as well as the person's biometric information to the UIDAI.

   b. In 2018, the Supreme Court of India struck down the applicability of Section 57 to private entities, stating that the provision enabled the "commercial exploitation of an individual's biometric and demographic information by the private entities" and was a

---

137 Krishnakumar, Law Enforcement Access to Data in India.

138 Krishnakumar, Law Enforcement Access to Data in India.

139 "Internet Privacy in India" (The Center for Internet and Society, India), https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india.

140 Rhyea Malik and Subhajit Basu, "India's Dodgy Mass Surveillance Project Should Concern Us All," *Wired*, August 25, 2017, https://www.wired.co.uk/article/india-aadhaar-biometrics-privacy.

141 Rachna Khaira, Aman Sethi, and Gopal Sathe, "Huffington Post," *UIDAI's Aadhaar Software Hacked, ID Database Compromised, Experts Confirm*, September 11, 2018, https://www.huffingtonpost.in/2018/09/11/uidai-s-aadhaar-software-hacked-id-database-compromised-experts-confirm_a_23522472/
Zack Whittaker, "Indian State Government Leaks Thousands of Aadhaar Numbers," *TechCrunch*, January 31, 2019, https://techcrunch.com/2019/01/31/aadhaar-data-leak/.

142 Ramanathan, Usha. "Coercion and Silence Are Integral Parts of the Aadhaar Project." *The Wire*, May 16, 2017. https://thewire.in/economy/coercion-aadhaar-project-ushar.

143 "The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits, and Services) Act, 2016," § 57 (2016), https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

glaring incursion on a person's privacy.[144] Shortly thereafter, the government tabled the Aadhaar and Other Laws (Amendment) Bill, 2018, in the Indian Parliament, which would allow private entities to use Aadhaar for voluntary verification purposes. The Bill was reintroduced after the general election in the country and passed by the Rajya Sabha (upper house of the Indian parliament) in July 2019. The constitutionality of such a provision is being questioned by rights advocates as it still allows private entities access to sensitive personal data of Indian citizens.[145]

4. Given the relative nascence of India's digital economy, the processing of user data has primarily been carried out by foreign internet companies such as Google and Facebook. As of 2020, Google's mobile operating software, Android, had a 95.73% market share in India.[146] As stated earlier, Facebook had 328 million users.[147]Comparatively, Paytm had approximately 39 million monthly users in 2020.[148] Only Indian telecommunications companies demonstrate comparable numbers of subscribers to the U.S. tech behemoths. However, as stated earlier, telecommunications companies are restricted from disclosing surveillance requests by both the Telegraph Act as well as their licenses. However, they may be able to quantitatively report on requests that are not legal per se as they are only required to maintain confidentiality around affairs related to *legal* interception. As such, it may be possible for the DoT to issue a policy surrounding transparency of telecommunication surveillance, under which the Telecom Regulatory Authority of India may prescribe the manner and form in which disclosures may be made. Additionally, as stated above, any request made by a judicial officer under Section 92 of the CrPC may be disclosed, provided the matter is disposed of.

Despite these challenges, there have been some efforts by Indian companies to provide greater transparency and accountability around their management of user data. In June 2019, Sharechat, an Indian social media company, issued its first transparency report. Although this report is not as exhaustive as the transparency reports produced by U.S. companies, it is a step in the right direction. In terms of surveillance-related data, Sharechat's report broadly details the number of government requests for user data that have been submitted, broken down by state. Sharechat also explains that in instances where it shares user data with the government, it only shares the mobile number an individual used for registration, the device type, IP address, and in certain cases, chat history. In comparison to reports issued by U.S. companies, however, Sharechat does not share vital information such as the legal reasons for requests received. Further, Sharechat's report only discloses data related to requests that are in the public interest. As mentioned earlier, these disclosures are legal as they pertain to Section 91 requests or requests made by agencies under statutes that do not encompass any express prohibition on the publication of such information. Given existing restrictions around data disclosures, however, it is unlikely that Sharechat will be able to expand its reporting further. Nonetheless, Sharechat's report is a valuable first step towards providing greater transparency and accountability around how the company manages and shares user data with the Indian government.

The reporting requirements in the IT Rules 2021 require larger intermediaries to publish content takedown requests are a further step in the right direction. Most major internet companies such as Google and Facebook have been publishing this data for some time now[149]. However, the mandate will go a long way in encouraging Indian companies to be more forthcoming about content takedowns on their platforms.

---

[144] Justice K.S. Puttaswamy and Anr. vs. Union of India and Ors. (Supreme Court of India September 2018).

[145] Vrinda Bhandari, "Why Amend the Aadhaar Act Without First Passing a Data Protection Bill?," *The Wire*, January 4, 2019, https://thewire.in/law/aadhaar-act-amendment-data-protection.

[146] "Stat Counter: Global Stats," August 2020. https://gs.statcounter.com/os-market-share/mobile/india.

[147] Wasia, "Facebook brings its A-game to India".

[148] Maji, Priyadarshini. "More Indians Visit Paytm than Google Pay and PhonePe Put Together: Report." Financial Express, June 25, 2020. https://www.financialexpress.com/money/more-indians-visit-paytm-than-google-pay-and-phonepe-put-together-report/2003638/#:~:text=convenient%20for%20users.,Paytm%20witnessed%20a%20surge%20in%20new%20users%20and%20merchant%20partners,to%20%24135.2%20billion%20in%202023.

[149] Google, "Government Requests to Remove Content: India", https://transparencyreport.google.com/government-removals/by-country/IN.

Hopefully, as privacy and transparency become increasingly important commercial imperatives, more Indian companies will follow suit and begin issuing at least limited, legally-permissible reports.

Hopefully, as privacy and transparency become increasingly important commercial imperatives, more Indian companies will follow suit and begin issuing at least limited, legally-permissible reports. In addition, going forward, the government should relax legal restrictions around data disclosures to at least permit companies to report aggregate data on the scope and scale of government requests for user data they receive, what laws govern the requests they receive, and what the company's compliance rates with such requests for user data are.

Another positive development in terms of corporate transparency is that the 2019 PDP Bill calls for a data auditor appointed by India's Data Protection Authority to audit the conduct and policies of entities that process data in India[150] and ensure they adhere to their statutory obligations.[151] Based on this evaluation, the data auditor will assign a data trust score to these entities, who must subsequently share these scores with the Data Protection Authority. However, the criteria for such a rating system has not yet been established or shared publicly.[152]

A data audit is a welcome procedure, and if performed correctly, it could provide transparency around how businesses in India handle user data. However, it is still uncertain whether an entity's data audit report or even its data score will be made available to the public, and how the results of the data audit will be utilized to incentivize change and improve privacy and security standards. The 2019 PDP Bill does outline that entities undergoing audits are required to share information related to their data trust scores, a rating given to it by the Data Protection Authority based on the audit, according to prescribed regulations. Such disclosures shall presumably be made to the data principal although the Bill does not explicitly state this. However, these regulations have yet to be developed, and, as a result, it is difficult to ascertain whether this audit process will truly be able to provide greater transparency around how companies manage user data, particularly in relation to government requests for such data.

U.S. civil society organizations and advocates can offer some valuable lessons to their counterparts in India when it comes to pushing for corporate transparency around government surveillance efforts. In the United States, these advocates have been particularly successful because they were able to outline the importance of adopting transparency-related principles for companies (e.g., as a mechanism for building user trust in an environment where users are generally wary of corporation's relationships with the government). These groups and individuals prioritize engaging with large companies that hold significant influence and user bases, and that are likely to be able to successfully lobby the government for change.

In addition, advocates in the United States made a strong case for adopting transparency reporting by capitalizing on major crises that demonstrated the need for corporate transparency around managing user data. This first crisis was sparked by growing scrutiny around how Google was handling requests from the Chinese government for user data. This pushed Google to begin issuing transparency reports. The Snowden disclosures further pushed technology companies to provide more transparency around their handling of user data.[153]

Additionally, the previously mentioned scandal surrounding Paytm's data sharing practices is an example of a crisis that could have been harnessed to advocate for change in India. Further, the ownership structures of many of Indian technology companies pose a significant national security risk. Specifically, the Chinese government (or Chinese companies) have a significant stake in many top Indian tech companies. For instance, Chinese e-commerce giant Alibaba has a 40% stake in Paytm. The data sharing practices of these entities, then, must be subject to greater public scrutiny. While the exact information requested by government authorities need not be disclosed, the number of requests can be made public without jeopardizing national security interests.

U.S. technology companies can also offer valuable lessons to their counterparts in India, especially around how to press for changes to the law to permit

[150] "*Personal Data Protection Bill*, 2019," § 29

[151] *Personal Data Protection Bill,* 2019, S. 29.

[152] *Personal Data Protection Bill*, 2019, S. 29.

[153] Bankston, Schulman, and Woolery, *Getting Internet*.

transparency reporting. At the very least, the transparency reports of U.S. companies which cover India can serve as a guide for what is legally permissible for Indian companies. As previously discussed, the Snowden disclosures outlined the extent of U.S. government surveillance and put technology and telecommunications under the spotlight for their role in aiding these surveillance efforts. Subsequently, these companies pushed the U.S. government to let them publicly share more information regarding the number of government requests for information they were receiving, partly to reassure consumers that despite large numbers of government demands, only a small percentage of their users were actually affected. This demonstrates that when companies, particularly large industry players, recognize the value of a certain practice, such as promoting transparency and accountability around surveillance, they can join forces with advocates and push for the government to permit change. This is a vital lesson that advocates and companies in India can learn from, as it creates a two-pronged advocacy strategy that has proven results in other countries.[154]

The potential formation of an Executive Agreement between the United States and India under the CLOUD Act could also help make corporate transparency reporting an industry-wide best practice in India. If transparency reporting is instituted as a legally permissible stipulation for both countries, it will not only augment insight around the rather opaque cross-border surveillance efforts of both nations,[155] but it could also sew the seeds for the institution and expansion of transparency reporting as a government and corporate practice in India in general. Thus far, companies such as Microsoft[156] and Dropbox[157] have supported this notion. Further, as previously outlined in order for the United States and India to establish an Executive Agreement, India would have to establish a minimum threshold for privacy and security of user data and the U.S. government would have to certify that India meets specified standards for safeguarding human rights such as privacy. This could create a valuable opportunity for the U.S. government, and advocates for privacy and security in the United States and India, to push for the adoption of more rights-respecting standards in India. The existing frameworks in place in the United States, although not perfect, could serve as guiding frameworks during this process.[158]

[154] Bankston, Schulman, and Woolery, *Getting Internet.*

[155]Madhulika Srikumar, "Sharing Data Across Borders," *The Hindu*, April 3, 2018, http://www.thehindu.com/opinion/op-ed/sharing-data-across-borders/article23417587.ece.

[156] Brad Smith, "A Call for Principle-Based International Agreements to Govern Law Enforcement Access to Data," *Microsoft Blog*, entry posted September 11, 2018, https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/.

[157]Bart Volkmer, "The CLOUD Act Passed: What's Next," *Dropbox Blog*, entry posted April 12, 2018, https://my.noodletools.com/web/bibliography.html.

[158] For an approach that helps bridge the gap between the lack of safeguards in India and stipulations in the CLOUD Act, please see: Sreenidhi Srinivasan et al., "INDIA-US DATA SHARING FOR LAW ENFORCEMENT : BLUEPRINT FOR REFORMS," 2019, https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf.

RECOMMENDATIONS

As discussed in this report, both the United States and India operate vast and complex surveillance programs, which were borne out of different contexts. In the United States, the legal authorities that govern surveillance efforts arose following a period of unfettered surveillance operations prior to the 1980s. Following the September 11, 2001, terrorist attacks and the enactment of the PATRIOT Act in October 2001, these legal authorities were further expanded. India's surveillance system, on the other hand, was largely the product of the legacies of colonialism, and has since been expanded upon based on desires by the state to monitor and exercise greater control over the citizenry. In the United States, debates around the privacy and security of users and their data have been more longstanding, and as a result, there are more established government and corporate transparency frameworks and practices which provide some limited accountability related to government surveillance efforts. Despite an enduring tradition of broad government powers for surveillance, India, on the other hand, only recently began grappling with rights-related issues. As a result, existing transparency and accountability frameworks in the country are comparably weak.

Below are recommendations for how the U.S. government, Indian government, and companies in both nations can provide greater transparency and accountability around surveillance efforts going forward.

The Indian government should:

1. **Enact a comprehensive statute in line with the International Principles on the Application of Human Rights to Communications Surveillance to balance surveillance powers in India against safeguards around user rights.** This statute should be used to provide greater transparency and accountability around the Centralized Monitoring System as well as create a mechanism for judicial and public scrutiny of such activities. In the interim, however, the government should publish quantitative information of surveillance requests made under both the Telegraph Rules as well as the Information Technology Rules in an act of good faith towards the citizens of the country.

2. **Publish granular data on surveillance-related requests made under the Telegraph Rules, telecom licenses, and the Information Technology Act, 2000.** In order to provide greater transparency and accountability around its surveillance operations and build citizen confidence, the Indian government should at a minimum publish aggregate quantitative data related to its surveillance operations, including the aggregate number of government requests for user data it has submitted to private companies. This data should be broken down by industry in order to outline which industries are being approached for access to user data and to demonstrate what kinds of user data law enforcement authorities are seeking/obtaining access to.

3. **Provide greater clarity and transparency around the data audit process outlined in the 2019 PDP Bill:** If conducted and implemented well, the data audit process outlined in the 2019 PDP Bill could prove to be a valuable method for providing transparency around how businesses in India manage user data. Going forward, the Data Protection Authority of India should provide greater clarity around the auditing process, including what the criteria for evaluating are. Further, the results of the data audit reports as well as companies' data trust scores should be shared publicly, in order to allow for public scrutiny of these companies' efforts and of the audit process as a whole.

4. **Restore independence of the Information Commissioners under the RTI Act:** The right of a citizen to seek information on how the government is functioning is an inexorable component of democracy. Elected representatives and the bodies of government operating under them must maintain a high level of transparency in governance to bridge trust deficits that may arise in society due to the opacity of executive or legislative decisions**.** Part of ensuring that trust is also retaining the independence of the officers charged with providing information to citizens on the workings of the state.

5. **Halt data localization and mirroring efforts:** Localization and mirroring do little in the way of ensuring security of data, particularly if standards for security are absent as mentioned before. As such, the government may have to reconsider the localization mandate altogether under the 2019 PDP Bill.

The U.S. government should:

1. **Utilize the CLOUD Act to push for better privacy and security standards in India:** The CLOUD Act requires any nation that the U.S. forms an Executive Agreement with to meet specified standards for safeguarding human rights such as privacy. As outlined, India does not currently meet these requirements and would have to introduce a new set of standards to do so. As the U.S. government considers forming an Executive Agreement with the Indian government, it should use this deliberation process to encourage the adoption and implementation of rights-respecting principles and practices, including transparency reporting. The U.S. government should engage and tap into the expertise of both U.S. and Indian civil society to support these efforts.

2. **Introduce significant surveillance reforms that include robust safeguards for privacy and civil liberties:** As outlined, a number of policymakers in the United States and around the world, as well as a broad swath of U.S. civil society organizations view the current surveillance system in the United States as broken. Policymakers in the United States should institute robust and comprehensive surveillance reforms that ensure surveillance operations are focused on "legitimate and appropriate targets," include strong safeguards for privacy and civil liberties, and encourage transparency.

3. **Provide greater transparency around FISA-related surveillance efforts to the public:** Current government transparency efforts related to the use of FISA authorities for surveillance primarily involve sharing classified and sensitive information with U.S. Congress. However, none of the information in these reports are disseminated to the public. Going forward, the government should provide greater transparency and accountability to the public around FISA operations by increasing the amount of this information that is available to the public. This information should include disclosures related to how FISA has been used to collect information on U.S. persons.

4. **Permit U.S. companies to disclose more granular information related to U.S. government surveillance activities and requests:** Currently, U.S. companies are permitted to report on national security requests they have received in numerical ranges. These numerical bands are arbitrary and hinder efforts to provide meaningful transparency and accountability around the scope and scale of U.S. government requests to U.S. companies. At the very least, these bands should be narrowed to offer more transparency to users. But further, the U.S. government should grant companies the authority to publish more granular statistics, which would paint a clearer picture of the number of national-security related requests technology companies receive.

5. **Publish a comprehensive and public report outlining how FISA surveillance activities have been used to target racial minorities and other protected groups, as well as First Amendment-protected activities:** This report should examine how FISA surveillance efforts have been used to target individuals based on their membership in a protected class or based on whether they are exercising their First Amendment rights, and what impact these surveillance operations have had. The PCLOB should publish this report, regardless of a Congressional mandate.

6. **Explain how the expiration of Section 215 of the PATRIOT Act and the roving wiretap provision and lone wolf authority under FISA have impacted surveillance operations:** Transparency around how the expirations of these provisions have impacted surveillance efforts will provide greater accountability around if and how intelligence agencies are using alternative surveillance mechanisms for data collection. Further, this transparency will allow for more informed policymaking, particularly around future surveillance reforms.

Internet platforms and telecommunications companies based in India should:

1. **Partner with civil society organizations and advocates to push the government to relax restrictions around voluntary corporate data disclosures:** The current legal restrictions around what surveillance-related information businesses can disclose create significant obstacles for companies seeking to provide adequate transparency and accountability around government surveillance efforts. Going forward, technology and telecommunications companies in India should collaborate with civil society organizations and advocates to push the government to relax the restrictions around data disclosures. At a minimum, the Indian government should permit companies to voluntarily report aggregate data on the scope and scale of government requests for user data they receive, what laws govern the requests they receive, and what the companies' compliance rates are.

2. **Publish clear and accessible information explaining how they manage user data and what their policies for sharing user data with the government are:** These policies should explain in detail the cases in which a company would share user data with the government, what kind of user data the company can share, what laws the company submits user data under, how the company evaluates requests for user data to ensure they are appropriate, and when the company pushes back on incomplete requests. These policies should be easy to access on a company's website and should be written in plain language that is digestible for the average user.

Finally, in the absence of stronger frameworks for transparency reporting in India, U.S. internet platforms and telecommunications companies should:

Publish more granular data related to government requests for user data in India: U.S. companies could, for example, report on the specific Indian laws that were used to make requests and which of a company's products received these requests. In doing so, U.S. based companies can help partly fill the transparency gap that exists around government surveillance efforts in India. Given that many U.S.-based companies have large user bases in India, an expansion of their transparency reporting data in this regard could help safeguard millions of users' rights.

SUMMARY OF RECOMMENDATIONS

Indian government	1. Enact a comprehensive statute in line with the International Principles on the Application of Human Rights to Communications Surveillance to balance surveillance powers in India against safeguards around user rights.
	2. Publish granular data on surveillance-related requests made under the Telegraph Rules, telecom licenses, and the Information Technology Act, 2000.
	3. Provide greater clarity and transparency around the data audit process outlined in the 2019 PDP Bill:
	4. Restore independence of the Information Commissioners under the RTI Act
	5. Halt data localization and mirroring efforts.
U.S. government	1. Utilize the CLOUD Act to push for better privacy and security standards in India
	2. Introduce significant surveillance reforms that include robust safeguards for privacy and civil liberties
	3. Provide greater transparency around FISA-related surveillance efforts to the public
	4. Permit U.S. companies to disclose more granular information related to U.S. government surveillance activities and requests
	5. Publish a comprehensive and public report outlining how FISA surveillance activities have been used to target racial minorities and other protected groups, as well as First Amendment-protected activities
	6. Explain how the expiration of Section 215 of the PATRIOT Act and the roving wiretap provision and lone wolf authority under FISA have impacted surveillance operations.

Internet platforms and telecommunications companies based in India	1. Partner with civil society organizations and advocates to push the government to relax restrictions around voluntary corporate data disclosures.
	2. Publish clear and accessible information explaining how they manage user data and what their policies for sharing user data with the government are.
Internet platforms and telecommunications companies based in the U.S.	Publish more granular data related to government requests for user data in India.

CONCLUSION

Over the past decade, government surveillance efforts in the United States and India have increasingly come to rely on the user data collected by technology and telecommunications companies. In addition, the surveillance apparatuses of both countries are increasingly becoming intertwined, especially as the two nations explore bilateral partnerships in the technology space. As such, the two governments and companies within their respective countries must work to provide adequate transparency around ongoing surveillance operations and how they implicate user data. Meaningful transparency in this regard can augment accountability and inform ongoing dialogues around appropriate surveillance safeguard as well as bilateral partnerships.


NEW
AMERICA

OPEN
TECHNOLOGY
INSTITUTE

ESYA
centre