**Annotated Timeline**

Timelines are chronological devices, giving the impression of progress. Yet, the timeline of events that we curate here is less to depict a story of progress or disrepair, and more to portray a snapshot of defining moments in the public life of the digital encounters that we trace in this book. These moments appear in the form of letters, court judgements, plans and policies, working together with the archive, provide something of a window into the key problems that motivate this book. They coalesce around the total and unprecedented re-organization of social and political life that has been mediated by digital technologies. Every event in this timeline thus points to an upheaval in the order of things, producing new problems in the world, and, for us, new opportunity to excavate the life-worlds of techno-political interventions.

Consider this timeline a roving flashlight then, selectively illuminating the torrid twenty years of digital governance and its prequel. It is not intended to be comprehensive. It is a curatorial accompaniment to the text, showcasing our authorial choices, our reading of the past. It is at the same time an invitation to readers to unpick up these moments, chart their own genealogies and, of course, to add to them. Some interventions are more well-known than others. The lesser-known ones are equally critical to our story of why the past twenty years need the attention and space this book offers.

**1975: The National Informatics Center (NIC) is set up.** An institution that brought irreversible change to the information generating and organizing capacities of the government, the NIC was set up under the Department of Electronics to digitize government offices. NIC’s founder Narasimhiah Seshagiri developed an internet before the Internet to create a distributed network of information sharing offices. In many important ways, this book (and the third essay in particular) tracks the excesses of this pioneering ambition.

**1976: Jaswanth Krishnayya’s May 15 1976 *aide memoire* to the Planning Commission on setting up ‘information systems and a computerized data bank’**. A systems thinker, Krishnayya may be considered as a prototype of today's ubiquitous management consultant of the sort dotting government offices. But, as is revealed in this defining letter, Krishnayya wasn’t just purveying technology to the civil servants of India’s Planning Commission. He was offering a paradigm shift, an ontological change in the information gathering and organizing model of government, a vision that game to define the material transformation in the sinews of government. This is a rare opportunity to glimpse the thought-work that accompanied digital change, something that is lost as technology interventions become more ‘plug and play’ in the decades to come.

**1984: New Computer Policy of the Department of Electronics**. One ofRajiv Gandhi first decisions on taking over Prime Ministership was to afford special status to the information technology industry, laying the foundations for the famous IT revolution a decade later. The New Computer Policy included reduced import duties for peripherals, foreign equity participation, liberalized import of computers and recognition of software as a separate industry, setting up the informational infrastructure that forms the background in this book.

**1998: Launch of the Simputer by four scientists from the Indian Institute of Science**. This was low-cost, smart-card-compliant, handheld end-user device using the IMLI (or ‘information mark-up language interface’) on a touchscreen intended to revolutionise a digital grassroots in India. According to Vijay Chandru, one of the four founders, it was imagined alongside two other equally revolutionary inventions, one, the Wireless-in-Local-Loop (WLL) technology set up in 2001 as part of the SARI (Sustainable Access in Rural India) project of Ashok Jhunjhunwala at the Indian institute of Technology, Chennai, often seen as the moment when mobile telephony took root in India, with kiosks providing telephone, Internet and other stand-alone computer services to villagers, and in 2002 of computational linguistics with the Language Technologies Research Centre at the Indian Institute of Informational Technology. Together, these were going to be the technologies for democratizing information in India.

In many ways, the problems of the Simputer were not hardware or design problems. They were, rather, that the digital ecosystem – like Aadhaar, for instance – had not yet been built. They were a cog without a wheel, without a system to support it. The Simputer nevertheless proved to be a key antecedent to complex e-governance systems, anticipating a complex legal ecosystem including, for example, the draft Personal Data Protection Bill, 2019.

**1999: DISNIC-PLAN, A NICNET Based Distributed Database for Micro-level Planning.** The first attempt to connect offices and introduce real time relay of data from the 200+ districts of India to the headquarters of the Planning Commission in Delhi. This was a distributed database, pre-empting relational database management systems. This book has explored the geography of this network, as it aimed to make data mobile and yet curtail its movement by mirroring the hierarchical structure of government. Debates around the localization of data, which is referenced across the chapters of this book, are reminiscent of this pioneering model of containing data within the geography of the district.

**1999: New Telecom Policy.** NICNet, established by the National Informatics Centre in 1995, as an inter-operability platform between government institutions, was also accompanied by the availability of the first public Internet service on 15th August 1995, by the Videsh Sanchar Nigam Limited (VSNL). In 1999, the New Telecom Policy spelled out Universal Services as among its main objectives, leading to India becoming a signatory to the USOF (Universal Services Obligation Fund), receiving funds to encourage universal access. In 2003, the USO was given statutory status, and in 2004 the Broadband policy act further consolidated the idea that digital connectivity is a fundamental right. It is important to emphasise that the history of universal access is and should remain central state responsibility, and that the current idea of universal access as administered by private telecoms, as in the partnership with Reliance Jio or the backdoor negotiation with Free Basics are an abdication of state responsibility to offer universal access and obligatory services.

**2000: Information Technology Act passed.** Although a technological regulation document, this Act is clearly an origin point of cultural and political expressions of technology. Throughout the book, across the essays, the different conditions of access, expression, speech, security, and integrity keep on drawing from this earliest historical document about regulation of the Internet. See especially its Section 3 on Electronic Governance, its licensing structure for electronic certification, its Section 43 announcing draconian penalties for ‘computer contaminants’, its cyber-regulation structure, its section 66 that brought the concept of ‘hacking’ for the first time into legal terminology, its emphasis on ‘sovereignty and integrity of India’, and finally its outlining of ‘service providers’ and their accountability. Subsequent annotations and amendments merely reinforce the centrality that ICTs have gained in imagining the apparatus of a digital India. It is important to trace many of the cultural, organisational, and bureaucratic events back to this Act that sought to contain and control the then emerging Internet networks.

**2003: The revised Citizenship Amendment Act**. This is the Act that first conceives theRules on Registration of Citizens and Issue of National Identity Cards that would become the National Population Register. The 2003 Rules were the first time when a ‘Local Register of Indian Citizens’ was defined, when ‘individuals whose Citizenship is doubtful’ would be weeded out. It was also the first time that illegal migrants or foreigners become central to defining citizenship.

**2005: The Right to Information Act.** This Act, though not quite about the digital technologies or infrastructure is critical in understanding the expectations and the ambitions of building a nation-wide internet infrastructure. RTI forced the government to recognise digital platforms as the only way of giving access to public information, thus precipitating massive digital reforms and e-governance initiatives in the very working of governments. It also suddenly changed government bureaucracy, replacing older structures with several new agents, using database logics to produce new interfaces and transactions for spreading of information. The institution of RTI also led to concerns around privacy, because a non-discrete scrutiny of public information could, it became apparent, lead to adverse consequences for those who had not consented for their data to be used beyond a particular context.

**2006. The Personal Data Protection Bill.** ThePDP, introduced to the Rajya Sabha in 2006, was the first recognition of the unregulated nature of personal data online. The Bill significantly anticipates and identifies the ways in which personal data can be harvested, consolidated, and often weaponised against users, in ways both unpredictable and uncontrollable. Ironically the PDP Bill was targeted at private use of citizen data but did not pose any questions to the state’s own ambitions of data surveillance and extraction. Thus, the most vulnerable data subjects – the YOUsers caught in the matrices of digitalisation – remained without agency and understanding of what happens to their data and how it can be used against them.

**2006. National E-Governance Plan** An ambitious and multi-pronged plan to digitize various facets of governance, radically re-imagining the location and scale at which government would operate. Aadhaar (see below) might be its most experiential and controversial project, but the plan, as a whole, marshalled a new technological architecture that included service centre nodes, fibre-optic networks and stable data centres. The NeGP, as it came to be known, offers some of the best instances of RDBMS-led datafication of government, and is frequently upgraded with new ways of reconfiguring service. It is thus a historical index to track the development of techno-legal mechanisms for the practice of government and the re-figuration of the individual as a citizen-recipient.

**2006**. **Orkut’s multi-lingual Indian iteration**. Themoment of the introduction of social media in India. Within the next four years India had 83 million internet users, sixty percent of whom had some kind of social media existence. Although Orkut led the way it would have a short shelf life, being replaced within two years on the frontlines by Facebook.

**2007: RSBY (Rashtriya Swasthya Bima Yojana, or National Health Insurance Scheme) announced as a cashless Mediclaim for the poor.** One of the first experiments to convert the slew of Centrally Sponsored Schemes to move to the cashless system, this health insurance system for the poor was imagining over multiple financial gateways of e-commerce and payments. It also introducing the idea of digital money to a largely disconnected population. A history of the Internet in India is also perhaps the history of shaping the image of the benefactor, and experimenting in their onboarding onto the Internet by shifting their basic services online, as we have seen both in the case of demonetization as well as Aadhaar.

**2008: Amendments to the IT ACT – the presentation of cyber security.** These amendments primarily addressedcyber-security. The first conversations around data transfer and safety, for which the 2004 Delhi Public School User Generated Pornography case was a central marker, resurfaced and found a resolution in these amendments. Of particular interest for this book are the sections that look at cyber-security, not in terms of keeping users safe but to keep data safe *from* users, and from their ability to corrupt, steal or manipulate digital data. The legacy of controlling users in order to keep the technologies safe, unfolds in many of the cases in this book, including ‘Whatsapp Lynch Mobs’ – where social media platform, ascribed both responsibility and accountability, in turn starts a ‘user literacy’ campaign to control user behaviour. Cyber security is critical also because it began allowing dissident voices to be examined from a national data security lens, bringing in new layers of control and silencing.

**2008: Second Administrative Reform Commission, Eleventh Report, Promoting e-Governance.** Another landmark in the turn towards datafication of government. Dedicating an entire report to electronic governance at the same time as the appearance of the NeGP (see above), suggests not just a firm resolve to a digital transition, but also the digital reform of Indian administration as a whole. E-governance became a relay point through which corporate and managerial idioms of transparency and efficiency, would shift from government to governance. It followed a series of financial crises during the late 1980s, and now planned for a new organizational structure that would shrink bureaucracy to the backend, foregrounding instead new bridges between service centres and clients. A managerial ideal of heightened efficiency suggested not so much a transformation as a transcendence of politics.

**2009**: **Launch of Aadhar**. In February of this month, the Unique Identification Authority of India (UIDAI) was started, initially within the Planning Commission, with former Infosys co-founded and CEO Nandan Nilekani in charge. A year earlier Nilekani had published his book *Imagining India: Ideas for the New Century*, which had laid out several of the revolutionary concepts around portable and bodily identity for every Indian resident, that he would now be tasked with implementing. The first UIDAI Working Paper, *Creating a Unique Identity for Every Resident in India*, effectively outlines a new biopolitical definition of residency, by ensuring repeatedly that the Aadhar number would be itself a dumb number containing no intelligence; it was not an identity card; and it was portable.

**2009: DoT issued blockage of porn websites.** Pornography has been one of the poster children for Internet regulation. The Department of Telecommunication’s continued attempts at blocking porn and censoring ‘obscene content’ has continually been rebuffed, and has never quite worked. The 2009 blocking of porn websites was the first national attempt that showed the inefficacy of content filtering online, and also the power of distributed content networks which could easily surpass the different content filters, as is discussed in the case of the Savita Bhabhi controversies. In many ways, the failure at content filtering and censorship can be seen as the trigger point for the government mediators to start looking at other forms of information shaping which lead to the reliance on Internet shutdowns and information blackouts as blanket strategies for blocking and censoring information.

**2011: Intermediary Liability Act**. A major moment inthe arrival of new telecom companies as performers of state-like activities, this Act. saw a new tacit arrangement of the public and the private in which social media platforms, made liable for the actions of their users, got enfranchised as independent and autonomous bodies of governance with Terms of Service taking precedence over independent judgements on censorship and agency. Not only did this produce a chilling effect, as self-censorship and arbitrary blocking became common, but it also registered new ways in which these companies began to lobby for and shape the future of the Internet, as in the Free Basics campaign and the fight to retain Net Neutrality. The Intermediary Liability Act also needs to be recognised as the precursor to the regimes of Internet blackouts and shutdowns, and disconnection which superseded the safeguards against censorship in older media technology regulations.

**2015: Digital India campaign launched**. Majorinitiative rhetorically linking digital technologies with national identity. Like many countries that have become production and service hubs for global IT industries, this campaign was focussed on the economic wealth that global outsourcing can bring the country. Digital India started ostentatiously, as an economic alliance and collaboration building project, but it also suggested a new kind of intentionality on the part of the state. Activities that were seen to be using digital technologies to disrupt, question, or challenge the overt intentionalities of development and economic wealth-creation, were seen as problematic and even traitorous (threatening to the ‘security and integrity of India’). This extended to arrests of activists, institutional prohibitions including harassment of digital groups demanding social justice, and governmental crackdowns on dissenting voices and communities.

**2015: The landmark ‘Shreya Singhal’ judgment**. A second-year law student, outraged by the arrest of two young women for putting up (or simply ‘liking’) Facebook posts, challenged the draconian section 66A of the Information Technology Act, and won. That amendment, which had taken direct aim at social media in threatening imprisonment to anyone sending ‘information that is grossly offensive’ or ‘causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will’ via ‘a computer, computer system, computer resource or communication device including attachments in text, image, audio, video and any other electronic record’, was struck down by the Court. However, the Court retained the equally draconian 69A that authorized the government to block any information ‘in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence’. A growing split in the two halves of the ‘reasonable restrictions’ on the right to free speech became increasingly clear, defining the uses of the Unlawful Activities (Prevention) Act and the conditions under which preventive detention began to be used.

**2016: Prohibition of Discriminatory Tariffs for Data Services Regulation.** India does not have any specific legislations regarding Net Neutrality. However, in 2016, the Telecom Regulatory Authority of India (TRAI) passed this new regulation after public consultations about the regulatory framework for Over-the-top (OTT) services. This effectively makes net neutrality a fundamental right and aligns India with many other countries that seek to keep the Internet services neutral and agnostic to the kinds of use and user. This regulation came into effect because of the ways in which private corporations (Airtel in 2014, Free Basics in 2015) were trying to fork the Indian Internet into basic and luxury services, intending to create a multi-tier userbase with differing advantages and services.

**2016: The India Stack takes shape**, taking Aadhar into a new era of ‘presenceless, paperless, cashless and consent’, with the launch of United Payments Interface (UPI), catapulting India into the age of digital payments. UPI works on increasingly integrating the banking system with a real-time mobile payments system, to to enable interoperability between money custodians, payment rails and front-end payment applications. Aadhar’s API is increasingly made available to build larger numbers of apps.

**2017 – K.S. Puttuswamy Judgment on the right to privacy**. In asserting such a right, the Supreme Court came up with several new conceptions of the biopolitical subject, now defined as a ‘natural person’ who possesses a bodily right to privacy, which is ‘a natural right’ and ‘inalienable’. It was also at the same time transactable, thus laying the foundations for data exchange and commodification. It is an underlying current through this book that the regulation around data privacy and data security also contribute to the regimes of data surveillance and data capitalisation by enforcing data as discrete computational set that create the user in what we are calling a YouSer.

**2017: Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017, amendment to the 1855 Telegraph Act.** Section 144 of the Code of Criminal Procedure (CrPC) allows local magistrates to direct properties like cellphones and mobile towers to be used in specific ways. The PAAS agitations in Gujarat was the first time that the Internet telecommunication was included under this, and infrastructure regulation was used as a way of information spreading. This was challenged in court and eventually, in 2017, the Telecom Internet Suspension Rules were formulated and codified as a part of the Telegraph Act, which made it possible for Internet shutdowns to be normalized, making India top the lists of the longest and largest number of Internet shutdowns in the world. Under the Telegraph Act amendment, shutdowns are often seen as modes of limiting speech, but its origin in the CrPC is a stark reminder that this is an infrastructure shaping that curtails free speech and a new form of censorship and control through infrastructural development.

**2018: K.S. Puttaswamy Judgment on Aadhar**: the landmark judgment on the validity of the Aadhar Act is best remembered for Justice D.Y. Chandrachud’s dissenting judgment. While the Act was passed, Chandrachud outlined a grim picture in which, for all the emphasis on privacy and data protection, when rights that are ‘freely exercised, liberties freely enjoyed, entitlements granted by the Constitution and laws’ become *‘*conditional, on a compulsory barter’, then the ‘barter compels the citizens to give up their biometrics ‘voluntarily’, allow their biometrics and demographic information to be stored by the State and private operators and then used for a process termed ‘authentication’’. It also allows for an extraordinary ability of the state to perform ‘civil death’ through turning off a digital resource at will.

**2018: M/S United India Insurance… vs Jai Prakash Tayal (26th Feb 2018).** A case on genetic data privacy and the weaponization of individual genetic data became an unlikely focal point to connect technological data and biological data to ensure protection for the individual. Digital data is often seen as discrete and separate from the embodied user that it refers to and, in this judgement, data (digital or otherwise) was established as intrinsic to the privacy and integrity of a person. The establishment of data as thus fundamental to personhood, leads to interesting questions around bodily security, safety, and individual safety in the face of continued data leaks and instances of trolling and doxing online. It perhaps can be seen as the first recognition of a Youser – a combination of multiple data streams – and its negotiations with agency and autonomy in the complex field of data regulation and security.

**2019: Personal Data Protection Bill based on the committee recommendations led by Justice B.N. Srikrishna**. Itcontains the government of India’s most recent response to the kinds of data overload, creep and excesses that this book aims to document. It sought to create a legal framework for the protection of personal data, through the creation of data fiduciaries and, more starkly, by proposing localization strategies to contain data within the geographic boundaries of the nation. In the ensuing public debate, some saw data localisation as an attempt to bring back the rule of law to our digital and datafied existence, whereas for others, this was an extension of the long arm of the state as a mode of surveillance or economic protectionism. Against the long-standing attempts by the government to secure data, starting in the 1970s, where the mobility of data was never compromised, this latest intervention suggests limiting the spread of data. As such, it is reminiscent of old information architectures that mapped data onto specific categories, such as the ‘district’. As far as government’s access to data is concerned, the situation has not changed much from the prior version of the Bill (see above), where the government continues to have unchecked access to public and personal data. As of the moment of completing this book, the Bill has been withdrawn and will be fundamentally redrafted.

**2019: Sabka Sath, Sabka Vikas, Sabka Vishwas** (‘The support of all, the advancement of all, the faith of all’). The slogan adopted by the Bharatiya Janata Party in 2019 has led to interesting socio-political and cultural arguments about who the intended ‘everybody’ is. The proposition of a ‘greater good for everybody’ has often been used to reinforce draconian authoritarian and surveillance practices, perhaps the most visible during the e-management of the covid19 pandemic in India. The idea that the greater good requires intrusive governance standards and that development becomes the ambition for all digitalisation also is used as justification for state generated crises like demonetization that led to a massive shift towards virtualisation of the financial ecosystem or extended lockdowns that isolated entire communities in the case of the abrogation of the constitution and reformulation of Kashmir, clearly show how the Internet is often used as a means of defining the greater good that fits specific political expressions of control and power.

**2019: The revised Unlawful Activities (Prevention Act)** specifically targetsindividuals as terrorists. A new kind of individual is born, alongside the ‘natural person’ and the ‘data principal’. Together with the further amendment to the Citizenship Act, now targeting Muslims with its own ruling that only migrants who entered India from ‘Afghanistan, Bangladesh or Pakistan… before the 31st day of December, 2014’ would be allowed if they ‘belonging to Hindu, Sikh, Buddhist, Jain, Parsi or Christian community’, and the National Register of Citizenship, this led to major protests across India, and especially in Delhi.

**2020 – Anuradha Bhasin vs. Union of India and Ors** The landmark judgement from the Supreme court upheld that blanket Internet shutdowns were constitutional breaches because they hampered the fundamental rights of self-determination, commerce, and freedom of speech and expression. It recognised the Internet has a central and non-optional infrastructure in contemporary acts of being and realising one’s citizenship and hence deemed Internet shutdowns illegal. It thus introduced the language of necessity and proportionality on to the regulation of the Internet infrastructure, and particularly Internet access. It also established that the Internet has a peculiar relationship with crises: It generates them and is also the tool for making interventions in times of crises, and that the very act of being online might be seen as entering a state of crisis. This is particularly critical to understanding that access to technology, which is often heralded as a universal right, is inherently suspicious and hence needs to be controlled with greater discretion, through public and private means, enabling both governments and private corporations to capitalise on different forms of Internet infrastructure regulation.

**2021: New Intermediary Guidelines and Digital Media Ethics Code “2021 Rules” establish two provisions for content moderation and regulation on the Internet in India: Rule 4(4) on Content Filtering Mandate and Rule 4(2) on Traceability Mandate.** The question of misinformation and conspiracy theories, accelerated by the supposition that all information is now subject to relative truth value, leads to these draconian principles. The Content Filtering Mandate overrides all end-to-end encryption and allows all digital content to be offered for review to authority. The traceability mandate emphasises the ‘real name’ principles that social media giants have already enforced on users, and ‘enables the identification of the first originator of the information on its computer resource’, thus implementing the 2009 Decryption Rules that allow authorities to request interception or monitoring of any decrypted digital information. These technological solutions claim to not compromise the K.S. Puttaswamy judgement that establishes the right of privacy as a fundamental right and allows new forms of information overload management tools and systems for the government. The monitoring of contemptuous comments, as in the case of the Agrima-Mishra controversy, or the prosecution of individuals who have made critical comments as in the case of Kanhaiya Kumar, were precursors to the establishment of these rules and show how these draconian measures are slowly leading to erasure of free-speech rights.