Lines in the sand: Digital India, ethical data practices and privacy

Tania Gupta

THE TOTAL NUMBER OF INTERNET users in India is said to surpass half a billion by 2018. Additionally, reports by The World Bank suggest that mobile penetration rates in many low and middle-income countries have crossed that 100% mark. In many such countries, including India, mobile phone subscriptions have outpaced developments in infrastructure, with many rural and inaccessible societies having more mobile subscriptions than instances of access to electricity. However, perhaps the most significant shift in nature of this rapidly growing Internet population is the profile of Internet users. Users in India are increasingly becoming older, more rural, more female, more mobile-led, and more vernacular. Given these statistics it comes with no surprise that some of the largest Internet and digital content companies are clambering for attention of individuals on three to six inch screens. India is one of the largest markets for social networking sites such as Facebook and LinkedIn.

Enter: Digital India

In the wake of the rapidly changing nature of Internet and mobile users, the Digital India project that many were anticipating is now here and amassing connectivity at an incredible pace. The Digital India project is an initiative by the Government of India, spearheaded by the Indian Prime Minister Narendra Modi, to provide electronic and digital access to Government services to citizens. The aim of this project is to improve internet connectivity, strengthen online infrastructure and digitally empower the country. Certain areas of the project are being supported by technology companies such as Google, Microsoft, Facebook and Qualcomm.

The project has three main tenets:

i) Digital Infrastructure as a utility to every citizen,
ii) Governance & services on demand,
iii) Digital Empowerment of citizens through services such as DigiLocker.

These tenets are driven by the principles of e-governance and providing a knowledge driven transformation of urban and rural Indian society. The aim is to leverage the role of the Internet as an enabling force, one that can encourage collaboration across industry, government, civil society and citizens as well as making information more openly available and accessible. Inherent in this project is a sense of ubiquity of digital technology and degrees of connectivity, access and literacy, more so, with India's rural and underrepresented populations.

This signals that societies have the ability to take great leaps towards ensuring the maintenance of basic human rights, and the bottom up development of communities through increased information access and sharing. Yet, as with Internet-connected devices and the data this technology has the ability to generate, the panacea comes with its own caveat in the form of concerns over privacy, data security and ethical media practices.

A nation of a billion cellphones: Digital India and privacy

However, the Digital India initiative is lacking in consideration for notions of personal data protection and privacy for individuals, organizations and civil society who stand to benefit from the project. There needs to be a deeper understanding of the compatibility of intellectual property law and privacy with traditional and local perceptions of privacy as we attempt to reinterpret them within the digital landscape. There is also the need to advocate for a more conscientious understanding of ethical media practices given implications of digitized forms of personal data and cultural artefacts that affect discussions of agency, representation, new forms of labor exchange, and attribution of economic value.

> "Privacy, as a concept, can be understood within the context of social interactions with technological devices"

Individuals operationalize the concept of privacy through the socio-economic norms that are built into the fabric of the societies and communities they are socialized into. While cultural norms determine how and why individuals required privacy, these notions seem to vary more strongly across socio-economic indicators such as income, gender and age. Social affordances built into the structure of the community influence the kind of information shared and exchanged. Additionally, the process of privacy management as a multi-mechanism process includes various verbal and non-verbal factors such as personal space, territoriality and conversational mechanisms to facilitate and control social interactions within the sphere of social affordances. These behavioral mechanisms are then used to regulate privacy and leverage information to maintain one's autonomy, identity and self-esteem. In its essence the overarching and reasonable expectation of privacy is a determinant of how individuals regulate their relationships within the community or a society.

Managing risks

Privacy, as a concept, can be understood within the context of social interactions with technological devices. Data is what it is because of its interpretation and it is the social construction. As a result, potential regimes for informational privacy and management must be envisioned as embracing these specific uses and interpretations. The following section suggests a model for sustainable management of privacy in the components of the Digital India project leveraging the principles of informational self-determination, and privacy by design.

Informational self-determination

The concept of the right to informational self-determination or self-determination over personal data was first defined by the German Federal Constitutional Court 1983. The concept was developed as an additional clause to the general right of privacy that was covered by the basic rights and guarantees of human dignity and personal liberty. Such a right grants every individual the right to self-determination over data that concerns in the individual. Such a right however, is limited by third-party interests, which may include criminal investigations, though the scope of what is lawful data collection without the consent or knowledge of the individual has not been fleshed out in principle. However, as recent discussions have shown that the possibility of having informational self-determination poses not significance. The argument of informational self-determination can be made with regards to the default entitlement over personal data, especially pertaining to data that concerns one's governmental or financial status. Default entitlements suggest that there is a legal entitlement and the further allocation of resources to exercise the ability to this legal entitlement.

However, the challenges emerge from the lack of such legal entitlements or resources to exercise them in countries such as India. While the concept of privacy does read out in national constitutions, these rights and processes are not drawn out in interpretations that are accessible to the larger society. Privacy laws exist, but are irrelevant in the discussions around data protection and informational privacy. When interpreted from the perspective of information as belonging to the individual,

notion of privacy can be instilled through the process of awareness, and education. Informational self-determination can be embedded into the social norms that drive informational flows by appeasing to the concept of privacy that is built into specific social norms. Information self-determination seeks to allow the individual to be empowered, recognize changes in the informational flow, and be able to self-regulate.

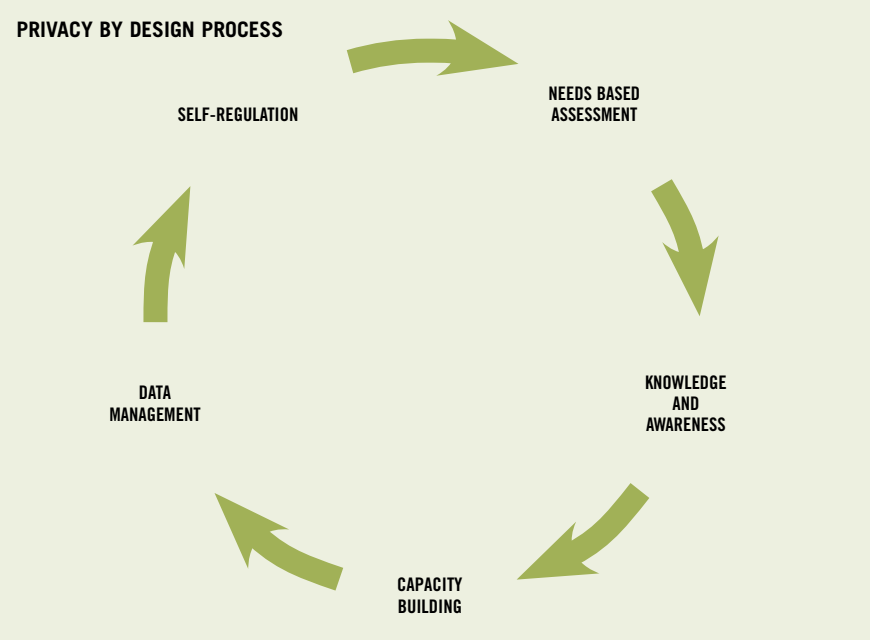
Privacy by design

Privacy by design is the approach that prescribes that privacy be built directly into the design and operation, not only of technology, bust also how a system is operationalized (e.g. work processes, management spaces, physical spaces and networked infrastructure). This approach has been envisioned through seven principles. The first two principles suggest that privacy by design be considered a proactive approach that takes into consideration privacy as a default in any technological process or operation. The third and fourth principles recommend embedding privacy into all possible aspects of the design. The fourth and fifth principles discuss providing end-to-end security, and visibility and transparency in the process of data collection, where as the seventh principle discusses making privacy management a user-centric approach.

Perhaps in the context of this analysis, all of the principles above culminate into the importance of providing a user centric approach to privacy management. Each of the seven aforementioned principles suggests a roadmap for the privacy and security component of the Digital India project. Simply stated, these principles allow for the conscientious inclusion of privacy within the design of the technology, but also more importantly, allow privacy to be built up from the society reflecting existing social norms and practices. Such an approach allows for the process of building awareness and capacity building frameworks, enabling individuals to take measures to preserve the integrity of their personal information.

Risk management by designing for privacy

A self-determination model for privacy by design seeks to identify the nuances of a society that is a recipient of the different components of the Digital India project. The concept of informational self-determination suggests that individuals need to be aware of, and control how information about oneself is collected, shared and used. Given this notion, we understand that the privacy and its subsequent management have elements that are inherent to an individual's worldview or social norms and concepts. If privacy is to be understood and built into the fabric of a society, there needs to be in place an assessment model to gauge this process. This article envisions such a reflective model with levels in the process and is summarized in the figure.



This draws out the process of creating informational flows that have privacy designed into the information channels.

There are different stages in the process, which begins with a *needs based assessment*. At this stage, a development project works with the community to understand both the need for health care, and the extent to which privacy needs to be built into the project, as well as existing concepts and practices for privacy.

This is then followed by the next stage of *knowledge and awareness*. Here, the existing flows of information and thus limits on privacy are identified. At this stage, universal privacy principles such as personal data handling, including purpose specification and use limitation, required reasons for collection, use and disclosure of personally identifiable information needs to be identified at or before the time of collection. Additional measures to identity the potential actors, and their impacts on the informational flows are examined.

The third stage is *capacity building* where members of the society or community are empowered and skilled with the ability to ensure basic security mechanisms to help alleviate any risks, and privacy breaches.

The fourth stage is *data management*. This stage may include enabling members of the community to understand and manage the mobile health care technology, or be able to educate the rest of the community. Empowerment through awareness is the key in enabling individuals to process to the last stage of *self-regulation*.

The fifth stage is self-regulation. At the stage of self-regulation, the informational flows created between the technology providers has been internalized and operationalized to the extent that social norms and behaviors around privacy have extended to the exchange of information facilitating this process.

To conclude briefly, the developments afforded by the Digital India project contribute to vulnerability to individual privacy. Risks to informational and decisional privacy include data commodification and security, surveillance and interception, and data subjectification.

A framework identifying channels of informational flows can help situate risks for to privacy. Such a framework can help associate the risks with a particular actor, and thus identify how these elements can be built into a sustainable management model.

A sustainable model that allows us to design privacy into the flow of information can help encourage informational self-determination, and the mitigation of risk. Such a model would be envisioned to have several layers. These layers include a needs based assessment, knowledge and capacity building, data management, and self-regulation. ■