Infosys®
Navigate your next

WHITEPAPER

PRIVACY IN THE DIGITAL WORLD

Data privacy has emerged as an important aspect of human rights. However, its fulfillment is challenged by the organizational and individual's desires to reap the rewards of a digital marketplace. Enterprises need to be responsible with the way they obtain and use data. A strategic decision is whether they want to use privacy as a differentiator or treat it as another compliance burden.

Infosys® | Knowledge Institute

Your own data is no longer private

Imagine that late one evening after a grueling day at work, you are trying to book a cab using your smartphone. Before you check whether the fare suits you, you realize your smartphone's battery is almost dead. Out of desperation, you confirm the cab despite the fare being unusually high. This high fare may not be the result of a shortage of cabs but is instead triggered to exploit your situation.

Behind the seemingly customer-friendly UX, the cab aggregator's algorithms work tirelessly to gather data from your smartphone including its "remaining battery power." Uber, for one, has denied such fare determination but has admitted collecting information on battery levels. According to an Uber spokesperson, battery levels are "one of the strongest predictors of whether or not you are going to be sensitive to surge pricing".[1] Even more concerning are the possibilities that exist when personal information, more than what is required, is available to service providers.

Here is another scenario: you are browsing on your smart TV and are shown advertisements of fast-food joints — this, after you have ordered dinner from your laptop. It dawns on you that your user behavior across internet-enabled devices is being tracked. According to a complaint filed by the FTC and the Office of the New Jersey Attorney General,[2] owners of VIZIO smart TVs didn't know that while they were watching television, VIZIO was, in turn, watching them every second. It did so by collecting a selection of pixels on the screen that matched a database of TV, movie and commercial content.

The company also identified viewing data from cable or broadband service providers, set-top boxes, streaming devices, DVD players and over-the-air broadcasts. In order to enable this for older models, VIZIO retrofitted the TVs by installing its tracking software remotely — all without the knowledge or consent of its customers. Our private lives within our homes are no longer private — whether we are watching TV or browsing the internet.

Finally: you notice a spike in your car insurance premium — not justified, given your accident-free history. Later you discover that your insurance provider uses telematics to charge premiums based on driving behavior generated from inputs such as speed, acceleration and usual time of driving.[3] All these data inputs were within legal limits and were received from various "internet of things" sensors installed in your car. Yet the sale and use of this data happen without your consent.

These are not hypothetical examples — they are real-life instances of privacy infringements or risks that can and sometimes do emerge from unscrupulous use of technology. At the same time, innovative technology delivers enhanced value and immense benefits to consumers. The aspiration should be to make this a positive-sum game. Organizations that benefit from the use of personal information should deploy appropriate privacy safeguards and empower consumers with knowledge and choice on how information collected from them could be used.

The evolution of privacy

Privacy is a basic trait among humans believed to exist since pre-historic times, right from early human civilization. In the days when food was gathered through hunting, the need for tribes to live together under one cave took precedence over privacy, but as the civilization progressed to farming and agriculture, with less dependence to live under one roof, the need for privacy evolved. The concept of privacy in those days and until about a century ago was a right to be let alone and not to intrude into anothers' personal physical space – ones' home, as example. Technology changed the concept of privacy with focus shifting from 'physical space' in which an individual lives, to 'the individual.'

Over the past few decades, data privacy has emerged as an extremely important dimension of human rights. However, its fulfillment is constantly challenged by the need to embrace the rewards of digital marketplace. The digital society is omnipresent — in the organizations we work for, mobile apps we use in our day-to-day lives, e-governance public utilities we avail ourselves of as citizens and social media on which we connect — all of which are a necessity today.

Consequently, many countries are either strengthening or enacting data privacy regulations that make organizations accountable and respect individual choices about their data and protect their privacy. The European Union and the state of California have already enacted the General Data Protection Regulation (GDPR) and California Consumer Privacy Act, respectively. In India, the draft Personal Data Protection Bill is under review by a joint parliamentary committee.

Privacy and its contexts

Privacy is context-sensitive. Individuals interact with multiple groups like family, friends and colleagues every day. They expect the information shared with each group will remain within the same group. This reasonable expectation of privacy that exists in the physical world, that one should have (a) control of one's information, including basic identity, and (b) control of how such information may be used by others, continues to hold even when one interacts with the internet and connected devices.

According to Professor Alan Westin[4], there are four states of privacy an individual requires at different times.

Solitude, which is about remaining separate and withdrawn from social life, one of the most relaxed states when one wants to heal, rest and prepare for reengagement with society.

Intimacy, when one wants to exchange thoughts, feelings, emotions and views with a spouse or close friends, or to receive help in a professional capacity from a family lawyer, doctor or counselor, among others.

Reserved, when one is present within a group but communicates to its members that there is a need to not share certain information or be noticed.

Anonymity, which is about achieving privacy by being in a crowd or public place. In this state, one is not noticed or recognized by virtue of being among the crowd, in a shopping mall, place of worship, theater, bar, sporting events and the like.

All these dimensions of privacy do not undermine the need for individuals

> Big-data and AI blur the boundaries between digital social contexts

to be social in society but instead provide an opportunity to introspect, unlearn undesirable experiences and recuperate before getting back into the social arena. While being with family, friends and colleagues gives an individual the opportunity to learn from their experiences, privacy, on the other hand, gives the freedom of thought to explore things, distinguish right from wrong and develop one's opinion; it allows one to decide without intrusion on topics such as occupation, life partnership, religion and so forth. Privacy is therefore a necessary ingredient for an individual, as much as being social is, to grow in the society and become a complete individual.

But big-data-driven technologies, along with the use of artificial intelligence, have blurred the boundaries between various social contexts in the digital world. Health monitoring apps, social media sites, job sites and dating apps access users' digital footprints to know and often predict when one is likely to be pregnant, depressed, going through a breakup or rejecting a job offer.

The impact of technology on privacy

Understanding the inherent harms caused to privacy due to intrusions that digital technologies introduce is a prerequisite to determining the right privacy safeguards. Three areas of impact on individuals that arise from informational and decisional privacy are:

Public disclosure of private facts

When private information about an individual, such as health and banking information, is made known to others without the knowledge or consent of the individual, it can cause irreversible harm. It can also cause distress to the individual in terms of loss of reputation, financial loss, physical damage and discrimination. In addition to security vulnerabilities, the release of information may also result from malicious or intentional deployment of technologies such as wiretapping, activating a microphone through a mobile app or tracking a location. For example, Truecaller, a Sweden-based app, imports the contacts of smartphone users from their address book without obtaining the consent of people whose contact number it imports and maintains in its database. Although the app helps promote freedom of expression and information, it impacts anonymity, an equally important facet in a democratic society. Home automation, or domotics, uses smart speakers and internet of things devices to enhance convenience and efficiency but can impact the state of intimacy unless configured appropriately. Tort or civil laws in most countries, as well as privacy laws, regulate such intrusion into privacy.

Subliminal influence

Often, information about an individual such as social media likes or dislikes, purchase preferences, reading habits, religious beliefs, associations, is analyzed along with other data for the purpose of profiling. The insights derived from such profiling, can be used to influence the individual's mind with the intent of steering towards certain desirable behavior. This in turn impacts individual's autonomy to take informed decisions, nudges them into behavioral change and creates bias at sub-conscious level. An e-commerce website suggesting books that may be of interest to an individual is a harmless and beneficial use case. However, a filter-bubble-enabled search engine that shows results driven by an algorithm prevents the individual from seeing a neutral set of results. The most infamous example may be of Cambridge Analytica[5], which exposed the extensive impact such subliminal influence can have on both individuals and society at large. Laws are emerging, and mostly at nascent stage to regulate this area.

Automated decisions made on individuals

When a decision about an individual is made solely by algorithms using data obtained from various sources, the outcome, particularly when unfavorable, may be challenged by the individual due to lack of human intervention and discretion.

Although AI improves efficiency, it lacks empathy. Suitability for employment, health insurance premium computation based on data from fitness apps and loan eligibility based on credit history are a few instances of the extensive applications of automated decisions. Since machine learning is more data- and statistics-driven, the efficacy of algorithms depends on design considerations such as variables chosen, quantity of data used to train the algorithms and accuracy of data obtained from various sources.[6]

Regulations such as GDPR[7] have emerged that stipulate the right for an individual not to be subject to a decision or profiling, based only on automated processing that significantly affects the person, including legally. In the United States, the Consumer Online Privacy Rights Act bill was introduced in November 2019[8].While yet to be passed, it tackles the issue of algorithmic decision-making. It requires those engaged in this practice to conduct an impact assessment annually for accuracy, fairness, bias and discrimination. Only then can they facilitate advertising or eligibility determination for housing, education, employment or credit.

Keys to minimize privacy risks

Almost all organizations collect and process personal data. Privacy risk exposure varies, depending on the degree to which a business is driven by deriving value from personal data. Cybersecurity deals with known or unknown hackers against whom the organizational machinery works to protect the enterprise. In case of data privacy, in addition to the hacker who may steal personal data, internal functions such as marketing, human resources, IT become potential sources for privacy violations, by virtue of their core business processes.

While it may be difficult to realize full potential of technology without impacting some degree of privacy, it is worth noting that privacy is not an absolute right. Embedding privacy into design, and empowering people with meaningful choices that are subsequently respected, will make the approach technology agnostic and minimize organizational risks.

> Embed privacy into design while adopting innovation, to make it a positive-sum game

Organizations should establish governance to ensure that its strategic business objectives are aligned with **privacy objectives** for processes involving personal data, and to manage risks arising from potential areas of noncompliance. With increasing globalization, organizations process data from different geographic locations and are subject to data privacy regulations of countries with varying privacy regulations. It is prudent to adopt an international privacy standard such as **ISO 27701**, which the organization's Privacy Information Management System (PIMS)can emulate. Making "**privacy by design**" an integral part of an organization's processes minimizes risks of noncompliance with privacy principles.

From the beginning of the data life cycle, **minimize data collection** and processing regardless of whether the data is collected directly from the individual or indirectly, such as IP address. Since the technology industry benefits from more and more information due to Big Data dividends, risks can be minimized by segregating essential and optional information, for which '**informed consent**' can be used as a lawful basis of collection for the latter category. Collecting specific data to process a service may be necessary — for instance, mobile phone numbers to provide multifactor authentication, but sharing data with third-party agents offering value-added services may not be made essential when offering a service. Individuals must be able to expose a minimal amount of personal data — for instance, the routing of calls to a cab driver through the cab aggregator's business telephone number.

Make personal information processing more **transparent** through modular and layered privacy notices at the point of data collection. These notices should include information on **profiling** and **automated decision-making**. Personal data collected must be **proportionate**, not excessive, and only **purpose-specific information** must be collected and processed. Personal data should be **retained only as long as necessary** and must be deleted or anonymized when the purpose of collection and preserving is fulfilled. **Data transfers to third parties** or disclosure to others, when legally not mandatory, must be based on an **opt-in or opt-out mechanism**, as required by applicable jurisdictions.

Consent is often construed as a silver bullet for collecting and processing any personal data. Yet in reality, consent should never be used as a substitute for **accountability**. Individuals find it difficult to decipher the fine print and complex processing details in a privacy notice to decide what is right. Volumes of information on a privacy notice does not absolve organizations of accountability in adhering to privacy principles.

Organizations that use AI to **automate decisions** must ensure **data accuracy** and **avoid algorithmic opacity**. They must inform individuals on the source of data and the logic used in making the decisions that affect them. For instance, recruitment-related algorithms trained from past interview data must avoid racial or gender bias that may be prevalent during the physical selection process.

When decisions have legal effects on individuals, additional safeguards may be required, including the right to seek human intervention as required by applicable regulations. Unfair **bias** must be avoided through periodic scrutiny of algorithms and the results they produce. Privacy-enhancing techniques, such as **differential privacy**, must be used when using big data to minimize risk of re-identification of anonymized data. Multiple privacy measures, including security-related controls, should be deployed based on the harm likely to be caused otherwise to the rights and freedom of individuals.

Value privacy or pay the price

Data privacy threats are real. Regulators and regulations will only become more stringent. Consumer awareness levels will rise, and it is for an organization to decide whether they want to use privacy as a differentiator or treat it as another compliance burden. The cost for privacy compliance is significant, but the cost of noncompliance is high too, and goes beyond legal implications to the brand itself.

References

1. https://www.independent.co.uk/life-style/gadgets-and-tech/news/uber-knows-when-your-phone-is-about-to-run-out-of-battery-a7042416.html
   https://metro.co.uk/2019/09/27/uber-charge-battery-lower-10778303/
2. https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it
3. https://www.efma.com/article/detail/30774
4. Privacy and Freedom by Dr. Alan F Westin - https://www7.tau.ac.il/ojs/index.php/til/article/view/1609/1711
5. https://newrepublic.com/article/151548/political-campaigns-big-data-manipulate-elections-weaken-democracy
6. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053
7. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679
8. https://iapp.org/news/a/u-s-senators-unveil-new-federal-privacy-legislation/

Author

Srinivas Poosarla

Chief Privacy Officer
Srinivasp@infosys.com

Contributor

Ramesh N

Principal – Infosys Knowledge Institute
Ramesh_N03@infosys.com

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.
To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

For more information, contact askus@infosys.com

Infosys®
Navigate your next