Seven commandments of privacy governance in information capitalist societies

There is a real need for corporations to endorse privacy management structures for their socio-technical systems, backed by strong regulatory policies, that better align with public values and sentiments about how firms should be handling raw personal data for their business gains while benefiting individuals equitably

BY RANJAN PAL, BODHIBRATA NAG AND CHARLES LIGHT

Ecommerce firms currently are driving home ad revenues without much concern about consumer privacy, the consumers are equally handicapped in protecting their privacy interests in the information capitalist economy

Information privacy is a complex construct that is context-dependent and driven by an imaginary control knob over-sharing and reuse. As for individual Internet consumers in the modern digital age, sharing information is often not a natural choice for them since sharing personal data (PD) is mandatory for getting access to basic day-to-day utilities, services, or products. Reciprocatively, the typical urban consumer's raw PD powered by modern AI is what drives the majority of the revenue of today's ecommerce firms. To cite an example, market data suggests that more than 95 percent of Meta's (erstwhile Facebook) revenue comes from advertising that solely relies on consumer PD. This business model can only be successful if the adverts are successful. In India, the digital advertising industry is projected to grow to approximately Rs 25K crore from around Rs 23K crore in 2021, with Google India and Meta India garnering combined ad revenues that are higher than that of the top 10 listed traditional media companies (Source: Indian Express).

On the one hand, where ecommerce firms currently are driving home ad revenues without much concern about consumer privacy, the consumers are equally handicapped in protecting their privacy interests in the information capitalist economy. Privacy experts around the globe have argued in favour of psychological and economic factors affecting individual choices to care about online privacy, in both a positive and a negative way. Furthermore, information asymmetries between the individual consumer and data-hungry ecommerce intermediaries create a non-level, privacy-risky, and non-transparent playing ground where the former has no idea who buys its PD (usually without consent), what purpose, and at what price. It is in these bleak circumstances, there is a real need for corporations to endorse privacy management structures for their socio-technical systems, backed by strong regulatory policies, that better align with public values and sentiments about how ecommerce firms should be handling raw personal data for their business gains while benefiting individuals equitably.

We propose the following seven commandments to healthy privacy governance by business organisations handling the personal data of individuals.

Ensure Data Transparency

Organisations must adopt a privacy policy whereby data flow from the individual consumer to the data intermediaries (including the organisation) should be transparent and with consent, as vouched by recent legally working regulations such as the GDPR CCPA, and PIPL. More specifically, the consumers should be told what personal data is being collected, used, stored, or transferred forward in the value chain. Organisations should make this policy Internet-public and easily accessible to both their business consumers and visitors and internal employees (via the Intranet). Moreover, the organisation should expend special human and monetary effort to undertake periodic internal audits and compliance tasks concerning procedure books adhering to time-updateable privacy policies. In exceptional cases, when PD deemed valuable to individual consumers is processed without consent, the organisation must complete a legitimate interests assessment exercise. Organisations must necessarily design appropriate privacy-enhancing and (transparent as possible) PD contracts with intermediaries, i.e., PD vendors, who buy PD from the former. This could either be done using privacy-enhancing technologies such as differential privacy or through a compliance checklist that provides a run-down of general privacy must-haves during PD sales. These PD contracts must ensure that when PD sale happens between cross borders, the business transactions should be completed lawfully using mechanisms such as binding corporate rules (BRCs). The contractual nitty-gritty should be made transparent and public.

Ensure data and storage minimization

As part of its internal policy, a personal data collecting organisation should properly define its legally-verified purpose for collecting specific PD types adequate and relevant to its business interests. There should be documentation (for both employee and leadership) for the clarity of purpose and this should not include collecting PD for a purpose not defined today but one that could arise in the future. Moreover, the scope of collected data should be pre-set in advance and aligned with the data transparency policy mentioned earlier. This would imply that an organisation should not extend its scope of PD use for capitalist gains beyond what is already there in the charted policy. Limiting the type and scope of PD collection and use holds an organisation accountable enough to minimize privacy breaches. Of equal importance as data minimization is the very related problem of storage minimization. An organisation must ensure that collected PD is stored and maintained securely enough to maintain the integrity of any client's PD throughout the business lifecycle. In addition, storage minimization principles should also be applied by an organisation, similar to data minimisation principles. These principles include
(a) PD be deleted when no longer in use or of interest to the organisation,
(b) PD be deleted when an individual wants it to be deleted or deactivates its account with a business enterprise, and
(c) A regular and/or periodic review of PD inventories and algorithmically setting up triggers to delete 'to-be-deleted' PD.

Ensure data security

Information privacy is aptly complemented by data security. An organisation dealing with personal data must appoint and significantly invest in a CISO-led team of IT security, and privacy experts who should necessarily ensure that
(a) Biometric-type data is segregated from PD information systems,
(b) Penetration and vulnerability assessment tests on PD-storing information systems are routinely conducted,
(c) Employee and customer access privileges to PD are managed,
(d) There is no unauthorised access to PD as an outcome of deploying multi-factor authentication, encryption, and CAPTCHA techniques, and
(e) The networks and distributed systems within an organisation handling PD communications are kept security-robust via the deployment of vendor systems security products such as firewalls, security software patches, and anti-virus software.

Ensure data and privacy fairness

Organisations must ensure their clients' privacy and data fairness whose PD it aggregates, for PD-driven services the clients get. For example, an organisation must make sure that advanced privacy settings are set as default and easy to understand for the consumers. The PD of minors and minorities must be well protected (via gaining parental control and consent before their processing), sensitive data (for example, racial and ethnic origin, health information, political and religious preferences) well secured and processed fairly, irrespective of privacy preferences.

Ensure robust and accountable PD privacy management

Organisations aggregating customer PD should deploy a robust and accountable privacy management framework, both in terms of technology (auditing) and human resource investments (dedicated privacy leadership), in line with the NIST privacy framework for effective continuous auditing and improvement of privacy-enhancing processes. A detailed record of the organisation's processing activities—personal data inventories, data flows, information assets, and third-party disclosures (post consultation with B2B customers) should be aptly stored and maintained. The organisation must be registered with public agencies/regulators to conduct PD-processing activities. The organisational C-suite should significantly invest in a specialised data protection officer (DPO) who must successfully run and market a privacy enhancement program for its customers and various stakeholders. One of the primary duties of the DPO will be to select internal department-specific privacy champions from within the organisation who would be the interface between the DPO and their departments (For example, information security, HR, marketing, communications, internal audit). Another duty of the DPO, and probably the most important one, will be to create a strategic roadmap of privacy improving practices within the organisation. This roadmap would involve the following privacy design principles:
(a) Engineered privacy constructs for business products should be proactive (preventative) instead of being reactive (remedial),
(b) Advanced privacy features should be made default,
(c) Privacy should be integrated into product design and development, and
(d) privacy policies should be made open to the public to build accountability and trust and show them (through intention-driven actions) that their privacy interests are a primary concern of the organisation.
Finally, the DPO should be responsible for a risk treatment plan that can help assess potential privacy risks from lawfully processing PD and suggest risk mitigation strategies.

Ensure privacy rights of organizational clients

Because of recent legislations around the globe (e.g., GDPR, CCPA, PIPL) in operation respecting privacy rights of PD owning consumers, the following rights need to be granted by organisations to their clients:
(a) Right to be informed,
(b) Right to PD access,
(c) Right to PD rectification,
(d) Right to be forgotten,
(e) Right to data portability,
(f) Right to object,
(g) Right to the restricted use of PD, and
(h) Right to opt-out of PD sale in a data economy.

Ensure proper incident (breach) management

In events of privacy breaches, an organisation should conduct a thorough forensic procedure—either internally, or through third parties—to quickly and systematically track down the cause of breach incidents, collect circumstantial evidence, and create a checklist of corrective measures to mitigate the adverse impact of the incidents. The DPO should train an internal cross-departmental incident response team to handle such events. The DPO should also be in charge to notify affected stakeholders of post-breach events and hold a subsequent post-mortem analysis with the incident response team to dig out learnings and find ways forward to prevent the likelihood of such incidents Happening in the future.

In summary, the proposed seven commandments adhere to local and international privacy standards. Organisations that handle the personal data of their clients and adopt them will implant trust and transparency in the minds of their clients. This will go a long way for organisations to reduce customer churn, improve customer retention percentages, gain a competitive advantage in the personal data economy, and boost annual revenues.

Ranjan Pal (University of Michigan, USA, University of Cambridge, UK)
Bodhibrata Nag (Indian Institute of Management Calcutta)
Chien-Lun Chen (Amazon Research, USA)

Source:https://www.forbesindia.com/article/iim-calcutta/seven-commandments-of-privacy-governance-in-information-capitalist-societies/75007/1