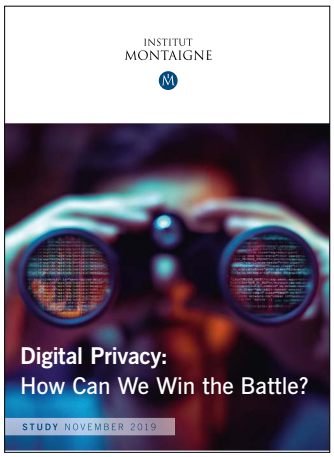
INSTITUT
MONTAIGNE



Executive Summary

"Gentlemen don't read other people's mail." Actually, they sometimes do, legally or surreptitiously. In the digital age, we constantly emit personal data far beyond traditional exchanges and this data floats in the cyberspace.

The digital age cannot be de-invented, and there can be no individual rights if there is no privacy. How societies deal with this challenge, involving both the positive uses of the digital age, its downside and some terrifying possibilities, is a question for everyone to consider.

On the issues of digital privacy and the protection of personal data, Institut Montaigne provides a concrete understanding of the major **regulatory environments.** From this comparative approach, we draw policy implications for improving or revising the GDPR.

Privacy is an umbrella term that is intuitively understood by everyone, but that is not easily defined. **In legal terms, privacy is mostly understood as data protection,** and personal data is the key focus of data protection regulations. The goal of protecting personal data and privacy stands in a **regulatory balance** with two other goals, that of **efficiency or economic gains** for individuals and companies, and **public interest** – from national security to whatever may be considered as a public good. All regulations navigate between these three goals.

The privacy debate has two matrixes. One is clearly the **United States.** Digital technologies are largely invented there, the giant and not so giant companies that pioneer these have a global influence. America is therefore the mother of all privacy debates, and it has previously enacted important yet diverse pieces of legislation. **Europe** has increasingly become the other major influencer, with its **path-breaking GDPR.** However, the GDPR is also a **catch-all text** that is built on an uneasy equilibrium between opposite objectives.

GDPR, a European regulatory feat

With its **88 pages of superb writing,** focusing on the collecting and processing of personal data (rather than on its use), the GDPR is a fine balancing act between the **protection of individuals,** the explicitly recognized **commercial need** for the free flow of data in and out of the EU, and a series of exemptions from protection where legal requirements or **public interest** are concerned.

One major innovation of the GDPR is to provide for cooperation among national boards for **cross-border cases,** many of which go through a **one-stop shop** mechanism, where a Lead Supervisory Authority must firstly be designated. However, the reality is less impressive as it does not apply in cases where the entity in question operates from outside the EU, nor does it differentiate well between place of legal establishment and location of actual operations. The risk of course is a **28 stops shop.**

The level of fines imposed by the GDPR is based on ***ex ante* assessment,** setting ceilings relative to turnover. Sanctions should also rely on ***ex post* action,** and that largely implies a shift towards **real damage assessment or tort litigation.** The reasoning is simple: **companies do cost/price analysis** for compliance. Individuals should obtain redress for the violation of their privacy.

Technology is a fast-moving frontier, and it is impossible to predict what type of data will turn out to be personal, sensitive or critical. Collection of data cannot be fully undone. What can more realistically be regulated is **the usage of collected data** and its interpretation.

To supplement our understanding of data protection, we have included two case studies on **India** and **China**, which are becoming increasingly central to the digital privacy debate and to browse through the spectrum of the privacy systems.

India, a digital blend between the EU and China

After a landmark ruling on the right to privacy by the **Indian Supreme Court,** the **Personal Data Protection Bill** (PDPB) was drafted by an expert committee in 2018, although it has yet to pass the legislative stage. PDPB largely follows the GDPR model, laying down obligations for data fiduciaries and giving rights to individuals. It sets up a **National Data Protection Authority**, introduces financial penalties for noncompliance, and **exempts authorities from obligations on grounds of national security and public interest.** Nevertheless, this Union legislation is not complemented by laws at the state level.

But **India is also a swing state,** a battle ground for privacy issues and sovereign control of data versus free flows. With concerns rising about the data security of Chinese apps and the prevailing GAFA in the Indian online market, there is **a push for data localization in the name of sovereignty and security.** This push is often judged to be a proxy for support to local industry and companies, and a hindrance to the free flow of data. India seems to be **a bridge** combining features from the European and Chinese cases, **modelling its legislation on the GDPR while using it as an instrument for its industrial policy.**

The PDPB leaves important decisions at the discretion of the **Union government.** State control over digital space is reflected in such instruments as content moderating guidelines for data intermediaries, facilitation of government access to data and source codes under the Draft Data Intermediaries Guidelines

and the proposed E-Commerce bill. Thus, **regulation can also go in the Chinese direction, emphasizing national security and control over free flow of data.**

China, the surveillance State with some privacy concerns

With **China,** we enter a different universe. Behind the Chinese firewall, the so-called BAT - Baidu, Alibaba and Tencent cut across different sectors. They **collect and process more big data, including personal data, than any international competitor.** In practice and even under a very loose regulation, the government has full access to digital data. The overall public discussion about privacy is therefore focused on **data security,** as a part of **national security,** rather than on protecting privacy.

China's cyber law of 2017 provides in principle protection to users. However, it is biased towards the **state's rights,** with a few **conditional or vague rights for the individual.** The rights and obligations of private actors are the subject of some debates. The law has been followed by a spate of supplementary laws, regulations and standards. The most important one is the 2018 **Personal information security specification** (PIS), which borrows some traits from GDPR and yet differs in key provisions. **Its requirement for consent is much looser than the GDPR's,** the result of a compromise reached between company representatives and experts.

The Chinese state can conceive to protect individuals as consumers against predatory commercial interests. It will not perform the same task against itself. Laws and regulations can be **interpreted at will,** with **ill-defined "other" categories**.

Health data and privacy: a positive spin

The health sector is our theme-in-focus. **Digital health** has started a revolution in moving **research** ahead and in facilitating care on the ground closer to each patient. But it all rests on pinpoint accuracy **in knowing and predicting individual health status,** and therefore it poses the most vital challenges to privacy that could be conceived outside the case of a technological surveillance state.

GDPR has only generic prescriptions, and is more open to the **use of medical data by public entities** than by private insurance or private health companies. While in theory Europeans have long built welfare states that include large sources of analog or digital health data, these were **often collected for reimbursement purposes** rather than for medical purposes, let alone research. **France** for instance, with a resolute policy push, is nonetheless only half-way through these issues.

The **Indian** approach appears so far to be sketchy on the regulatory front, while major digital developments are under way. A major health data protection act, **DISHA,** has been submitted to Parliament. It is so protective of patient data in its present form that it will either be hard to implement or likely to **inhibit medical research.**

By contrast, **China**'s digital planners envision health data as an integral part of the development of medical care and the pharma industry as an **economic resource** for the country. There are few holds barred, and China is wooing foreign companies to use its **loosely regulated environment** for big data.

From these various observations, we move on to seven specific propositions:

Proposition 1: Strengthening the GDPR's oversight, enforcement and adaptability

A rule can only be as good as its actual implementation. A revised GDPR should prevent restrictions that damage a unitary decision-process. It should focus in priority on clarity, simplicity, and ease of implementation.

Proposition 2: Making privacy policies more readable and ergonomic

User experience (UX) is as important as the understanding of rules by users. Ensuring the improvement of user experience is crucial to achieve one of the primary goals of the GDPR: to put individuals back in control of their personal data.

Proposition 3: Ensuring privacy by design in practice

Individuals should be unburdened from choices they cannot make. Privacy by design has been incorporated into the GDPR but there is a need for clear policies, guidelines and work instructions related to privacy by design.

Proposition 4: Providing an effective right to explanation under the GDPR

Algorithms are black boxes to almost all users, but the public has a right to explanations for decisions reached by automated process. Explainability, reliability, accountability and transparency of the algorithms have to be ensured, especially in the public sector.

Proposition 5: Creating avenues for torts and litigation

Regulation must also rely on ex post action, and create a framework that imposes greater tort liability. As a quid pro quo for more ex-post liability to litigation, there could be less requirement for transparency of private algorithms, since they are a business resource.

Proposition 6: Introducing sector-specific regulations

There are clearly sectors that require specific or more fine-tuned regulation. These, in the case of the health sector, financial services, and policy data, must be encouraged.

Proposition 7: Creating simulated health data for better anonymization

Simulated health data is an emerging technology that provides solutions to both the need for a big health data research and guarantees for data privacy. Further studies on techniques to ensure the balance between the two are needed.