epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER to the

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY of the

GOVERNMENT OF INDIA

White Paper of the Committee of Experts on a Data Protection Framework for India

January 31, 3018

I. Introduction

We submit these comments in response to the *White Paper of the Committee of Experts on a Data Protection Framework for India*.[1] 2017 marked the "worst year ever" for data breaches, according to a pair of reports by Thales[2] and the Online Trust Alliance.[3] The need for comprehensive data protection regulations has never been greater. We are encouraged to see that the Government of India has recognized this and is carefully formulating a data protection law.

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, DC. EPIC was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age. EPIC has shaped the development of privacy law in the U.S., testifying before Congress,[4] participating in the administrative agency rulemaking process,[5] and litigating

[1] http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf.
[2] https://dtr.thalesesecurity.com
[3] https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf
[4] https://epic.org/testimony/congress/
[5] https://epic.org/apa/comments/

landmark privacy cases.[6] EPIC has also been an international leader,[7] writing a report on privacy and human rights around the world[8] and, more recently, filing an amicus brief in *United States v. Microsoft*[9], a case before the US Supreme Court concerning law enforcement access to personal data stored in Ireland.

Last year, the Supreme Court held that privacy is a fundamental right under the Indian Constitution. The landmark *Puttaswamy* decision was a major turning point for the state of data protection in India. At the same time, Aadhar, India's enormous national biometric identification system, raises serious privacy concerns. India is in a position to be a world leader in data protection, and this White Paper is an important step in protecting the privacy of 1.3 billion people.

The White Paper's provisional views and seven key principles of a data protection law will support the drafting of a strong bill. We provide these comments to address a few provisions that we wish to emphasize and believe will be critical in India's drafting of a data protection law.

II. Scope and Exemptions

Chapter 3: What is personal data?

One of the key provisions in any data protection legislation is the definition of "personal data." This definition is critical because it will determine when the obligations of the legislation should be applied and when they can be ignored. EPIC suggests a construction that would define personal data as information that "identifies or could identify a particular person," followed by

[6] https://epic.org/privacy/litigation/#cases
[7] https://epic.org/international/
[8] https://epic.org/phr06/
[9] https://epic.org/2018/01/in-supreme-court-brief-epic-ba.html

the examples cited as illustrations, with the qualifying phrase "including, but not limited to." This approach is technology neutral and more likely to adapt over time.

III. Grounds of Processing, Obligation on Entities and Individual Rights

Chapter 7: Storage Limitation and Data Quality

First, we support a data minimization requirement. It has become clear that one of the best strategies to reduce the likelihood of an attack and to minimize the harm when such attacks do occur is to collect less sensitive personal information at the outset. It is the credit card numbers, the bank account numbers, the government identification numbers, and the passwords that draw the attention of computer criminals. Reducing the target size reduces the vulnerability.

There are many examples of data minimization requirements in privacy law. For example, the Video Privacy Protection Act requires businesses to:

> Destroy personally identifiable information as soon as practicable, but not later than one year from the date the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information . . .[10]

Other U.S. privacy laws include similar requirement.[11] The simple message to business should be "if you can't protect it, don't collect it."

IV. Regulation and Enforcement

Chapter 2: Accountability and Enforcement Tools

B. Personal Data Breach Notification

We support a 48-hour requirement for breach notification. Legislation should include provisions on data breach notification that create deadlines for notification of law enforcement

[10] 18 U.S. Code § 2710(e).
[11] *See e.g.* Gramm-Leach-Bliley Financial Services Modernization Act, Title V of the Financial Services.

and consumers. Law enforcement must be notified within 48 hours of discovery. Companies must assess the scope of the breach, identify the nature of the breach, and address the vulnerabilities that created the breach. Within 48 hours of conducting this assessment, companies may have to notify consumers. The shorter time period will require companies to respond quickly when there is a problem. This shorter period will also allow consumers to react more quickly and take preventative or mitigating actions.

The White Paper does not address methods of notification, but legislation should specify how data controllers should inform consumers that their information has been breached. It should require the use of either written notification or email notification when an obligation to provide notification arises. Additionally, we suggest that you include an additional obligation to provide a text message where possible. A text message would not be an effective substitute for written notification or email, because it is essentially ephemeral. But is a very effective technique for notification and it could help make people aware that they should look for a notice that might arrive in the mail or show up in the email box.

Legislation should also account for providing notification by means of a "website or social network presence." Many organizations today are interacting with users though popular social network services such as Facebook. In many configurations, the data remains with Facebook, so there is no direct data collection by third parties. But in other circumstances, for application developers and advertisers for example, third party companies obtain information from users through Facebook. If security breaches arise in these circumstances, notification by means of the social network service may be the most effective way to reach the target population.

Chapter 4: Remedies

We support the inclusion of provisions allowing enforcement by the data protection authority, but would recommend also including a private right of action for consumers in the legislation. This would empower citizens—who have no bargaining power with companies that collect their data—to have a check on corporate power. Many U.S. state data breach laws include private right of action provisions. California, Hawaii, Louisiana, and Washington, for instance, include provisions in their laws that allow consumers to bring a civil action and recover damages.[12] Such provisions allow privacy jurisprudence to develop through a diverse set of real use cases over many years, adapting to changes in technology. Therefore, including a private right of action will both strengthen consumer protection and improve the development of privacy law in India.

V. Conclusion

EPIC supports the Government of India's goal of passing comprehensive data protection legislation and we look forward to working with the Ministry of Electronics and Information Technology on this issue of vital importance to the people of India.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President
Rotenberg@epic.org

/s/ Christine Bannan
Christine Bannan
EPIC Administrative Law & Policy Fellow
Bannan@epic.org

[12] Cal. Civ. Code 1798.82 (2011), Haw. Rev. Stat. § 487N-2 (2011), La. Rev. Stat. § 51:3071 et seq.(2011), Wash. Rev. Code § 19.255.010, 42, 56, 590 (2011).