The DPDP Act's Unanswered Question: Can Privacy Law Block a Software Piracy Investigation?

News & Updates • August 30, 2026

I. The Infringer’s Privacy Paradox

The Digital Personal Data Protection Act, 2023 ("DPDP Act") is built around a clear rule. Personal data may be processed only for a lawful purpose and only with the consent of the individual or for one of the "certain legitimate uses" listed in Section 7. This framework is easy to apply when the relationship between the Data Fiduciary and the Data Principal is lawful. For example, a customer opens a bank account, an employee joins a company, or a consumer buys software. The individual receives a privacy notice, accepts the relevant terms and either gives consent or falls within a specific category of legitimate use recognised by the Act.

However, software piracy cases or unauthorized software use creates a different situation.

Consider two individuals using the same software program of a particular software company. The first person purchases a valid licence, accepts the End User Licence Agreement (EULA) and is informed that the software uses licence-verification technology called “phone-home” which collects or detects any information regarding any unauthorized usage of the software. The second person illegally installs a cracked copy of the software, using keygens available and thereafter bypasses the genuine activation process and is not exposed to the screen on which the notice or the EULA and consent would normally appear. Thereafter at the time of use, certain technical information such as MAC Id, User ID and Username, Email Domain of the company, Wifi SSID, some of which may be categorized as Personal Identifiable Information (PII) under the DPDP Act. These technical and personal information are provided by the infringer while activating the software.

Can the software publisher or any entity on behalf of the software publisher use to process these PII data of the infringers without their consent?

The DPDP Act does not give a direct answer to this specific question. Furthermore, the Copyright Act focuses on the violation of the source code in the underlying software program. However, collection of the evidence of violation is the subject matter of the procedural laws such as Bharatiya Sakshya Adhiniyamand, 2023 and the Code of Civil Procedure, 1908 (CPC). The act of evidence collection is also governed by the judicial precedents which have legalized the use of such procedures which helps in identifying the violation that already occurred. The processing activity within the DPDP Act does not specifically legalise processing of such data for identifying the wrong of software violation.

Processing within the Act is largely based upon the consent of the Data Principal as well as the process being fundamentally legitimate in nature.

This creates what may be called the "**Infringer's Privacy Paradox".** It is not merely theoretical. Modern software publishers use activation records, licence verification systems and limited telemetry to distinguish genuine installations from unauthorized copies. Some of that information may qualify as PII such as Username, Email Id etc. Without it, enforcement of intellectual property rights in a digital environment can become practically ineffective.

The licensed user, who follows the rules, procures the software lawfully is subject to disclosed genuine use verification through phone-home technology.

While the unauthorised user argues that they have not given consent to process their personal data and the absence of consent prevents the software publisher from investigating the unauthorized usage of the software.

The issue is therefore not whether an unauthorized user continues to enjoy privacy protections under the DPDP Act. Rather, it is whether the absence of consent—resulting from the user's deliberate circumvention of the licensing framework, should prevent the limited processing of personal data reasonably necessary to detect and investigate copyright infringement.

II. Why Consent Alone Does Not Resolve the Issue

Consent is paramount to the DPDP Act because it gives individuals control over their personal data. Any interpretation of the Act must preserve that protection. However, consent cannot answer every situation in the same way.

In an ordinary transaction, the organisation has a fair opportunity to give notice and obtain consent. In a software piracy cases, the unauthorised user may have deliberately removed that opportunity by using a crack, a false activation key or any other method designed to defeat the licensing or software activation system. Requiring the publisher to obtain prior consent in that situation would make the investigation depend on the cooperation of the suspected infringer.

A simple example helps. A car owner installs a GPS recovery device in the car. If the car is stolen, the thief has not consented to the transmission of the car's location. Yet it would be difficult to say that the owner must ignore the signal and abandon recovery of the vehicle. The location data is being used for a narrow purpose: to recover property and enforce an existing legal right for a legitimate use. This is a practical concern in software copyright infringement in India.

The analogy may not be applicable in the present case because software telemetry may involve processing of personal data without consent but for the purpose of identifying the extent of the

infringement. Therefore, in such cases the identification of the infringement becomes a legitimate use case under Section 7 of the DPDP Act.

However, this does not mean that an alleged infringer loses privacy rights as guaranteed under Article 21 of the Constitution of India. A software publisher cannot justify the collection of unlimited personal data merely by characterising its activities as "anti-piracy" or "licence enforcement". Any processing must be strictly limited to the personal data reasonably necessary to verify unauthorised use and enforce the publisher's legal rights. Such data must not be collected, retained, or used for any purpose unrelated to that enforcement objective. The publisher must therefore be able to justify what data it collects, why each category of data is necessary, how long it is retained, who may access it and ensure that the data is not processed for any secondary or unrelated purpose. As an example, this phone-home data should not be used by the sales teams of the software publisher in order to increase their business or for any other such purposes.

The collection and processing of data within the DPDP Act should be solely for the purpose of initiating a legal action against the infringer.

III. Licence-Verification Technology Is Not the Same as General Surveillance

The term "phone-home technology" is often used as though it describes one uniform practice. It does not. In this article, the term means technology built into software that communicates with the publisher to confirm whether the copy is genuine and properly licensed. To avoid confusion, it is referred to below as "licence-verification technology".

Depending on how it is designed, the technology may transmit a licence key, activation status, software version, device identifier, email addresses, IP address, date and time of installation, or similar technical information. Some of this data may be linked to an identifiable individual and may therefore be personal data under the DPDP Act.

The purpose of the technology matters. There is a clear difference between the following two situations:

Type of processing	Example
Licence verification	The software sends a device identifier, licence status and activation record to check whether the software installation is genuine.
Intrusive monitoring	The software records unrelated files, browsing activity, emails, confidential information, employee behaviour or other information that is not needed to verify the licence.

Both activities involves personal data, but they are not legally or ethically equivalent. The first may be capable of justification if it is narrow, necessary and properly controlled. The second is much harder

to defend because the information is unrelated to the enforcement purpose.

A software publisher's strongest position is therefore not: "The user is an infringer, so privacy does not apply." The stronger and more defensible position is: "We process only the limited technical data needed to determine whether our software was being used without authorisation and we did not use that data for any unrelated purpose."

IV. Reading the DPDP Act Alongside the Copyright Act

The DPDP Act should not be read in isolation. It operates alongside the Copyright Act, 1957, which protects software as a form of copyrightable work and gives the owner legal remedies against unauthorised reproduction and use. The two laws protect different interests, but they are not natural opponents. Privacy law protects individuals against misuse of their data; copyright law protects creativity, investment and proprietary rights. The question sits at the intersection of software piracy and copyright law.

The difficulty is that the DPDP Act does not contain an open-ended "legitimate interests" ground like the European Union's General Data Protection Regulation. Nor does Section 7 expressly mention the investigation or enforcement of private legal claims. A software publisher should therefore not assume that copyright enforcement automatically creates a lawful basis for processing under the DPDP Act.

At the same time, a reading that prohibits every use of limited licence-verification data would make digital copyright enforcement unusually difficult. Software can be copied, installed and used remotely, often without any direct interaction with the publisher. In many cases, the embedded licence check may be the only practical way to identify the unauthorised installation.

Software publishers should, however, be mindful of Section 17 of the DPDP Act. While Section 17 is not a standalone source of authority for unrestricted processing of personal data, it demonstrates that Parliament recognised that the consent-based framework cannot apply uniformly in every factual situation. The provision acknowledges that, in limited circumstances, personal data may necessarily be processed in connection with legal proceedings, the establishment, exercise or defence of legal rights, or the investigation of offences. The existence of this exception reinforces the broader legislative principle that privacy protections should coexist with the effective administration of justice and the enforcement of rights recognised under law.

Accordingly, where a software publisher processes only such personal data as is reasonably necessary to identify an unauthorised installation, preserve evidence of copyright infringement or pursue legal remedies arising from that infringement, the processing should be assessed in light of the principles reflected in Section 17.

At the same time, reliance on Section 17 cannot become a justification for indiscriminate data collection. The exception is inherently narrow. It cannot legitimise the collection of personal data unrelated to the alleged infringement, nor can information collected for enforcement purposes subsequently be used for marketing, customer analytics or any other commercial purpose. The processing must remain confined to investigation, enforcement and the conduct of related legal proceedings, supported by appropriate governance, retention controls and internal safeguards.

V. A Clear Test for Licence-Enforcement Data

When the Board examines a complaint involving licence-verification technology, it should ask five simple questions. These questions translate broad privacy principles into a practical test. This also raises the broader issue of DPDP Act and copyright infringement.

1. Is there a specific legal purpose?

The publisher should identify the precise purpose of the processing, such as confirming that a licence key has been used on unauthorised devices, investigating a particular cracked installation, preserving evidence or pursuing related legal proceedings. A vague statement such as "protecting our business" should not be enough.

2. Is each item of data genuinely needed?

The publisher should collect only what is reasonably necessary. For example, a licence key, device identifier, activation record and IP address may help link an installation to an infringement. Access to unrelated documents, messages, photographs or browsing history would ordinarily go far beyond that purpose.

3. Is the method proportionate?

The system should use the least intrusive method that can reasonably achieve the objective. A one-time or event-based licence check is easier to justify than continuous monitoring of a device. The seriousness and scale of the suspected infringement should also be relevant. The question of personal data in copyright enforcement therefore becomes central to effective IP remedies.

4. Is the data used only for legal enforcement?

This illustrates the practical tension between IP enforcement and data protection. Technical data collected to investigate piracy should not be added to marketing databases, used for behavioural advertising, sold to third parties or repurposed for employee monitoring. It should remain separated from ordinary commercial analytics.

5. Are there proper controls and a clear end point?

Access should be limited to authorised legal, compliance and technical personnel. The publisher should keep records of why the data was collected, protect it against unauthorised access and delete it when it is no longer needed, subject to legitimate requirements relating to settlement, limitation periods and legal proceedings.

A publisher that cannot answer these questions should not be permitted to rely on the language of copyright enforcement as a general defence. Conversely, where the answers show a narrow, documented and proportionate process, the absence of consent should not automatically make the investigation unlawful. The issue also illustrates the wider relationship between IP enforcement and data protection.

VI. Why This Question Matters Beyond Software Piracy

The same problem may arise in other digital disputes. A company may use embedded identifiers to trace stolen source code. A platform may analyse technical logs to investigate online fraud. A developer may use access records to identify the unauthorised copying of an artificial intelligence model. In each case, personal data may become relevant to the enforcement of another legal right. This distinction is especially relevant to software piracy and copyright law.

A rule that treats the absence of consent as conclusive could prevent legitimate investigations. A rule that gives organisations a broad enforcement exception could permit intrusive monitoring. The law therefore needs a middle path: a close link to a specific legal claim, collection of the minimum necessary data, strict limits on use and strong accountability.

This is also why clear guidance would benefit both individuals and software publishers. Individuals would know that anti-piracy tools cannot become a cover for general surveillance. Publishers would know the conditions they must satisfy before relying on technical data in an investigation or legal proceeding. The analysis therefore remains relevant to the broader question of DPDP Act and copyright infringement.

VII. Conclusion

The unresolved question under the DPDP Act is not whether copyright owners may ignore privacy law. They may not. Nor is it whether an unauthorised user loses all rights over personal data. The user does not.

The real question is whether a person who deliberately bypasses a lawful licensing process can use the resulting absence of consent to block the limited processing needed to identify and investigate the infringement. These safeguards are important when considering personal data in copyright enforcement.

A balanced answer should focus on what the publisher actually did. If it collected extensive or unrelated information, retained it indefinitely or used it for commercial profiling, the privacy concerns are strong. If it collected only the technical data needed to verify an unauthorised installation, kept the data secure and used it only for enforcement, the legal position is materially different. The issue is particularly significant in software copyright infringement in India. The DPDP Act and the Copyright Act should be applied in a way that protects both privacy and innovation. The simplest principle is also the most useful: enforcement cannot become an excuse for surveillance, but privacy should not become an unintende

KEY CONTACT

Shantanu Sahay

Partner

View Bio of Shantanu Sahay

RELATED INDUSTRIES

DIGITAL PERSONAL DATA PROTECTION

RELATED PRACTICES

COPYRIGHT