Privacy vs Security

14 September, 2024 | created using PDF Newspaper from FiveFilters.org

Privacy vs Security: Telegram CEO Pavel Durov's arrest reignites global debate

Sep 12, 2024 06:11AM

The arrest of Telegram CEO Pavel Durov has sparked a global debate on the balance between privacy and security in the digital age. French authorities' charges against Telegram have raised questions about government regulation of online networks.

Telegram CEO Pavel Durov/Facebook

Telegram Chief Executive Officer Pavel Durov's arrest reignited a global debate on the delicate balance between privacy and security in the digital age. The French authorities' charges against Telegram, including a lack of content control and encouraging illegal activity, have prompted questions about governments' responsibility in regulating online networks.

The incident has raised concerns about the scope of government surveillance and the necessity for better online legislation to prevent abuse of digital platforms.

The Privacy vs Security Debate

The incident has rekindled the debate between privacy and security, with many claiming that the arrest is a clear example of government overreach and a threat to digital freedom. Others argue that the government has legitimate jurisdiction to investigate and regulate online platforms to prevent criminal activity and preserve national security.

Since the introduction of modern technology, governments have explored ways to obtain private information for national security purposes. Following major terrorist incidents, such as 9/11, there has been a significant increase in state-sponsored surveillance. Wiretapping, data monitoring, and access to encrypted communications are more widespread.

Governments make a clear argument: intelligence agencies must be permitted to intercept communications to safeguard citizens from potential dangers. However, every security measure erodes personal privacy. Some people find this trade-off intolerable. Critics argue that once governments have access to private information, there is no turning back, resulting in a future in which privacy is no longer valued.

mid-day.com spoke to experts to draw viewpoints and insights to understand the persistent relationship between privacy and security.

Cybersecurity ExpertSpeak

Speaking about how the government can conduct surveillance, Ritesh Bhatia, a cybersecurity expert and a cybercrime investigator, said, "Imagine entering an office building. Outside, you're visible, but once inside, you're hidden—this is encryption. However, notifications that pop up on your phone from encrypted apps like WhatsApp are in plain text and accessible to other apps. So, if we discuss buying an SUV on WhatsApp, Instagram may show car ads based on the notification. This is how big tech companies like Meta access data indirectly, including your interactions."

"Governments can pressure these companies to monitor conversations by setting specific keywords for surveillance. While direct snooping is illegal, indirect methods—like through apps you download, such as government apps—allow more access to your data, leading to concerns about surveillance. The balance between national security and privacy is a delicate one. It's reminiscent of situations where sacrificing the privacy of a few may seem justified for the safety of many. But the question remains—what is being taken from us in the name of security," he added.

He said that to address concerns around surveillance and privacy, it was important to understand how these systems operate. "For instance, the Digital Personal Data Protection Bill exempts certain government agencies from its provisions, allowing them to access data without the same restrictions that apply to others."

The cybercrime investigator based in Mumbai added, "The government may use such situations to justify increased surveillance, employing artificial intelligence to track conversations and detect potential threats. However, this can result in false positives and an overreach into citizens' private lives."

Ritesh, elaborating further, stated, "While technology may enable cybercrime, offline solutions should be strong enough to manage these threats. The issue arises when privacy is violated in the pursuit of security. For example, apps like Tinder are private spaces where users expect a certain level of privacy. However, if the government demands data from intermediaries like Tinder, it crosses a line unless users are informed."

"Transparency is key," he said and added, " When it comes to the balance between national security and privacy, the boundaries need to be clearly defined: who is being surveilled, when, for how long, and why. The Data Privacy Bill emphasises consent, and any

collection of data should be transparent and consensual. National security is important, but it must not come at the cost of unchecked surveillance."

Meanwhile, senior journalist and cybersecurity expert Gautam S Mengle, while responding to a question regarding the privacy vs national security debate, said, "There isn't a simple yes or no answer to the debate between privacy and national security. The issue is complex because our approach to it is fragmented, rather than holistic. We aren't striving for a solution that simultaneously guarantees individual privacy and national security. Instead, national security is often invoked as a convenient fallback when other systems fail. If we truly prioritised privacy, why do dark web markets thrive, where personal data like yours and mine is bought and sold so easily? And why do commercial entities, which collect our mobile numbers and email addresses, get away with selling that data to third parties without accountability? There are no robust laws or systems in place to curb these practices."

Elaborating on the case that Durov was embroiled in, he said that Telegram has long faced criticism for being a platform where illicit activities including child pornography and dark web markets, can occur.

"If authorities request access to information related to sensitive cases, such as child sexual abuse material, and Telegram refuses to cooperate, pursuing legal action is justifiable. The company has been given the opportunity to comply but failed. However, if the goal is to exploit encryption technology for mass surveillance of citizens, then the issue becomes much more problematic. The refusal to enable blanket surveillance shouldn't be a pretext for undermining privacy. Justice and privacy are both essential, but they need to be addressed separately and with clarity," he added.

Mengle remarked any system, law & practice implementing blanket surveillance without a valid reason is inherently dangerous.

He said, "When it comes to surveillance, blanket monitoring is problematic. Yet, it's important to recognise that surveillance in some form has been present since the earliest days of civilization. When the first telecom services were launched in India, their headquarters had rooms where intelligence officers could tap citizens' phones. But, at least on paper, this has to be done under legal provisions. Even today, government surveillance requires a legal framework."

"Authorities must file an affidavit in court, proving the need for surveillance on the grounds of national security before they can tap phones or monitor individuals. Even tapping phones of underworld figures required this process to be followed in the 1990s, when gangland violence was at its peak," Mengle further stated.

He said that while targeted surveillance with proper legal oversight is justifiable in cases like terrorism, child pornography, or criminal activity, blanket surveillance is not.

"It's a slippery slope—once that power is granted, it's difficult to control how it is used. Effective surveillance requires a balance—knowing where and how it's applied without infringing on individual privacy," he added.

"The general public's understanding of privacy issues remains limited, **because we don't talk about it enough. Even in the news, cybersecurity is often relegated to the tech-related sections. How, then, is the lay person supposed to even begin to understand something as deep as digital and data privacy?" said Mengle.

He added that it is the government's responsibility to protect national security that cannot be overstated. However, prioritising security over privacy is not a long-term solution. As technology progresses, surveillance becomes easier and more pervasive, raising the question: How can governments ensure they balance both?

The solution lies in transparency and accountability. Surveillance is important in some circumstances to address legitimate national security concerns, but it must be done within specific parameters. Law enforcement and government organisations should implement a strategy that requires oversight to ensure that privacy rights are not violated without justification.

Digital Rights AdvocateSpeak

Prateek Waghare of the Internet Freedom Foundation, a digital rights organisation based in Delhi, said that there has often been perceived tension between privacy and national security. He said that privacy itself is integral to national security.

"At an individual level, if the privacy of people involved in sensitive national issues is compromised, it directly becomes a national security concern. For instance, if external actors are snooping on key individuals, it can lead to severe consequences for the country's safety," said Waghare.

He added that historically, finding the perfect balance has been elusive. " While we may never discover a simple way to manage this balance, we do have frameworks that can guide us. In India, for instance, there are legal restrictions in place that require surveillance to have a legitimate basis and be conducted in the least intrusive manner possible," he said.

Waghare said that if the guidelines are followed in both letter and spirit, a significant part of the tension can be resolved and pointed out that challenges shall remain particularly with ensuring surveillance is only carried out when necessary and does not infringe on individual rights unnecessarily.

Speaking about whether we have managed to strike a balance between national security and privacy, Waghare noted, "There is a propensity to over-emphasise national security in conversations, portraying a wide variety of issues—such as privacy or even free speech—as security concerns. Governments frequently say that monitoring is required and that if the subjects are aware of it, the entire objective of spying is defeated. This creates a scenario in which institutional supervision is critical."

He added that one key distinction should be made between targeted surveillance and mass surveillance.

"The current trend seems to lean towards mass surveillance, where authorities attempt to collect as much information as possible and process it later. This blanket approach is highly problematic. Mass surveillance not only raises concerns about misuse but also has a chilling effect on how people communicate and behave. While we may not have sufficient research to fully understand this behavioural change, it is reasonable to expect that knowing they are being surveilled could alter how individuals speak and act," said Prateek in a conversation with mid-day.com.

Surveillance needs to be under strict institutional oversight to prevent misuse. One of the risks of mass surveillance is the ability to collect detailed profiles of individuals. While current technology may not fully enable this yet, it remains a significant threat, said Prateek Waghare when asked potential risks of increased vigil.

He added that surveillance can interfere with conversations as seen with apps like WeChat, and WhatsApp, where "certain messages never reach their intended recipients due to censorship".

"This creates a "black box" effect—citizens are unaware of what information is being intercepted or how it could be used in the future. This uncertainty raises concerns about potential prosecution or manipulation based on the intercepted data, said Prateek Waghare.

LawyerSpeak

Advocate (Dr.) Prashant Mali, a Cyber and Privacy Expert Lawyer from Bombay High Court speaking to mid-day.com, said that national security has always been prioritised and that it will keep happening. However, he stated that the right to privacy is not an absolute right and National security is an exception.

When asked about the ways how governments can ensure national security without infringing on privacy rights, he said that the governments can ensure national security " while protecting privacy through targeted", transparent, and accountable practices.

" By employing advanced privacy-preserving technologies, robust legal frameworks, and oversight mechanisms, governments can effectively mitigate threats while upholding the privacy rights of their citizens. Collaboration with civil society and technology experts further enhances this balance," Mali said.

When asked about the effectiveness of GDPR (General Data Protection Regulation) in Europe and India's Information Technology (IT) Act in India, Mali said, "While GDPR and the IT Act provide some safeguards against government overreach in surveillance, both have significant limitations, particularly when national security is invoked."

Mali, further speaking about it, said, "GDPR is more effective in offering clear protections, but national security exemptions and inconsistent enforcement remain major weaknesses. The IT Act, on the other hand, offers fewer protections, with broad surveillance powers and limited oversight mechanisms. Strengthening data protection laws, enhancing transparency, and ensuring robust judicial oversight are critical steps to better balancing national security needs with privacy rights."

Meanwhile, Adv Bindu " play a critical role in curbing potential overreach by governments in surveillance activities. However, their effectiveness can vary based on several factors".

While India's IT Act has data privacy safeguards, enforcement can be inconsistent, and the legislative framework is now being revised to improve its effectiveness, Dubey told mid-day.com.

She added that both GDPR and the IT Act allow exceptions to data protection laws, especially in the context of national security and law enforcement.

"These exemptions can sometimes be broad, potentially leading to overreach. Effective implementation requires a balance where exemptions are narrowly defined and subject to rigorous scrutiny to prevent misuse," Adv Dubey said and added, "Both GDPR and the IT Act incorporate principles aimed at protecting individual privacy and data. GDPR is particularly robust, with its strict requirements for consent, transparency, and data protection. It mandates that personal data be processed lawfully, fairly, and transparently, and it provides strong rights to individuals regarding their data. The IT Act also contains provisions for data protection and privacy, though its scope and application are more limited compared to GDPR."

Adv Dubey also suggested while GDPR and the IT Act provide important frameworks for protecting data and privacy, their effectiveness in preventing government overreach in surveillance activities depends on robust enforcement, clear limitations on exemptions, judicial oversight, and ongoing updates to address new challenges. The arrest of Telegram CEO Pavel Durov highlights the need for continuous vigilance and adaptation to ensure that data protection laws adequately safeguard individual rights without stifling legitimate security measures.

Public awareness and education

Gautam Mengle, speaking to mid-day, noted, "Public awareness needs to be considerably increased. People have to know that their privacy is being violated for them to complain about it. Governments frequently claim to be conducting awareness programs, yet many individuals, particularly vulnerable populations such as seniors, are not reached. An effective campaign should use user-friendly platforms that target the appropriate demographic, ensuring that people are aware of the trade-offs between privacy and security."

When asked about how the public views the trade-off, Waghare said, "There is a wide spectrum of how individuals view the trade-off between privacy and national security. Some people don't fully understand the risks, while others feel defeated and believe that their data is already compromised, so there is no point in protecting it further. There are also those who mistakenly conflate privacy with secrecy, believing that if they have nothing to hide, there's no harm in being surveilled."

Waghare said, "A major challenge is raising awareness about the implications of privacy and surveillance. Literacy campaigns and public education could help, but there also needs to be a broader societal shift in how we view privacy—whether in the context of information, physical spaces, or personal communication."

He added, "Governments and corporations need to signal respect for privacy through regulations, laws, and responsible practices. Additionally, understanding the functioning of data brokers and how information is traded can help empower individuals to protect their data more effectively."

One of the significant gaps in awareness is the lack of research into how data brokers operate, particularly in India. Many people receive unsolicited calls from various services and wonder how their personal information was obtained. Investigating these data economies is crucial for understanding the full scope of how personal information is traded and used, and it forms a vital part of raising public awareness, he added.

"Exciting news! Mid-day is now on WhatsApp Channels

Subscribe today by clicking the link and stay updated with the latest news!” Click here!