Digital surveillance and Constitutional morality

Subhashis Banerjee
Department of Computer Science
Ashoka University
(on leave from IIT Delhi)

July 26, 2021

The recent allegations and reports by Arsenal Consulting and Amnesty International on targeted electronic surveillance of selected activists, politicians, journalists, businessmen and even scientists are disconcerting to say the least. Not only do the sophistication of the attacks engender a sense of resigned helplessness, but also the incidents – if true – have a chilling effect on personal and civil liberties that are crucial for a democracy to function. What is even more worrisome is that there seems to be a significant veiled popular opinion – among friends and families – that justify such transgressions in the name of national security.

If indeed the charges against some of the jailed activists in the Bhima Koregaon case are primarily based on evidences in the seized hard disks, then the Arsenal reports – if verified – should weaken the grounds significantly. According to the Arsenal reports there are clear evidences that the incriminating files were planted in the hard disks from remote command and control centres by unknown entities, even before the disks were seized, and that the activists were apparently not even aware of their existence. While some parts of Arsenal's forensic analysis were based on proprietary tools, several other aspects of the reports should be verifiable by independent experts – and there are many in India who should be able to do this – using publicly available resources. The offending files were apparently injected by planting a Trojan malware called NetWire by orchestrating some kind of phishing attacks on the unsuspecting activists. This kind of an attack is fairly standard and the presence of NetWire can apparently even be detected by some of the commonly available virus and malware scanners. Given that such attacks are a reality today, governments and legal authorities need to ensure that digital evidences arising out of such forensic analysis are admissible in courts.

In contrast, the Pegasus attacks described in the Amnesty International report are significantly more sophisticated, and defending against such attacks, even by careful and informed victims, is going to be almost impossible. They are 'zero click' attacks that do not even require a mistake by a victim to be successful. They exploit carefully analysed vulnerabilities in software and apps, or orchestrate network injection attacks through clever redirections using tactical devices, compromised network devices, or even rogue cell towers.

For example, they apparently exploited unknown vulnerabilities in the WhatsApp and iMessage apps to inject malware payload through fake WhatsApp videos and iPhone messages. For general purpose devices with a wide variety of applications, it is almost always going to be computationally intractable for the hardware and software designers to ensure that no compromised state can ever be reached. Hence vulnerabilities are inevitable, and some or the other can more likely than not be discovered if a large number of well-paid expert attackers have a go at things. Also, given the current legacy network access protocols, it is rather difficult to prevent a determined and resourceful attacker from successfully carrying out silent network injection attacks in commodity user devices.

Moreover, it is difficult to detect attacks like Pegasus' because they frequently change methods and signatures. Pegasus was apparently also designed to self-destruct on detection attempts, though according to the Amnesty report it did not entirely succeed and left traces. While one always theoretically understood the possibilities, that such James Bond-like tools actually exist and are used by governments is certainly an eye-opener.

So, what can be done? Can a data protection law help victims seek redressal and hold the perpetrators accountable as suggested by Justice Srikrishna (IE, July 23)? Perhaps unlikely, because for every instance of an Amnesty report there will likely be many more undetected instances of Pegasus-like infringements. Stealth attacks are not only difficult to detect but are also difficult to prove and easy to deny, so ex-post redressal will always be uncertain.

This is not to say that a data protection law is not required. Such a framework is essential for defining the contours of lawful surveillance and data processing. The state may have some legitimate requirements for surveillance if it has to keep us safe, but they cannot be outside the ambit of law. There can be no doubt that the country urgently requires surveillance reforms and data protection standards. However, for them to be effective, apart from analysing the proportionality of the surveillance requirements, they must also address the operational aspects of the legal and technical standards necessary for an effective privacy protection architecture. There has to be clear standards for defining authorisation chains and purpose specification, and technical guarantees for purpose limitation, access control and prevention of authorisation violations. This, in turn, would require maintaining tamper-proof logs, regulatory oversight and audit. The emphasis has to be on ex-ante prevention rather than on ex-post detection of violations.

But what if a malware injection and surveillance attempt as sophisticated as Pegasus' altogether bypasses the data protection architecture and regulatory oversight? Then, opposition from within the organisations, as well as strong public outrage and disapproval, can perhaps be the only effective deterrents for such misadventures. Without these neither law nor technology can be of much help. However, for such resistance to find sufficient voice, the society has to repose faith in Constitutional morality.

Right to dissent is a hallmark of democracy, and we must ultimately learn to distinguish criticism and protests from terrorism and other criminal acts. Unfortunately, in recent times, there have been significant erosion of Constitutional values, and they probably do not even teach the Constitutional principles in our schools any more. The commitment to the rights to free speech and liberty – as espoused in the Articles 19 and 21 of our Constitution – seems to be wavering not only in government functionaries and administrators, but also in the public at large. As such, combatting unlawful surveillance through stealth attacks and protecting privacy are going to be uphill tasks.