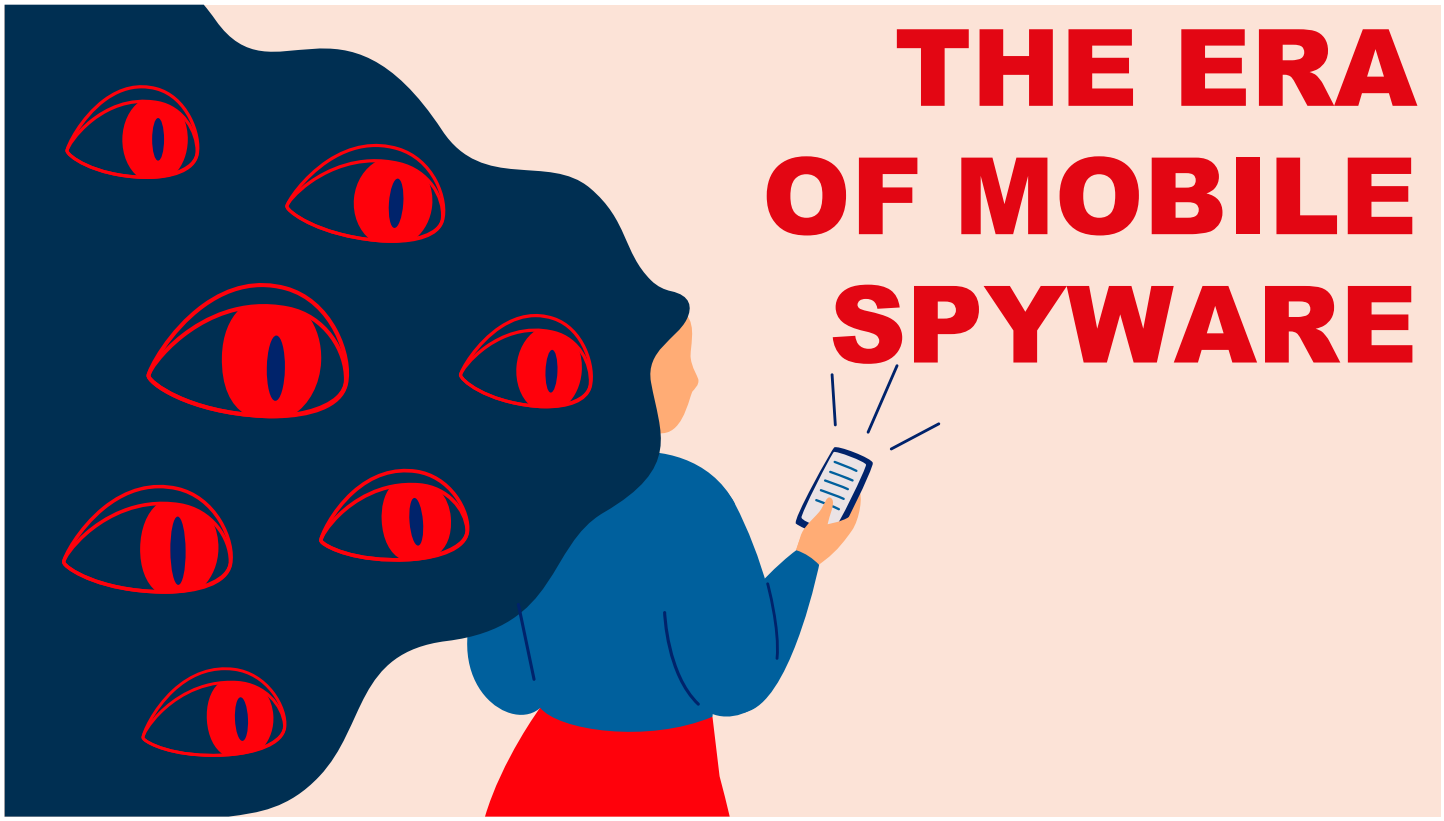

THE ERA OF MOBILE SPYWARE

Authored by: Nat Abramov - Crystal Vantage

In recent years a select group of specialised alumni from Israel's elite signals intelligence units have developed a globally game-changing cyber weapon: software capable of capturing virtually all data on a mobile device entirely undetected. It is hard to overstate the significance of this development on our societies. It has repercussions on the powers of law enforcement agencies, anti-terrorism and anti-fraud investigations, judicial authorities, the rule of law, right to privacy, and international diplomacy. Like with all new technology, there is a lag between breakout and a settled consensus on its use and limits. Recent events in Israel expose that gap vividly. This briefing draws on revelations of abuse of this technology in Israel, mobile spyware's maiden market, to reflect on wider questions around its impact on our private, professional and civic lives.

What is the latest mobile spyware?

Developed by a handful of Israeli cyber companies, the software exposes vulnerabilities in Apple's iOS operating system to grant an intruder access to a Subject's mobile device. Once a device has been penetrated, the software can collect passwords, location data, contacts, documents, photos and videos, audio and calls, emails, instant messages across all major platforms (including encrypted services), and a plethora of other stored data. This allows the intruder to harvest a device, and/or to monitor it live. Critically, most intrusions are zero-click, meaning no action is required on the part of the user in order to compromise their device.

The most high-profile developer of this type of mobile spyware is NSO Group, which was sanctioned by the US in November 2021 after it emerged that its platform Pegasus had been used to "maliciously target" journalists, activists, dissidents and government officials around the world. Several other lesser-known companies have developed similar tools, including the secretive Tel Aviv-based outfit Candiru.

Who authorises its sale?

Offensive mobile hacking software is considered in Israel a military product. Private companies wishing to sell these systems overseas require the authorisation of Israel's Defence Exports Control Agency (known colloquially as API), a unit of the Defence Ministry. The API committee includes representatives of Israel's main intelligence agencies and government officials. It is charged with determining whether the transfer of capabilities risks harming the state's interests, complies with its policies on arms exports, and/or risks falling into enemy hands.

In practice API has been willing to rubber stamp the sale of these systems to a wide group of clients overseas, including law enforcement and intelligence departments operating at the instructions of authoritarian leaders.

This unregulated system exposes a glaring inadequacy: a mobile phone belonging to an individual anywhere in the world can be hacked and harvested by an agency or police force of another country, so long as they have purchased a software licence from the Israeli private developer. The sole regulator of this technology is an opaque committee in the Israeli Defence Ministry. Neither the jurisdiction of the mobile phone user, nor the elected officials of the country where the law enforcement agency is operating, have the knowledge or power to prevent an intrusion in real time. Furthermore, states do not have the capability to disable the software from operating in their territories, or even to detect its use.

Who has the latest mobile hacking software?

Israeli providers of phone hacking technology predictably do not disclose their clients. Various leaks and forensic work by NGOs have exposed a partial list of law enforcement agencies, who are suspected of having acquired access. These include the CIA and FBI in the US; a series of European governments; the UAE, Saudi Arabia, Bahrain and Morocco; several Latin American governments, and other client states labelled high risk, such as Djibouti, Kazakhstan, Azerbaijan. Several of these states have been accused of dual use of Pegasus: to fight crime and to settle personal or political scores.

The list of countries whose agencies have phone hacking capabilities is constantly evolving and is being exposed periodically in piecemeal fashion. For a current snapshot, it is advisable to consult the latest available reports and Citizen Lab studies.

Can it be used against me and my clients?

If you have a smartphone and are involved in activities of potential interest to a law enforcement agency, the answer is yes. At present, there is no preventative way of avoiding abuse of the technology to target government opponents, personal or business rivals, their legal advisors, or individuals working on politically sensitive cases. The most prominent example of this is Fiona Shackleton and her legal team, who were targeted by Pegasus hacking from the UAE in August 2020. They were representing Princess Haya during her sensitive legal battle with former husband, Ruler of Dubai, Sheikh Mohammed bin Rashid Al Maktoum.

Following the Prince Haya case, NSO reportedly restricted the ability to hack UK numbers with a +44 prefix. Similar reports suggested it had barred hacking of numbers from the US, Israel and Five Eyes member states Canada, Australia and New Zealand. However, these claims are unverified, and it remains likely domestic agencies in these countries retain the ability to harvest devices in their jurisdictions. This raises a series of questions about the adequacy of laws and oversight processes in age of undetected mobile hacking and harvesting.

Who authorises the use of phone hacking?

Advanced phone hacking and harvesting can be commissioned by (a) a domestic law enforcement agency; or (b) an intelligence agency. Each country has its own rules on how these organisations gain permission to hack phones and under which circumstances.

In the UK, the police, NCA and intelligence agencies require a ‘double-lock’ warrant granted by the Home Secretary and approved by a Judicial Commissioner.

In the US, mobile wiretapping usually requires a prosecutor with Department of Justice to apply for a 30-day warrant from a federal judge. US intelligence agencies, however, have availed themselves of post-9/11 legislation, including FISA Amendments Act of 2008, to intercept communications overseas. As the Edward Snowden NSA leaks showed, warrantless wiretapping was not averted in real time.

In Israel, the police use phone hacking technology domestically based on warrants issued by a judge. Intelligence agencies deploy phone hacking technologies on overseas subjects using case-by-case orders signed off by the Prime Minister himself.

Are warrants fit for purpose or properly overseen?

Technology has moved far more quickly than the law in this regard. Countries around the world are using all-encompassing mobile phone harvesting and tracking technology on the basis of wiretapping warrants created at a time when agencies wished to listen to a phone conversation between two individuals. Some countries have created legal provisions for digital data interception, but neither the law nor its custodians are fit for the mobile hacking technology that state agencies currently possess.

Since the technology has only come into recent use, most law enforcement agencies have not yet faced scandals over the targets and methods of their phone hacking. There is little doubt these episodes will surface increasingly over time. In Israel, they are beginning to emerge.

Notably, Israeli police were recently found to have used mobile spyware beyond their permitted remit to harvest the mobile phone of Shlomo Filber, a key witness in the country’s high-profile corruption trial of former Prime Minister Netanyahu. The police’s wrongdoing may alter the trajectory of the most significant case in Israeli courts.

Israeli police been accused by the country’s leading business publication Calaclist of having used the technology improperly on mayors, politicians and other key figures. In one case, they allegedly discovered the homosexuality of a suspect who was married with children and used the revelation as leverage in his interrogation. These allegations were denied by Israeli police. A committee of intelligence experts assembled by the Attorney General recently cleared the police of material wrongdoing, save for small technical breaches of warrants. Many in Israel remain unconvinced that these tools are being used properly.

Anecdotal reports have emerged that some overseas law enforcement agencies turned to NSO informally to gather information from a suspect’s mobile. NSO is then said to have handed over incriminating material to support a local warrant application. The practice is a clear circumvention of the prohibition on “fishing expeditions”, a proud fixture of many legal systems around the world.

Fundamentally it is impossible to know how many agencies worldwide are overstepping their phone hacking powers. A component of the problem is the inadequacy of the warrant approval process. An Israeli judge who had previously granted hundreds of wiretap warrants was recently disclosed that judges in his position simply did not understand the capabilities of the new mobile hacking technologies whose use they were authorising. He alleged that requesting authorities would frequently fail to make it clear to judges that their warrant would be used to harvest a phone, to turn on its microphone and camera, to extract deleted WhatsApp messages, to gather emails, and to extract a huge range of other data that would "strip naked" the user of the phone.

A reality in which judges do not fully appreciate the application and purpose of their warrants encompasses a major vulnerability. This stands to be exploited by agencies keen to secure authorisation to use their tools unabated. There exists a clear risk that agencies withhold from judges the capabilities of their new tools, thereby avoiding any uncomfortable lines of questioning and preserving an "old world" perception of what wiretapping allows them to do.

Plainly, there does not exist in any jurisdiction at present an effective system to ensure an agency performs only what the judge intended to permit them to do with a mobile device.

In the UK, the tendency for agencies to over-interpret their powers was laid bare in a recent challenge to their use of hacking warrants. It took a High Court petition by an NGO in *Privacy International v. Investigatory Powers Tribunal* to establish that intelligence agencies could not use 'general warrants' allowing mass data hacking of a whole class of property to compromise the devices of specific people. Agencies had hitherto used these warrants, issued by the Secretary of State and not a judge, to hack individual devices. Until the successful High Court action, these agencies had also been backed to engage in this practice by the intelligence oversight body, the IPT.

In the US, there remains legal ambiguity around the permissibility of warrantless wiretapping on foreign nationals for national security purposes. This leaves open a lacuna for US agencies to hack the phones of individuals around the world without any judicial involvement or oversight.

What happens to data harvested from phones?

The materials recovered from a mobile device by a police force or agency are at the behest of the organisation that collected it. In ongoing investigations, or cases that reach prosecution, relevant data is naturally preserved as evidence. But the fate of the mountain of surrounding data that has been collected, particularly in cases that have been closed, remains an under-scrutinised topic.

In jurisdictions that have strict privacy laws, agencies are bound by the relevant local legislation and data regulators. In January 2022, the European Data Protection Supervisor made a landmark decision to order Europol to delete a large part of its big data ark, which was drawn from a range of sources including hacked mobile phones. Similar provisions may apply to agencies at a national level, in accordance with domestic laws and regulations.

However, most jurisdictions around the world where government phone hacking is used have neither strict data protection laws nor regulators with teeth to compel agencies to destroy data that is no longer relevant. There is good reason to believe that sensitive data is widely retained. The recent account of a former investigating police officer in Israel suggested that agencies kept troves of harvested mobile phone data on file as intelligence, available to be called upon if necessary in subsequent investigations.

This paints a sobering picture: our devices are vulnerable to hacking from agencies overseas, who may continue to hold our sensitive data indefinitely without our knowledge and without meaningful oversight.

That data may re-appear in the context of future investigations, or may simply sit as one of billions of other data points in government databases.

What can we do to protect ourselves?

In responding to the new reality of advanced phone hacking and harvesting, the first imperative is awareness. Given even encrypted communications can now be remotely intercepted, it is prudent for individuals working with sensitive data, and their clients, to take precautions to limit risk of compromise. Advisable steps include:

A. Keeping sensitive and confidential information off mobile devices. Matters that can be discussed in person, or on a secure video link, are better done through those mediums than via a recoverable message trail.

B. Periodically deleting non-essential data from communication platforms on a device, including email, WhatsApp, Signal, Telegram and Wire.

C. Wherever possible, applying the potential leak test: would you be prepared for the information exchanged to surface with a law enforcement agency, newspaper, or court of law. If that creates discomfort, an alternative means of secure information exchange is preferable.

Additionally, there is a pressing need to regulate the availability and use of phone hacking and harvesting tools. Below are initial suggestions:

A. Adoption of international standards and oversight mechanism to approve the agencies that are granted access, and to ensure their appropriate use of the technology.

B. Limitations on the operation of phone hacking and harvesting tools out of jurisdiction. Providing a kill switch to senior authorities, elected officials, or parliamentary oversight committees to disable access in the case of abuse.

C. A review in all relevant jurisdictions of the warrant process, including updated guidance to judges, and oversight of agency compliance.