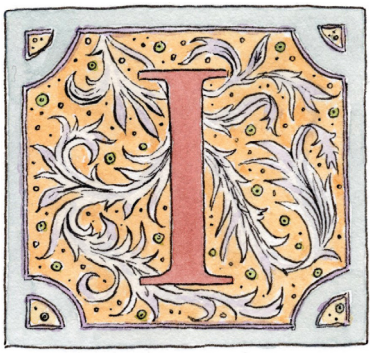
TEHILLA SHWARTZ ALTSHULER

Israel's Snowden Moment



IT IS WELL KNOWN that smartphones can serve as mobile surveillance devices, leaving a trail of digital breadcrumbs that reveal much about our behavior and preferences. It is also widely known that the Israeli tech company NSO created a form of spyware called Pegasus, which enables remote access to mobile devices. It can operate on a "zero-click" basis, precluding the need for clicking on a link or opening an email. Once the spyware embeds itself within a device, it can access virtually everything: emails, WhatsApp messages, social-media interactions, photos, geolocation data, documents, notes, and metadata. It can even remotely activate the phone's microphone and camera. Essentially, Pegasus provides an intimate window into our digital hearts and minds.

For years, the State of Israel has presented Pegasus as a kind of diplomatic gesture to various fledgling democracies and authoritarian

regimes. Observing Prime Minister Benjamin Netanyahu's diplomatic endeavors from 2015 to 2021, one could discern a striking correlation between his visits to countries such as India, Hungary, Mexico, Saudi Arabia, Morocco, and the United Arab Emirates, and the subsequent deployment of NSO surveillance licenses. As one joke had it, Netanyahu rode to the Abraham Accords on the back of a Pegasus.

It's also no secret that Pegasus was deployed in the Palestinian territories: Traces of the software had been detected on devices belonging to individuals from various organizations, some of which are labeled by the government as terrorist organizations. However, like many others, I had rationalized that such measures, taken in the name of combating terrorism and ensuring security, occasionally necessitated compromising individual privacy.

Then, at the outset of 2022, came Tomer Ganon's startling revelations, in the Israeli business paper *Calcalist*, about the Israel Police's own use of Pegasus.

Ganon's explosive investigation — worthy of a Sapir Prize, the Israeli equivalent of the Pulitzer — prompted me to tell Israeli news platforms that this revelation was a watershed moment for the police and the attorney general entrusted with overseeing such operations. They needed to reconsider the legality of their actions. What neither I nor my fellow digital-rights advocates in Israel had anticipated was the momentum our efforts would gain when it was revealed that the spyware had been deployed against Shlomo Filber, one of the state's witnesses in Benjamin Netanyahu's trial.

During recent deliberations in the Knesset's Constitution, Law, and Justice Committee, proponents of privacy and civil liberties

found themselves allied unexpectedly with committee members on the Right who were criticizing the police and the State Prosecutor's Office for illegal surveillance. By late August, the Israeli government established a governmental commission of inquiry into the police's use of Pegasus, implicitly granting the commission the authority to probe Pegasus's involvement in the ongoing cases against Netanyahu.

It's certainly ironic: Netanyahu, who utilized Pegasus for political advantage, now contends that the very same tool precipitated his domestic downfall. He clearly now hopes that the revelations, adding another layer to the narrative, will turn his legal situation around, allowing him to emerge relatively unscathed by showing that his accusers engaged in unauthorized surveillance.

But the Pegasus revelations are not the only recent exposure of the remarkable surveillance powers of the Israeli authorities.

In the wake of the initial outbreak of the Covid pandemic in March 2020, Israel activated the Shin Bet surveillance "Tool," as it is known, to facilitate contact tracing by identifying potential virus-transmission chains. The Tool is a database populated with data on everyone who uses telecom services in Israel — data on the location of every device, the cell and antenna zone to which each is connected, the metadata for every voice call and text message each sends or receives, and each one's internet browsing history. Alarmingly, the health authorities provided the Shin Bet with the names and phone numbers of people who tested positive for Covid and asked to get a list of those who were nearby. Tasking the Shin Bet with digital contact tracing was a drastic and unparalleled step. Never before had the Shin Bet been utilized for domestic surveillance on such a grand scale. Regrettably, those in power deemed this encroachment upon the constitutional right to privacy entirely warranted by Covid. More than three years later, it remains the most intrusive surveillance measure adopted by Western countries throughout the pandemic.

The Tool became public knowledge when journalist Ronen Bergman published an exposé in the *New York Times* and *Yediot Ahronoth*. When I wrote about it some months later, I assumed that unveiling a surveillance apparatus arguably more invasive than the one brought to light by Edward Snowden would make waves. I was wrong. Perhaps this was because Netanyahu himself had authorized its use. Or perhaps, as Thomas Hobbes noted, the fear of death is an extraordinarily potent political motivator.

Now we have had our second "Snowden moment." Will things change? However history judges the use, for good and ill, of the extraordinary technology powers Israel has developed, this series of events has made clear to the Israeli public that issues of privacy and surveillance transcend conventional political dichotomies.

To grasp the essence of Israel's two Snowden moments, you have to understand the phenomenon of "function creep," the expansion of a technology beyond its intended purpose. In Israel, we see three main kinds of function creep — from one kind of *territory* to another, one kind of *target* to another, and one kind of *user* to another.

Territorial creep. The most prominent example of this in Israel is the shift from using technology in the occupied territories to using it within Israel proper. For instance, in 2021, the *Washington Post* spotlighted Blue Wolf, a facial-recognition application enabling IDF soldiers to capture images of Palestinians, with which they populate a growing biometric database. By 2023, the Israel Police was contemplating its deployment to pinpoint disruptive soccer fans.

Target creep. Function creep also manifests itself when intrusive surveillance systems, ostensibly designed for combating grave threats such as terrorism and pedophilia, are rechanneled to suppress pro-

testors, regulators, or human-rights advocates — as evidenced by the use of Pegasus in countries such as Mexico, India, and Hungary. A variation on this theme concerns the seep of security technologies into civilian realms — for example, when military intelligence-gathering techniques are utilized in the commercial world. Harvey Weinstein employed BlackCube, an Israeli investigatory firm, in an attempt to prevent the publication of a *New York Times* article that revealed the sexual-misconduct allegations against him that sparked the #MeToo movement. BlackCube's staff consists largely of Mossad alumni.

User creep. The most prevalent creep today is the transition from civilian applications to security or law enforcement. The Tool, for example, functions thanks to a confidential appendix within Israeli cellular-company licenses. Citizens sign contracts allowing companies to collect and retain specific metadata for a set period. But the Shin Bet can access and use this data for extended periods for security reasons. We also see this kind of creep when ancestral research services collect genetic data, or when companies utilize sensors for tracking athletic metrics and then share this information with intelligence or law-enforcement agencies. With the rise of what Shoshana Zuboff has termed "surveillance capitalism," which generates vast quantities of data on consumers, creep of this kind by law enforcement and security agencies has become a serious threat.

Obviously, there are overlaps among these kinds of function creep. What should be clear is that the two Snowden moments noted above are glaring examples of a slippery slope: It seems that any invasive technology sanctioned for use in the Palestinian territories will eventually be used against the Israeli public, and tools designed to protect the country's citizens will inevitably turn upon dissenters and political adversaries.

When surveillance technologies meet privacy rights, the degree of

privacy intrusion hinges on myriad factors. These include the nature of the technology, the data collected, how it is acquired and processed, who gets to access it, how securely it is stored, how long it is retained, and what it is collected and used for. A given technology's application might be deemed appropriate in one context, but as it creeps into another domain, it becomes essential to scrutinize, regulate, and oversee its use.

Part of the problem is that function creep is gradual and incremental, occurring without full consideration of the inevitable problems that follow. Typically, a technology first makes its way into an unintended domain without a clear mandate, or based on broad legal interpretations, often of archaic laws ill-equipped for current technological advancements. Only when thrust into the spotlight — whether through media revelations, court decisions, or public outcry — does the march toward comprehensive statutory regulation commence.

But when function creep occurs covertly and goes undiscovered, this process is delayed — and, crucially, incomplete. It's rare for powerful surveillance programs — especially ones the public doesn't know about — to be scaled back. None of this relieves us of the challenge of establishing the right balance among competing values and ensuring that technologies are used in a proportionate and appropriately monitored fashion.

Israel's Basic Law: Human Dignity and Liberty, from 1992, upholds the right to privacy. This law is Israel's closest equivalent to a Bill of Rights. But this constitutional foundation is only the start of any serious dialogue about privacy. The right to privacy in Israel is shrouded in ambiguity, a situation exacerbated by the nation's open and informal culture and the prevailing sentiment of prioritizing security above all. Today's Israel lacks an updated privacy-protection law akin to the progressive frameworks of California's Consumer Privacy Act (CCPA) or Europe's General Data Protection Regulation (GDPR). Also absent

are preemptive mechanisms to guide the acquisition and deployment of surveillance technologies before their actual implementation, a norm in cities such as New York and San Francisco.

Furthermore, internal organizational oversight invariably falls short. Examples include the Shin Bet's legal counsel, which legitimized the preliminary usage of the Tool for contact tracing, and the Israel Police's sanctioning of Pegasus. External oversight mechanisms are also flawed — whether they be the attorney general, the judicial bodies that increasingly act as a rubber stamp in approving surveillance orders, or Knesset committees that have demonstrated a reactive and superficial approach.

Now that the overreach of Pegasus has become public, we see the usual finger-pointing and assignment of blame. The focus is on who procured the spyware, who oversaw its use, whether that use was legal, whether judicial authorization was obtained, and whether the court orders were lawful. These are valid concerns, but they merely scratch the surface. The crux of the matter is a profound gap in understanding the intricacies of cyberspace. In 2011, Michael Hayden, a former head of both the National Security Agency and the Central Intelligence Agency, noted: "Rarely has something been so important and so talked about with less clarity and less apparent understanding than this phenomenon." Hayden wasn't talking about specific technologies or tactical operations. He was lamenting the absence of a broader conceptual framework that would allow us to comprehend and therefore debate the ramifications of technological tools.

Cyberspace blurs conventional lines: between criminals and police, allies and adversaries, cyber offense and intelligence collection, private and public. Coupled with the resulting ambiguity is a

shortage of historical and practical experience. This is not surprising, given the relative novelty of cyberspace and the fact that many decision-makers are "digital immigrants." But that does not make it less serious. Further, this deficiency in understanding is evident across the board — among politicians, military leaders, law enforcement, judges, legal advisers, and more.

This digital illiteracy puts us at an extraordinary disadvantage in both grasping the implications of technological systems and envisaging their potential. There are many digitally literate people involved in cyberspace activities, but they are generally the ones promoting new technologies, rather than worrying about whether and how to use and monitor them. As we grapple with this issue, urgent social questions come to the fore. Should the police ever be permitted to engage in vast data-fishing expeditions? Should they ever view public domains as open playing fields for unrestricted surveillance? Is there a case, in a free society, for the police to collect sensitive personal information, such as sexual orientation, even if it comes from data in the public sphere?

While technology often outpaces regulation, the core of the issue remains constant. Today's concern might be Pegasus; tomorrow, it could be artificial intelligence predicting crime based on ethnicity. The digital era has blurred the lines between intelligence gathering and police investigations: Both now harness similar tools within similar spheres. And current worries about law enforcement and its appropriate limits hardly begin to describe the problem: Why not make use of available technologies, simply for efficiency?

If we are to solve these problems, we need to understand that the primary argument is not about the legalities of any particular case. Rather, the key question is "Who should have access to these technologies?" Only once this is publicly clarified should we ponder the development of legal regulations.

I say *should* because there are moral and ethical considerations involved. Historically, the significant roles played by veterans of the IDF and other security entities in Israel's thriving tech ecosystem — an ecosystem in which Israel leads the world, enormously bolstering the nation's economy and prestige — have led us to be complacent about the murky waters into which we are wading. It is well past time to address the difficult questions involved.

It's a common belief that the genie is already out of the bottle. All our data is out there, the tech companies already know every detail about our lives — perhaps we have nothing left to hide. That may be true. But the implications are far graver when the police collect the data in question. Such data, whether collected "honestly" or via function creep, has potent consequences as they morph into evidence, leading to investigations, arrests, and penalties.

Israel's recent Snowden moments underscore the shift from the privacy encroachments of commercial enterprises, driven by the logic of capitalism, to the state's overt and covert surveillance measures, evoking not Adam Smith's invisible hand but George Orwell's Big Brother. The terror of Big Brother is that its knowledge of every detail of our daily lives can be turned on any of us, at any time. The good news is that we have not yet quite arrived at a point where Orwell's vision is today's reality. If we are vigilant, it is not too late to maintain appropriate limits and even roll them back where they have overreached. To do that successfully, we must broaden the frame from questions of what is legal to questions of what is moral and ethical, and beyond — to broader issues of democracy and threats to democratic systems of justice. ✳