Privacy in Peril: Rise of the Surveillance State

It was almost 75 years ago when *1984* was written prophetically by Englishman, George Orwell in 1949. Orwell depicted a dystopian vision of the future in which the state controls its citizens with a vice-like totalitarian grip. Perpetual war exists between two main nation states. Society is subject to mass surveillance, brainwashing and propaganda while its citizens may be tortured and killed if found guilty of "thoughtcrime", ideas that challenge and go against the Party. According to Andrew Bernstein writing in his article, *The Terrifying Prescience of George Orwell's 1984,* published in *The Objective Standard,* the author has foretold of many problems that exist in today's world (2023). A new lexicon was delivered in the seminal text that has come into being; *Big Brother* (see fig. 1) is the state watching and listening through CCTV's, webcams and microphones while *doublethink* is the contradictory control of information. *Newspeak* is an apt analogy for fake news, while *The Ministry of Truth* elevates propaganda over knowledge, just like corporate news channels do today. Ironically Bernstein has written, "it is unlikely that, in real life, a totalitarian state could develop a two-way tele-screen technology, enabling its agents to spy on every person every second of the day," as is featured in the novel. The term spyware is not mentioned once. This well-read writer has failed to connect the concept of "*camfecting*", the ability to hack into a computers webcam and access the camera and microphone without alerting the user, such is the clandestine nature of this technology. The FBI stated in *the Washington Post* in 2013 they've had this ability, which can be weaponized as malware, for several years. Not so long ago those who covered their webcams at the office were ridiculed as paranoid, despite Facebook founder Mark Zuckerberg being famously photographed with his webcam covered in 2016. Only now with a 2023 expose by *Frontline* and *Forbidden Stories*, a consortium of French journalists based in Paris, has the extent of the use of Pegasus spyware been uncovered. This has enabled more scrutiny from authorities and an increased level of awareness for the public.

Orwell's *1984* is happening right now. In this new hyper-connected world individuals must be empowered to fully understand the capabilities of the technology they wield, along with its shortcomings. If systems cannot be fully secured this should be plainly disclosed. Consumers must demand that tech products adhere to strict security standards that cannot be easily breached. As such governments and corporations must be held to account so that the basic principles of personal privacy remained enshrined as fundamental inalienable rights. If the capabilities are found to be too powerful for responsible use the spyware should be heavily restricted or banned.

Fig. 1. Illustration of Big Brother propaganda poster from George Orwell's *1984.*

As highlighted in the stunning Frontline special, *Global Spyware Scandal: Exposing Pegasus,* the software is far beyond global regulation and public perception, in terms of its capabilities. Over the course of a year the Pegasus spyware and its Israeli makers, NSO Group, are investigated. Both iPhone and Android devices are vulnerable. Once infected by a malware message, that does not require an active click, all content may be accessed, such as location, images, emails, messages, in-app communication, camera, microphone, even deleted messages (see fig. 2). An important link is established between Pegasus and the murder of Jamal Khashoggi, a *Washington Post* journalist known to be critical of the Saudi Prince, at the Saudi

consulate in Istanbul in 2018. Evidence of the spyware is located on Khashoggi's widow's phone in the documentary. This is a process that technologists and investigators can employ using the Mobile Verification Toolkit or MVT, a project developed and released by the Amnesty International Security Lab in July 2021. Technologist Bojan Jovanovic explains on DataProt.com how command-line tools are required, meaning it is not intended for typical end users. Due to these important human rights implications Amnesty International has taken the lead with this issue providing significant resources in the form of detailed reports of misuse, the aforementioned tools for detecting the software and a hub for tracking breaking information connected to the spyware. Amnesty International has been tracking the misuse of Pegasus in relation to ongoing human rights violations since 2016. NSO group insists the software is only used to investigate terrorism and crime yet it is highly problematic when the software is provided to authoritarian regimes such as Saudi Arabia or the United Arab Emirates.

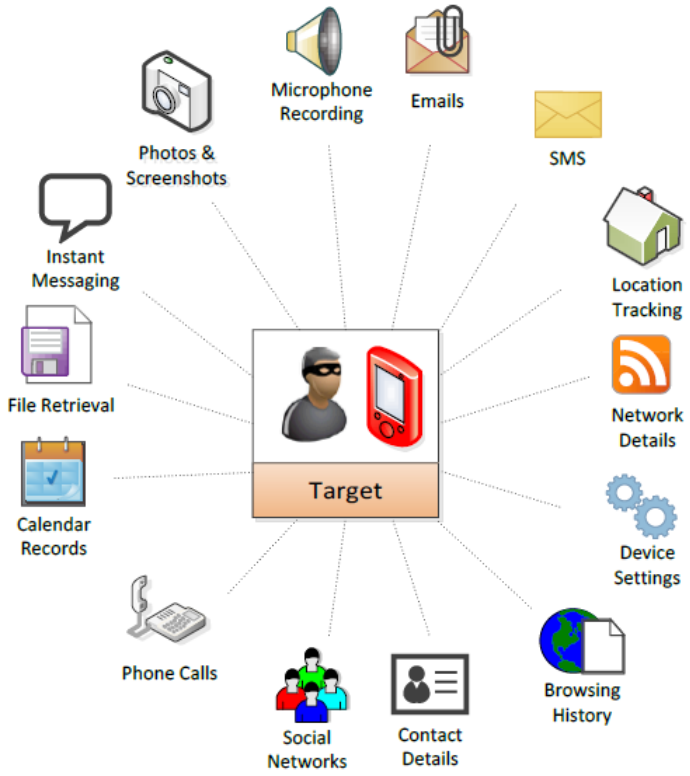

Fig. 2. Once targeted and infected all of a user's content may be accessed with Pegasus.

The atmosphere in which software like this can be developed is examined in detail and the integrity of Israeli Prime Minister Benjamin Netanyahu, and his allegiance to military interests, questioned. The case is made that members of the Israeli military are encouraged to maintain important relationships as they leave the governments employ. This may take the form of companies who are well funded by, and in alignment with, government armed forces. During an interview in 2019 advocating for financial support for the cyber security industry, whilst simultaneously extoling the virtues of minimized regulations for the same sector, Netanyahu seems to inadvertently made a Freudian slip, "it's like [regulating] weapons… it *is* a weapon!". Having such a tool in its arsenal only adds to the power of an established or emerging regime. By tracking Netanyahu's global movements on diplomatic visits, to Hungary for example, the roll out of Pegasus has been detected in the same country not long after. In other instance this has occurred in reverse, whereby a dignitary has come to Israel to make a diplomatic visit, and soon after Pegasus activity is logged originating in that particular country. Despite evidence to the contrary of the spyware being used as diplomatic currency NSO Group denies this vehemently and is quoted as saying Pegasus, "is not a tool for Israeli diplomacy (…) is not a backdoor for Israeli intelligence [and], does not take direction from any government leader."

One of the most notorious cases of the spyware's successful use is in the capture of Joaquín Archivaldo Guzmán Loera, otherwise known as El Chapo. Newly crowned as public enemy number one after the death of Osama bin Laden in 2011, the software was acquired by the Mexican government around the same time. According to Bojan Jovanovic writing on the security website *DataProt.com*, by using "off-center" targeting, the practice of hacking the devices of friends, relatives or anyone close to the target, in this instance well known Mexican-American TV actress Kate Del Castillo, an individual may be easily compromised (2023). This ultimately led to the capture of El Chapo, who was in contact with Castillo and Sean Penn while

in discussions to make a program based on his life (see fig. 3). Mexico is singled out as having used the software extensively as a test market. According to Nina Lakhani writing in the Guardian, a Mexican journalist named Cecilio Pineda Birto was murdered in 2017 hours after making a report accusing state police and politicians of colluding with violent local gangs. It was alleged that Birto's phone number was selected to be surveilled by a Mexican client of the NSO Group. Contradicting claims from the company, that only criminals are targeted, at least 26 Mexican journalists phone numbers were discovered on the leaked list. Lawyers for NSO Group commenting on the case revealed, "even if" his phone had been targeted,

> "that does not mean that the NSO Group client or data collected by NSO Group software were in any way connected to the journalist's murder the following month. Correlation does not equal causation, and the gunmen who murdered the journalist could have learned of his location at a public carwash through any number of means not related to NSO Group, technologies, or its clients." (2021).

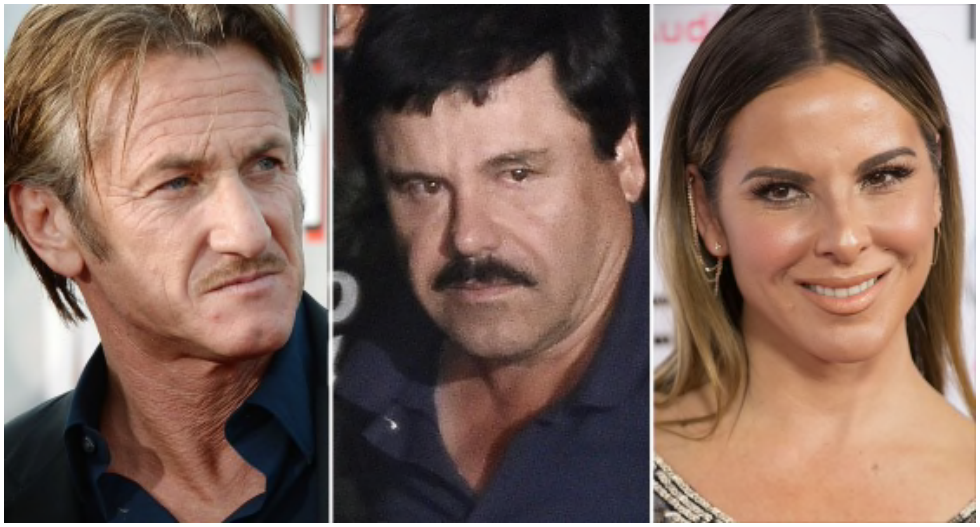

Fig. 3. Sean Penn, El Chapo and Kate Del Castillo, whose phone was infected with Pegasus and used to capture El Chapo (2016).

Even with the capture of El Chapo, “the worlds’ most wanted man”, the company’s strenuous denial raises more questions than it answers. Prominent journalists from around the world are well represented on the list of about 50,000 hacked phone numbers discovered by *Forbidden Stories,* including about 15,000 from Mexico. Extensive cross-referencing was used by the investigative team to track down owners of the compromised numbers shown to include activists, lawyers, reporters and family members connected to these individuals. Murdered Mexican journalist Cecilio Pineda Birto was eventually found among those on the list (see fig. 4). In his final report Birto promised to reveal key players behind corruption in local law enforcement and government. He was killed before he got the chance. Mexico is the world’s most dangerous location for reporting outside of warzones. Those who are most at risk are the correspondents covering webs of organized crime connected to security forces, cartels and politicians. To confirm if Pegasus has infected a particular user’s device it must be examined. In Birto’s case his phone was never located.

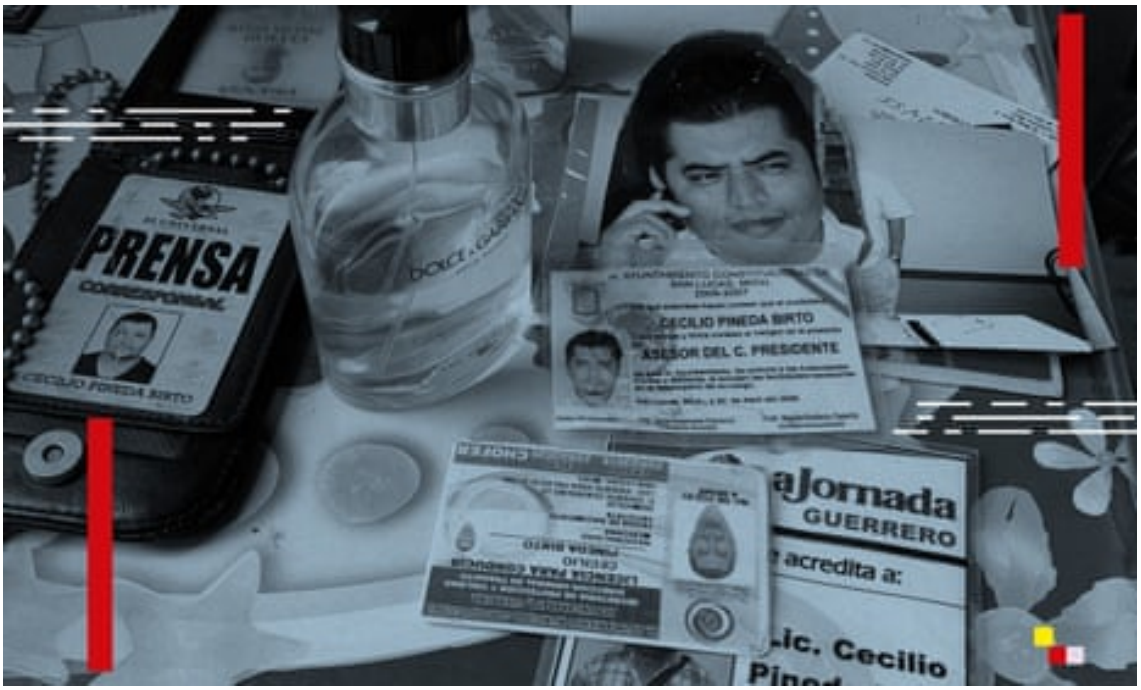

Fig. 4. Mexican journalist Cecilio Pineda Birto’s press credentials among belongings kept by his widow.

Among the 50,000 numbers discovered around 1000 were found to be French with up to 14 government ministers shown to be connected. Even French President Emmanuel Macron's phone number was discovered among the compromised numbers on the list (see fig. 5). When the team from French Newspaper *Le Monde* contacted the president's number to see if it was still active his team responded confirming the number was correct. Within a few hours the *Le Monde* journalists are invited to Elysée Palace to discuss what they have discovered. The full implications of high-level politicians and officials being compromised in this way are unimaginable, especially if the nation states using the spyware are in conflict or at war. Writing for *CNET* in his article *Pegasus Spyware and Citizen Surveillance: Here's What You Should Know*, Stephen Shankland points out that of the 37 phones that Pegasus software was discovered to have been installed on, 34 were Apple iPhones. Security features developed in 2022, and put into Apple's iOS 16, were intended to patch the vulnerabilities being exploited, though this is an ongoing game of cat and mouse that clever engineers usually circumvent. It's not a matter of if your operating system will be breached but when. This hasn't helped Apple's reputation and the company has since donated $10 million towards online surveillance research, which may be considered an unimpressive amount when offset against quarter earnings that frequently exceed $20 billion. The nature of the high-profile targets and exorbitant cost to implement dictates that the likelihood Pegasus would be used, on a typical US citizen for example, is low. Learning that individual privacy may be invaded to this extent is still chilling. Edward Snowden may be regarded as an industry insider and authority on this subject. After notoriously whistleblowing with leaked information about US National Security Agency surveillance practices, he recently called for a ban on the sale of the invasive software. Snowden reasons logically, "When we're talking about something like an iPhone, they're all running the same software around the world.

So, if they find a way to hack one iPhone, they've found a way to hack all of them." (2022). He makes a lucid point.

Fig. 5. “France’s Macron Tapped as Potential Target for NSO Spyware, Investigation Reveals.” *Haaretz.Com*, 20 July 2021

Since the groundbreaking documentary was released and follow up investigative work has gone forward a number of agencies have sprung into action responding to this rising threat to privacy and civil liberties. The US government in particular cut off NSO Group (see fig. 6) as a customer of US products, which includes phones and computer processors, that it uses to make its spyware. The US commerce department declared, “These tools have enabled foreign governments to conduct transnational repression,” recognizing that government officials, business people, activists, embassy workers and academics around the world have been targeted maliciously. Ursula von der Leyen, European Commission chief, announced if the allegations were proven Pegasus use is totally unacceptable and completely at odds with the core values of the EU. These include freedom of media and a free press (CNET, 2022). Apple sued NSO Group

in 2022 seeking to bar the company from using their software on their devices following a similar suit from Meta's wildly popular messaging and phone application, WhatsApp, in 2019. In January of 2023 the US Supreme court rejected an appeal from NSO to stop the case from moving forward. The argument that NSO Group tried to make, that they are entitled to immunity as an agent of a foreign state, is heavily contested as "baseless" with Meta declaring, "We firmly believe that their operations violate US law and they must be held to account for their unlawful operations." (Reuters, 2023).

Fig. 6. NSO Group is under fire for providing Pegasus spyware to different global governments and their agencies who have been found to have misused the software.

It is apparent that governments and technology companies alike are paying attention to this fluid surveillance situation as new information comes to light. The public is slowly awakening to the level of power that current spyware systems possess yet there is a whole generation of children and young adults who have grown accustomed to using technology ad infinitum. Especially now there are popular innovations available such as the Apple Watch, that can track a wearers heartrate and geolocation simultaneously. Even Amazon's popular digital

assistant Alexa has been caught spying on behalf of big tech. The Amazon Echo, Dot and Show devices are known to record and store conversations which will be analyzed by a computer, and maybe even a human, later down the line. There's no way to know if, how or when. Alexa is beholden to algorithms designed to learn human behavioral patterns and movements through repeated vocal commands. According to Grant Clauser, writing in the *Wirecutter* section of *The New York Times,* Amazon responded to criticisms by giving users the option to prevent human screeners. Users can achieve this by going to the Privacy section of the settings menu and deselecting the "allow recordings for Alexa developers" option. Google has had similar issues, according to the same *Wirecutter* article, with sub-contractors having been found listening to Google Assistant voice recordings that were captured accidently. Google has assured users and technology observers the recordings are not associated with individual accounts and are completely anonymous. Apple's Siri recordings are also stripped of identifiers, though kept for up to two years on servers. Human "grading" has been suspended from Siri's infrastructure until the process has been reviewed (2019).

Where technology has been embraced at large by society as desktop computers, laptops, mobile phones and smart products have become ubiquitous a system of check and balances must be implemented with a healthy dose of skepticism when approaching new products. When Google and Facebook exploded onto the tech scene generating capital was not included in the mission statement, nor was it explicitly stated as a primary goal of either entity. These companies were built on a youthful wave of innovation and new utopian, if somewhat naïve, visions of interconnectedness. The way information is gathered and shared has been altered completely in the last two decades yet it has occurred incrementally. Shifting financial landscapes have driven company interests to incorporate these powerful tools into their business models. Today many entities cannot survive without them. As corporate America came to invest and benefit from the

huge profits available in the tech sector it was open season. Now a nexus point has been reached where the power available to nation states through technology is so immense that profit driven motives are not enough to keep societal forces in check. Human considerations must become a larger part of the technology equation for improved outcomes. The pursuit of unlimited growth rather than sustainability, has shown to be capitalism's greatest weakness. Technology far too often is designed and manufactured primarily to enhance the producers share price rather than to improve life for the consumer. In this unbalanced environment new devices are inherently easy to compromise while the temptation to do so, for those seeking profit or strategic advantage, is simply too great. NSO Group is just one player in the space who has tried to fill that gap.

Visions of Orwell's dystopian future, imagined halfway through the last century, can be seen most clearly in current day China where artificial intelligence and biometrics have been harnessed to frightening new heights. Enhanced levels of surveillance have been deployed on their population en masse. According to a recent *The New York Times* article Chinese authorities position cameras where they can capture the maximum number of faces in crowded areas. Smartphone trackers, known as WiFi sniffers and IMSI catchers, glean details from nearby user's phones. Law enforcement agencies attempt to links people's digital lives to their physical movements. Male DNA samples, with Y chromosome data related to multiple generations, and indiscriminate iris scans, are being taken from non-criminals. All of these innovations are intended to connect a series of data points collected on an individual to build a comprehensive profile. That profile may be accessed on a nationwide database (Qian, et al., 2022). In a multitude of ways Orwell's worst nightmares have been realized yet he did provide prior warning in writing. Those who have been paying attention will appreciate that the current social climate has been a long time coming, with the tell-tale signs of totalitarianism having been easily detected. The best defense is to develop a greater understanding of the political and social

ramifications of unchecked technological innovation with minimal regulation, before it's too late. Humankind's next round of lifechanging solutions are going to be generated by AI in conjunction with emerging green technology. As caretakers of the human genome it is the responsibility of those who possess the intellect and the willingness to ensure the sanctity of the species is protected, through exercising basic rights to life, liberty and happiness, with privacy acknowledged as an indispensable component. This is a once in a century opportunity to harness the wealth of human evolution for the good of society, through technology. The power to listen to, and observe, a neighbor undetected may have been revealed due to recent advances. That does not necessarily mean that power should be exercised. There are times when common sense and basic courtesy do apply. Morally speaking eavesdropping simply isn't polite or civilized, nor is it needed, unless under extreme circumstances. It may not be justified at all. Albert Einstein summed up humankind's complex relationship with innovation perfectly saying "The human spirit must prevail over technology." It would be wise to remember and heed his timeless words.

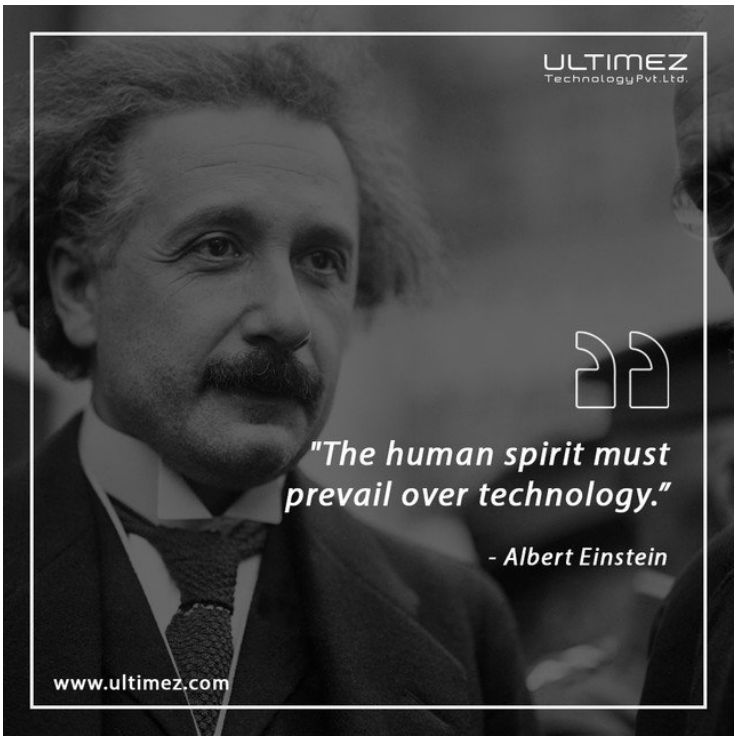

Fig. 7. "The human spirit must prevail over technology." - Albert Einstein

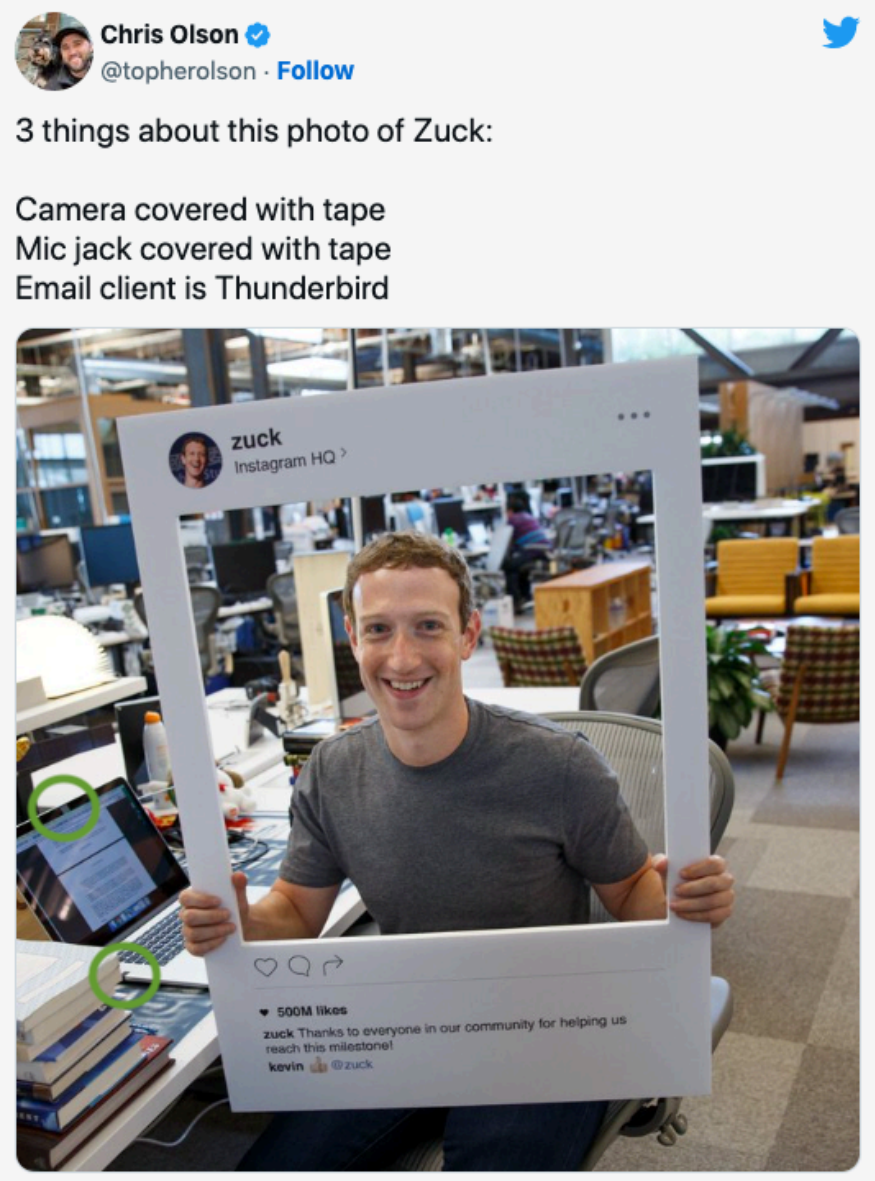

Fig. 8. “Mark Zuckerberg Tapes over His Webcam. Should You?” *The Guardian*, 22 June, 2016.

Works Cited

Benjakob, Omer. "France's Macron Tapped as Potential Target for NSO Spyware, Investigation Reveals." *Haaretz.Com*, 20 July 2021, www.haaretz.com/israel-news/2021-07-20/ty-article/frances-macron-tapped-as-target-for-nso-spyware-by-moroccans-investigation-revea/0000017f-e3f2-df7c-a5ff-e3faed8c0000.

Bernstein, Andrew. "The Terrifying Prescience of George Orwell's 1984." *The Objective Standard*, 6 Mar. 2023, theobjectivestandard.com/2023/02/the-terrifying-prescience-of-george-orwells-1984/.

Clauser, Grant. "Amazon's Alexa Never Stops Listening to You. Should You Worry?" *The New York Times*, 8 Aug. 2019, www.nytimes.com/wirecutter/blog/amazons-alexa-never-stops-listening-to-you/.

"FBI's Search for 'mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance." *The Washington Post*, 17 May 2023, www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story_2.html.

Fieldstadt, Elisha. "Kate Del Castillo Speaks out in the New Yorker about 'El Chapo' Meeting, Sean Penn." *NBCNews.Com*, 12 Mar. 2016, www.nbcnews.com/news/latino/kate-del-castillo-speaks-out-new-yorker-about-el-chapo-n537071.

Forbidden Stories Staff. "Frontline: Global Spyware Scandal: Exposing Pegasus." *Frontline, PBS.Org*, 3 Jan. 2023, www.pbs.org/video/global-spyware-scandal-exposing-pegasus-part-1-knbyuj/.

Hern, Alex. “Mark Zuckerberg Tapes over His Webcam. Should You?” *The Guardian*, 22 June 2016, www.theguardian.com/technology/2016/jun/22/mark-zuckerberg-tape-webcam-microphone-facebook.

Jovanovic, Bojan. “How to Detect Pegasus Spyware on Your Phone.” *How to Detect Pegasus Spyware on Your Phone | Dataprot.Net*, 6 May 2023, dataprot.net/guides/how-to-detect-pegasus-spyware/.

Katibah, Leila. “The Politics of Pegasus Spyware: Examining the Impact of Surveillance on Journalism.” *eScholarship, University of California*, 5 July 2023, escholarship.org/uc/item/02k620g6.

Mvt-Project. “MVT-Project/MVT: MVT (Mobile Verification Toolkit) Helps with Conducting Forensics of Mobile Devices in Order to Find Signs of a Potential Compromise.” *GitHub*, github.com/mvt-project/mvt. Accessed 26 July 2023.

Orwell, George. “Nineteen Eighty-Four: A Novel.” *Amazon*, 1949, www.amazon.com/Nineteen-Eighty-Four/dp/0241453518.

Qian, Isabelle, et al. “Four Takeaways from a Times Investigation into China’s Expanding Surveillance State.” *The New York Times*, 21 June 2022, www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html.

Raymond, Nate. “U.S. Supreme Court Lets Meta’s Whatsapp Pursue ‘pegasus’ Spyware Suit.” *Reuters*, 9 Jan. 2023, www.reuters.com/legal/us-supreme-court-lets-metas-whatsapp-pursue-pegasus-spyware-suit-2023-01-09/.

Shankland, Stephen. “Pegasus Spyware and Citizen Surveillance: Here’s What You Should Know.” *CNET*, 19 July 2022, www.cnet.com/tech/services-and-software/best-mobile-vpn/.

Washington Post Staff. “Takeaways from the Pegasus Project.” *The Washington Post*, 2 Feb. 2022, www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.