LIBRARY AWARD FOR UNDERGRADUATE RESEARCH

Second Place
Social Sciences

UC SANTA BARBARA
Library

www.library.ucsb.edu

Leila Katibah
LAUR Reflective Essay

I first learned of Pegasus spyware through social media news posts exposing the newest cutting-edge spyware threatening the world's digital citizens. Years later, in the GLOBAL124 course at UCSB, I was reintroduced to Pegasus, after which it was contextualized in a greater discussion of global paradigms of securitization, sparking further interest. This was during a Summer Session, just before I was about to start working on a thesis for the Sociology Honors Practicum, instructed by Dr. Hannah Wohl. I knew this would be the perfect opportunity to investigate this particular spyware, and the broader sociological issue of surveillance studies. I narrowed down the scope of my research by focusing on the case of journalists targeted by Pegasus. I felt this would be especially relevant in a time where the integrity of journalism is under global threat by powerful bad-faith actors propagating alternate truths. I wanted to investigate how this spyware has changed the practice of journalism around the globe, and the broader implications this has on democracy and human rights.

Throughout the research process, I sought to answer the following questions through interviews with impacted journalists: 1) What is the political and social climate of governments deploying Pegasus against journalists? 2) How effective are the responses of publications and human rights organizations to the threat of Pegasus? 3) What is the impact of Pegasus on journalists' personal and professional lives? 4) How do journalists retaliate and continue to report in spite of surveillance? I analyzed a total of eight primary sources, consisting of my personal communications with journalists verified by research labs to have been targeted by Pegasus. To start, I decided to go to the source that first broke the news of Pegasus: Forbidden Stories, which listed over 180 targeted journalists. Once I had their names, I scoured the internet for their official work emails and social media profiles, direct messaging or emailing everyone I could find, and conducting snowball sampling with those I was able to connect with. I found the

contact information of approximately fifty journalists, and received eleven responses. Of those responses, I was able to schedule interviews via Zoom with six journalists, with one respondent providing a previous interview transcript, and another agreeing to a questionnaire via email.

In gathering secondary sources to form the literature review, I decided it would be best divided into three segments: surveillance theory, resistance to surveillance, and the fusion of surveillance and settler-colonialism. First, I searched the library databases for topical journals, after which I found a very helpful article that summarized modern developments in surveillance theory (Galic et al 2017). This pointed me to research by prominent scholars in the field, like Foucault, Agamben, Bigo, Deleuze, Haggerty, and Zuboff, which I was able to access through the library database. Then, I searched through the database for sources that focused on my case study, the surveillance of journalists (i.e. Thorsen, Mills, Waters). The final section of the literature review fused theories of surveillance and settler-colonialism to contextualize the development of Pegasus in a settler-colonial society, and its distribution to governments around the world. In navigating this section, my thesis advisor Dr. Lisa Hajjar pointed me to relevant research papers by her colleagues. I cited the ones I deemed relevant to my research, such as the works of Zureik, Stein, Lyon, and Sa'adi. This section was also informed by searches of scholarly articles on Pegasus spyware within the library database.

Once I started my thesis, I realized how much I was missing out and taking for granted by neglecting the abundance of knowledge I have access to via the UCSB library. I used many of its databases, including Sage Journals, Taylor & Francis, Springer, Wiley, Proquest, all of which have a plethora of academic journals that significantly aided me in the literature review. I had never even attempted to check out a book from the library, until I checked out David Lyon's *Theorizing surveillance: the panopticon and beyond*, after requesting an interlibrary loan from

UCI to UCSB. I also submitted a request to Special Research Collections regarding another book by Lyon, after which I was guided by library staff to microfilm and a link to access the book.

THE POLITICS OF PEGASUS SPYWARE:
EXAMINING THE IMPACT OF SURVEILLANCE ON JOURNALISM

a thesis submitted by

Leila Katibah

to

The University of California, Santa Barbara

Department of Sociology

in partial fulfillment for the degree of

Bachelor of Arts Degree in Sociology

with Distinction in the Major

Honors Practicum Instructor: Dr. Hannah Wohl

Faculty Adviser: Dr. Lisa Hajjar

June 2023

Table of Contents

Acknowledgements

Dr. Hannah Wohl for her unwavering support, tutelage, and kindness.

Dr. Lisa Hajjar for her insight, guidance, mentorship, and attentive feedback.

My parents for supporting me in all my educational endeavors.

My interviewees for continuing to report on important news in the face of threats and surveillance, and for taking the time to speak with me.

Abstract

This research aims to understand the geopolitical context of surveillance practices on journalists, the impact of surveillance on journalistic practices, and the ways in which journalists continue to report in spite of surveillance. By conducting semi-structured interviews with journalists around the world who have been surveilled via Pegasus spyware, I was able to gather the data to answer these questions, and expand upon previous literature on surveillance theory in relation to control, counter-surveillance, and the fusion of colonialism with surveillance studies. Pegasus, developed by an Israeli tech company, is a zero-click spyware sold and licensed to governments across the world. Pegasus has been wielded against journalists, dissidents, activists, and even high-level government officials. My findings show that governments accused of deploying Pegasus are characterized by highly controlled media landscapes and popular harassment campaigns against critical journalists. Most journalists felt supported in one way or another by the gravity and tenacity of the response of either their national publications or international journalist coalitions or human rights organizations, but ultimately believe that their resources do not match official, corporate, and militarized entities behind the Pegasus attacks. The Pegasus attacks have had adverse impacts on journalists' lives and careers, including lingering paranoia on behalf of themselves and their sources, hindering communication with sources, and stagnancy in news reporting operations. Lastly, some impacted journalists have exercised counter-surveillance practices, such as involvement in lawsuits and litigation regarding Pegasus, cryptography practices, and limited use of technology altogether. This research uses journalists as a case study to assess the broader implications of surveillance on freedom and democracy, and implies the need for more accessible resources to ensure journalists' cybersecurity, and for legislation outlawing surveillance of journalists and the distribution of Pegasus spyware altogether.

Introduction

Surveillance is always a means to an end, whether that end is power, influence, management, entitlement, profit, or control (Lyon 2007). As an increasingly globalized phenomenon, accelerated in response to 9/11 (Norris 2017), the market for spyware has vastly expanded, with governments deploying sophisticated surveillance technologies developed by private tech companies to spy on political opponents, activists, journalists, etc. While anyone is potentially susceptible to such pervasive surveillance, some groups, such as journalists and political dissidents, are at higher risk of targeted surveillance by governments, in turn threatening democracy and privacy while empowering global authoritarianism (Gurses et al 2016).

Drawing from a qualitative case study based on interviews with impacted journalists, this thesis aims to assess how journalists are selected, targeted, and impacted by governments deploying Pegasus software, which is manufactured by a private Israeli company, the NSO Group. It also aims to address how journalists continue reporting in spite of being surveilled, and the efficacy of current journalistic and institutional responses to the human rights abuses linked to the use of Pegasus technologies. The grave threats that surveillance poses on freedom of the press speak to the larger issues of global freedom, power, and democracy. Hence my focus on journalists as a case study to understand the implications of Pegasus spyware, as they depend on the willingness of sources to discuss sensitive and confidential material to contextualize and report a story.

Sociological research on surveillance has historically assessed the monitoring, discipline, and control of human behavior. Surveillance theories were initially developed as all-encompassing paradigms. Eventually, the field developed through separate case studies, when the age of digital information rendered surveillance practices more advanced, ubiquitous, varied,

and malleable. More researchers are focusing on targeted surveillance, and an increasing number of scholars are beginning to assess the racial, colonial, and neoliberal logics that shape contemporary surveillance practices. Specifically, the use of surveillance technologies as a means to control indigenous land and populations in Israel/Palestine has major implications for social control on the local, regional, and global level, as Israel tests its technologies of control on occupied Palestinian populations, then markets them to governments across the globe (Zureik et al 2011). Herein lies the fusion between studies of surveillance and settler colonialism, as colonialism shaped the development and practice of surveillance and technologies of control (Zureik 2020). The development of Pegasus by an Israeli corporation and its licensing to governments across the world exemplifies this. The advancement of surveillance technologies has fostered research and development of methods of counter-surveillance, focused mostly on privacy law and advocacy, sousveillance, and cryptography.

My findings support and expand on the findings of other scholars studying surveillance theory, counter-surveillance theory, and the politics and deployment of Pegasus. Through the interviews I conducted with journalists targeted via Pegasus spyware, I found that the media landscapes of the respective nations deploying Pegasus varied. India and Turkey have very limited press freedom, with the majority of national media outlets being government owned. El Salvador and Hungary, while having a media climate highly influenced and threatened by the government, has a more varied media landscape, with critical journalists often subject to online or physical harassment. Unlike the other cases, the Moroccan government was the only nation to have surveilled journalists of another nation, France, in an effort to collect information to criminalize French-Moroccan journalists. My findings also assess the efficacy of national publications' and international organizations' response to Pegasus, which have mostly been very

responsive and supportive of journalists, but whose resources ultimately do not match up to the NSO Group and the governments deploying Pegasus. Additionally, the interviews also reveal the adverse and unexpected impact of the Pegasus scandal on the personal lives of journalists, their professional reputations, and their communications with sources. Lastly, my findings delve into the ways journalists practice counter-surveillance, through limited technology use, cryptography practices, and involvement in lawsuits aiming to ban the use of Pegasus and overall surveillance of journalists.

Literature Review

Surveillance Theory

With rapid developments in governance and technologies, coupled with new initiatives in theoretical explanations, the field of surveillance studies has grown rapidly over the past few decades (Lyon 2006). Surveillance studies has found its place on the academic agenda, particularly in sociology, which historically has been concerned with the study of supervising, monitoring, recording, and processing others' behavior (Lyon 2007). Surveillance practices have been around for centuries, but in the modern world, it has taken a routine, systematic form, based on bureaucratic organization and individuation (Dandeker 1990).

The Classics: Pre-Panoptic Ideas

Some of the earliest social scientists mapped what much later developed into the field of surveillance studies, either by drawing attention to capitalist supervision (Marx 1848), bureaucratic record keeping (Weber 1947), urban metropoli as hubs for mobility and anonymity (Simmel 1903), or disciplinary responses to growing social inequalities and the sense of anomie they produce (Durkheim 1897). These themes set the stage for a field of study examining "the scopic regimes of modernity" (Jay 1993), or how some may watch over others, metaphorically or physically (Lyon 2006). The conspiratorial and hyper-paranoid metaphors and images of surveillance, with an omnipresent power constantly watching reminiscent of George Orwell's idea of "Big Brother" in the novel *1984* (1949), should not be confused with more nuanced sociological analysis of surveillance (Lyon 2007). Specifically, Orwellian notions of mass surveillance presume mass society. As such, they often fail to recognize dimensions of targeted surveillance based on race, gender, and coloniality (Gurses et al 2016).

The Panopticon & Control Societies

Some sociologists have addressed the issue of surveillance as a method of discipline. Foucault's analysis of Bentham's Panopticon, an architectural design of a prison with the goal of surveilling and controlling people efficiently, posits the Panopticon as a metaphor to talk about discipline and punishment in modern society; this is foundational in the conceptual framework of modern surveillance theory. Foucault adapts Bentham's model to make sense of how contemporary society is structurally divergent from preceding societies, through the government's pervasive efforts to control even the most private aspects of daily life (1977). By exploring the transition from punishment as a public display of torture, to modern punishment as an internalized, overt practice revolving around control of social subjects, Foucault delineates a transition from "culture of spectacle" to a "carceral culture."

The Post-panoptics

Some sociologists and philosophers have been critical of panopticism and disciplinary societies, as the power dynamics between individuals and institutions have expanded and evolved beyond Foucault's theorization. While surveillance theory should not ignore the panoptic, it can certainly move beyond it. Deleuze (1992), while agreeing with the shift from disciplinary societies to societies of control, discerned that modes of surveillance and power are far more corporatized in a modern, globalized, and capitalist society. Deleuze and Guattari (1987) diverge from the Foucauldian Panopticon, positing discipline as central to governance, and instead focus on socio-technical mechanisms of control, rather than discipline, in a world where institutions such as hospitals, schools, and factories are now corporations. Their contention is that disciplinary technologies and practices seek to achieve a long-term goal of

producing a stable, docile population for governments, while corporations instead focus on short-term results, requiring constant control, through surveillance of markets, workforces, strategies, etc. Unlike a national government that aims to develop society as a whole, corporations seek to dominate specific parts of an international market. Whereas Foucault described effective discipline as visible and active, Deleuze (1992) notes how modulation - when institutions are in a constant state of flux - occurs invisibly, producing both abstract and quantifiable forms of surveillance. Ultimately, in *Discipline and Punish*, Foucault focused on enclosed institutions such as prisons, whereas Deleuze focused on open spaces exhibiting social control at a distance.

The post-panoptics, such as Deleuze, Agamben, and Hardt and Negri, address new political and technological factors at work. Agamben speaks to how the panopticon was a distinct, bounded space, but now, zones of indistinction are loci of power. He notes how states obsessed with security are taking a massive risk, because prioritizing security as a source of legitimacy can cause a nation to turn itself terroristic (Agamben 2002). Building on the ideas of Agamben, Dider Bigo (2008) reimagined the panoptic model to assess surveillance in the context of global twenty first century developments. In an attempt to conceptualize what 9/11 did to notions of control, freedom, and security, Bigo explored the "banopticon," in which profiling technologies are employed to determine targets of surveillance. Rather than monitoring and tracking groups to capture misbehavior, the banopticon aims at keeping the bad ones out, banning those who do not conform to the rules of entry or access in a particular society (Bigo 2008). The 9/11 attacks triggered an American-imposed idea of global insecurity, leading to a rhetoric of "better safe than sorry" in which increased surveillance and experimentation could take place (Bigo 2008). Some scholars point out that societies after 9/11 can be named true

surveillance societies, in which every citizen is a potential threat, in need of monitoring (Lyon 2001). With this perspective, the Panopticon as a diagram re-emerges, with access points creating a confined and bordered space in which both visitors and inmates suffer a constant gaze (Lyon 2006).

Surveillance Assemblages

When surveillance technologies became more advanced, vast, and ubiquitous, sociologists and surveillance scholars built upon Deleuze's ideas. Haggerty and Ericson (2000) argued that Foucault's panoptic metaphor is ultimately outdated, that new analytical methods are required. They draw on the works of Deleuze and Guattari (1987) to posit that modern society is exhibiting a convergence of discrete surveillance practices and a "surveillance assemblage." This assemblage relies on abstracting humans and their settings, sorting them into "discrete flows" that are reassembled into distinct "data doubles" subject to scrutiny and attack, creating a hierarchy of surveillance targeting groups that would have been previously exempt from routine surveillance. The panoptic model also positions the marginalized groups of society as disproportionately surveilled, by other humans, and limits surveillance to contained and enclosed institutions like schools or prisons. Because of developments that have rendered the panoptic model inapplicable to modern societies, Haggerty and Ericson conceptualized the "surveillant assemblage," a post-Panoptic development in that it shifted from territorial to de-territorialized forms of social control.

Deleuze and Guattari defined assemblages as a multiplicity of heterogenous objects, united by working together as a functional entity. An assemblage is composed of discrete flows of a boundless myriad of phenomena. These phenomena can be people, knowledge, or

institutions, that become fixed into unstable, asymmetrical arrangements, or assemblages, in the form of devices that host auditory, olfactory, visual, and informational stimuli. This creates systems of domination that allow an entity to control a population, with surveillance assemblages acting as recording mechanisms that capture flows and convert them into reproducible events. Haggerty and Ericson (2000) defined modern surveillance as unstable, limitless, and lacking governmental accountability, and therefore as post-panoptic. Post-panoptic surveillance is exponentially larger in its capacity, as it is expanding its functions for purposes of control, governance, security, profit, and entertainment, all made possible through technological innovation such as computer databases. It levels hierarchies of surveillance by monitoring new target populations with vast technological possibilities. Because of corporatization, post-panoptic surveillance works across state and non-state institutions, primarily targeting humans, understood as a "flesh-technology-information amalgam," while relying on machines to make and record discrete observations.

Haggerty and Ericson (2000) describe surveillance as "rhizomatic," another concept adapted from Deleuze and Guattari (1987). Rhizomes are plants that grow through interconnected vertical root systems, unlike trees which have deep root structures that grow along the branch of a trunk. Conceiving surveillance as rhizomatic, is better for understanding the shift from a disciplinary society to a control society, as people are no longer subject to repressive modes of surveillance in an enclosed space. Instead, they are posited as consumers "seduced into the market economy" because contemporary surveillance is used primarily to track consumer patterns and create consumer profiles, with the goal of narrowing access to information and places. This results in the offering or refusal of social perks like credit ratings or moving through customs quickly. Thus, surveillance in the present day serves to monitor

humans, to limit access, and foster the creation of consumer profiles through an ex post facto reproduction of human behavior, habits, and actions. Haggerty and Ericson (2000) theorized this surveillance assemblage because of how the body is broken down into an abstract, decorporealized, de-territorialized series of data flows that become reassembled. This creates a data double that goes beyond representing the physical self, with the goal of being useful to institutions that seek to allow or deny access to places, information, and things, and to discriminate between people. In practice, the data doubles flow through centers of reassembly like forensic laboratories, financial institutions, and corporate or military headquarters, where they are reassembled and judged for development strategies of commerce, administration, and control. Ultimately, such a system is based on the notion of surplus value in capitalism, with the surplus being information in the form of data generated in daily behavior like credit card use, browsing the internet, Smartphone applications, traveling, walking on the street, etc., in which profit should be made.

Surveillance Capitalism

Marxist surveillance theory poses a third aspect of post-panoptic surveillance theory. While connections between surveillance and capitalism are not new, surveillance capitalism is nevertheless a new subspecies of information capitalism (Galic et al. 2017). Marx understood surveillance as an essential political and economic concept for the capitalist economy and modern nation-state (Fuchs 2013). Surveillance capitalism conceptualizes Haggerty and Ericson's "surveillant assemblage" to a further, all-encompassing level, as an overarching feature of capitalist society. Although it was first coined by Bellamy and McChesney (2014), surveillance capitalism was more thoroughly explored and disseminated by Zuboff (2015, 2016).

Zuboff has laid out a foundation for an all-encompassing theory of surveillance capitalism, at a civilizational scale, in an attempt to explain and understand a new kind of social relations and economic-political system that produce novel conceptions of authority and power. Contemporary surveillance works in tandem with an economy heavily reliant on metadata, so a significant shift in larger economic foundations is required for meaningful reforms.

Zuboff conceptualizes surveillance capitalism as an economic system gradually developed to derive profits from the unilateral surveillance and modification of human behavior (2016). This new form of capitalism, imbued with surveillance, seeks to produce revenue and completely control the market by predicting and directing human behavior. Human behavior is in turn exploited as an unlimited raw material (Zuboff 2019). The dominant logic of the new form of capitalism, therefore, is based on data accumulation. This subverts traditional capitalist mechanisms focused on the unity of supply and demand. While flawed, it is meant to work for the needs of societies, in turn expanding market democracy. In contrast, surveillance capitalism is utterly disconnected and uninterested in the needs of people, societies, and states. As an economic logic, surveillance capitalism could lead to the concentration of knowledge in the hands of a few technology companies that have total control over algorithms, research, and digital knowledge. This would allocate them power that threatens individual autonomy, sovereignty, dignity, and the foundations of democracy (Zuboff 2019). Big data, which is based on predicting and monetizing the real-time flow of individuals' daily life, works to influence and modify human behaviors for profit. While still underdeveloped as a theory, surveillance capitalism as described by Zuboff relies on a logic of accumulation that pervades privacy and threatens democracy by replacing political canons of modern liberal order defined by individuality and self-determination across the public and private sphere. In this model,

surveillance is a technologically dependent concept, with the development of new technologies changing social organization and governance.

However, descriptions of surveillance centered on the latest technological trend still would not encompass all the different forms of surveillance in a surveillance state (Galic et al 2017). The increase in size and complexity of surveillance practices makes it nearly impossible to develop an overarching theory of surveillance that captures surveillance as a unitary phenomenon like Foucault's and Deleuze's theories (Galic et al 2017). Instead of an all-encompassing theory, contemporary surveillance theory is characterized by particular surveillance concepts or diagrams studied in specific case studies, often revisiting and rethinking concepts of surveillance in relation to on-going technological development (Elmer 2003). Additionally, critics regard Zuboff's conceptualization of surveillance capitalism as failing to assess how organizations interact within their business and government facing operations, as she focuses primarily on consumer-facing operations (Jansen et al 2021).

Dataveillance

The term dataveillance was coined to show how it has become easier for governing actors to trace individuals or groups through computational and digital means rather than previous forms of architectural or institutional surveillance (Clarke 1988). Dataveillance is a form of surveillance based on mass data collection with "unstated preset purposes" that allows the building of profiles on individual behavior, as well as predicting future behavior and interfering in individual decision-making (Van Dijk 2014: 205). These profiles are in turn traded as commercial goods, making sensitive information about individuals, groups, and organizations accessible to a wide range of third-party actors with different interests, who may utilize such

access for malicious purposes (Galic et al 2017). Commercially motivated surveillance practices affect individuals and civil society as a whole, although the risks and social consequences for trading behavioral data are especially high for some groups, such as journalists (Salzmann 2021).

With technologies such as smartphones being used as work tools, journalists engaging in mobile journalism are at risk of dataveillance (Salzmann 2021). Simultaneously, the role of a journalist is to be an investigator reporting current events. As they are tracking others, they are being watched in a manner that is radically transparent to third parties, with the observations translated into data, then sold to business and government markets (Salzmann 2021). In the digital age, journalists and their sources are increasingly vulnerable to digital attacks from state and nonstate adversaries. This threatens source confidentiality and undermines investigative journalism (Thorsen 2019).

The use of digital surveillance harms journalists in a myriad of ways, including: tracking of their activities, hacking and theft of data, disrupting operations through account hijacking and denial of service attacks, public shaming, online harassment, cyberstalking, confiscation or destruction of computer hardware, and physical threats to persons (Thorsen 2019). The surveillance of journalists in a digital landscape substantively changes the ways in which news is reported. It is difficult to quantitatively assess how many stories have not been covered out of fear on the part of editors, journalists, and sources to come forward as a result of substantive or perceived surveillance powers (Mills 2019). The panopticism framework states that those under real or perceived observation will alter their behavior to be more subservient to authority. In the case of journalists, this causes increased difficulty in their work and potentially damaging communications with sources (Waters 2017).

On a psychological level, the effect of state surveillance sparks paranoia in journalists with regard to their own personal safety and that of their sources (Mills 2018). On a professional level, journalists have reported hindrances and internal hesitation as a result of the fear to pursue investigative modes of work as they did previously. On a meso-level, journalists, newsrooms, and entire media platforms are becoming more cautious and vulnerable, as a result of surveillance and financial pressures (Mills 2018). Lastly, on a macro-level, the implications of surveilling journalists create dire consequences for democracy as well as the role of journalists in society. This is especially true for mature democracies, who may bask in the glow of that self-congratulatory phrase, believing freedoms could never be threatened in their democracy. A mature democracy often perceives itself as exempt from the savagery of history and the depredations of an unbridled government, resulting in gradual institutional unwillingness and incapacitation to curtail surveillance of journalists (Mills 2018).

Surveillance in the Global War on Terror

Following the September 11, 2001 attacks and the commencement of the Global War on Terror, fear for personal and national security became far more widespread, resulting in the implementation of draconian measures including stricter surveillance methods and technologies at the expense of target groups like political activists, immigrants, Muslims, journalists, minority racial groups, etc. (Zureik 2011). The responses to 9/11 testify to the ever-changing dynamics of surveillance in nation-states, shifting from centralized surveillance to decentralized and malleable set of surveillance processes designed in the flows of everyday existence, known as a "surveillant assemblage" (Lyon 2001). Surveillant assemblages work to abstract bodies from

places, percolating personal and group data through discrete systems and flows (Haggerty & Erickson 2000).

Following 9/11, surveillance data was extracted from myriad sources, such as supermarkets, credit card transactions, motels, and traffic control points to trace activities of 'terrorists' in the moments before attacks (Lyon 2001). Public data opinion in the West shows that to question such intrusive surveillance practices of the state as a deterrent to terrorism is tantamount to compromising state security. Anyone who opposes or questions such surveillance, is posited as a potential dissident or terrorist (Zureik 2011). Although, over time, the public has begun to shift away from unquestioning acceptance of infringements on privacy and personal liberties, rendering the globalization of fear and terror a self-fulfilling prophecy (Zureik 2011).

Counter-Surveillance Theory

Counter-surveillance refers to "intentional, tactical uses, or disruptions of surveillance technologies to challenge institutional power asymmetries" (Monohan 2006: 1). It also involves turning the tables and surveilling those who are doing surveillance, which Mann (2002) calls "sousveillance," in which this inverse panopticon resituates technologies of control onto authority figures. Technological developments in surveillance capacities have raised problems so immeasurable that no kind of typical political action would adequately challenge it (Ellul 1967). The assumption that with technological progress comes political progress, is optimistic and flawed, as radically different political aims have co-opted technology to depict their respective notions of justice (Stein 2021). Consequently, discussions of surveillance should be accompanied by references to counter-surveillance, dissimulation, resistance, and critical assessment of privacy law (Zureik 2011). Just as important is assessing surveillance practices in relation to

social justice, citizenship, human rights, individual autonomy, and mobility. While mainstream literature focuses more on surveillance practices rather than resistance to surveillance, there are a number of scholars and activists filling this absence (Zureik 2011).

Privacy Law & Advocacy

Technological expert and privacy advocate Chris Soghoian stated "It would be fairer if there was a situation where consumers could choose privacy" (Gurses et al 2016). Within the neoliberal marketplace, surveillance is depoliticized, and often discussed in terms of individual consumer preference. Turning privacy into a marketable commodity would foster new power dynamics centering tech corporations, thereby rendering privacy a privilege for those who can afford it (Gurses et al 2016). Therefore, counter-surveillance in the form of privacy advocacy focused on technical progress in private sectors merely reshapes interactions between industry and government surveillance. With the rise of surveillance capitalism, addressing the root of the problem of targeted surveillance may have to be addressed in relation to the broader economic system of capitalism itself rather than more legal reforms within neoliberal empires (Morozov 2019).

Cryptography, Encryption, & Limitations

Cryptography in the digital age refers to the principles and practices that prevent unauthorized use of information. It entails transforming data so that it is illegible to unintended audiences and institutions (Thorsen 2019). Encryption is a form of cryptography which involves transforming plain text (legible data) to ciphertext (illegible data) to ensure confidentiality (Thorsen 2019). Among privacy advocates, progressive security engineers, and policy makers,

the problem of surveillance is framed primarily as everybody being under surveillance, and the proposed solutions are technical defense mechanisms like the use of encryption, or "crypto" (Gurses et al 2016). Such popular market-driven, techno-legal responses tend to focus on mass surveillance rather than targeted surveillance. This fails to address the racial, gendered, classed, and colonial dimensions of surveillance programs (Gurses et al 2016). Consequently, these discussions neglect the ways surveillance disproportionately impacts marginalized groups, particularly in the form of racialized violence, extrajudicial killings, and torture. This is linked to the United States and Europe's colonial histories and more recently, the Global War on Terror's construction of Muslims as objects of racial surveillance (Kundnani 2014). In public debates on surveillance and counter-surveillance, US industry and government officials generally agree upon the need and desirability to ensure US dominance in foreign tech markets, citing economic gain and national security (Gurses et al 2016).

The issue of encryption is especially prevalent in the journalistic community, as journalists across the world are being surveilled by state and nonstate actors, threatening news work and source confidentiality. The lack of knowledge about how to integrate defensive measures and digital security such as encryption into everyday routine journalistic work poses many challenges for journalists, as demonstrated by UNESCO reports by Henrichsen, Betz, and Lisosky (2015) based on an international survey of journalists; Posetti's (2017) report on protecting journalism sources in a digital age; Kleberg's (2015) report on digital source protection; Bradshaw's (2016) study of U.K. regional journalists' source protection and information security; and Lashmar's (2016) interviews with journalists from countries of the Five Eyes intelligence alliance (Australia, Canada, New Zealand, United Kingdom, and the United States). These studies show a perceived lack of usability of encryption tools, highlighting

that journalists and their sources do not understand data anonymization or digital communication security sufficiently. These arguments are widespread among journalists as it hinders the ability of journalists to guarantee their sources' safety, whistleblowers or not, in such a complex digital communications landscape.

Sousveillance & Political Activism

The first two decades of the 21st century were characterized by the global proliferation of photographic technologies (Stein 2021).The act of counter-surveillance, by definition, serves to challenge disparate institutional power dynamics (Monahan 2006). For example, this can include disabling or destroying surveillance cameras, mapping paths of surveillance and distributing that information on the internet, staging public plays to highlight the surveillance state, or employing video cameras to monitor state personnel and surveillance systems (Monohan 2006). Counter-surveillance, however, is very ambiguous, and can include efforts by political activists to adopt visual technologies to protest state violence, such as police misconduct (Wilson and Serisier 2010). This can be included in the category of "sousveillance" in which the police, as a state authority, is now being surveilled by a population increasingly critical of their misconduct (Mann 2003). While surveillance refers to the act of organizations observing people, counter-surveillance resituates technologies of control to help individuals observe those in authority, and such an inverse panopticon is called "sousveillance," from the French word for "sous" (below) and "veiller" (to watch) (Mann 2003). The use of digital photography as an act of sousveillance attached to political dreams has been seen throughout social movements throughout the 21st century, such as the Arab revolts, the Occupy movement, Black Lives Matter, and the Syrian revolution, each dependent on the internet and camera as tools of citizen

witnessing (Stein 2021). It can be argued that journalists engage in sousveillance, a broader form of surveillance of power from below (Mills 2018). In a world where journalists are increasingly targets of state and corporate surveillance, the new media and power politics of sousveillance aim to shift toward a form of a relative equilibrium. This is because in democracy, there is a platform for many voices, and journalists serve democracy by bringing these voices to the forefront by asking the difficult questions to powerful entities, while also informing the general public (Mills 2018).

The colonial present of Israel/Palestine in a digital age exemplifies the ways in which a camera lens is employed by Palestinian video-activists, Israeli military and police, human rights workers, and Jewish settlers alike to contest state violence or consolidate it (Stein 2021). Palestinian and Israeli human rights activists were among the first to utilize cameras and "networked visuality" as political tools (Stein 2021:3). Those with radically diverging political aims and access to technologies and literacies of the digital age hoped that the photographic technologies of the digital age would deliver on their respective political aspirations (Stein 2021). While the presence of a camera at a scene of political violence is meant to ensue public shock and outrage by bearing truer witness and therefore yield justice, in most cases it does not adequately disrupt systems of oppression, particularly when surveillance is so widespread that it erodes investments by prior generations into liberation technology and digital democracy. At first, the presence of the camera during an act of state violence, as seen through the police beating of Rodney King and Abu Ghraib torture sites, was shocking, if not revolutionary. Now, the eyewitness camera is an anticipated feature on the landscape of state violence, but it does not necessarily dissuade the Israeli justice system and public, or produce convictions in most US police killings, and is often met with staunch retaliation (Stein 2021) On the other hand, the

Black Lives Matter Movement in 2020 reinforced popular investment in the radical potential of a bystander camera as a tool of social change (Stein 2021).

Fusing Surveillance Studies and Colonialism: The Politics & Deployment of Pegasus

Surveillance is defined as "the focused, systematic, and routine attention to personal details for the purposes of influence, management, protection, or direction" (Lyon 2007:14). Colonial surveillance in particular is a strategy of domination, based on dimensions of inclusion and exclusion, population sorting, and citizenship rights (Zureik 2011). Centuries of colonial rule has left its mark on modern states, not only in a territorial and economic sense, but also in regards to Orientalist colonial cultures in Europe and its instruments of power (Said 1978). Colonialism adopts different forms and structures, such as occupying and permanently settling into a country while displacing natives (e.g. the Americas), or a military occupation (e.g. India under British rule), or a hybrid of both (e.g. the French in Algeria) (Zureik 2011). The Israeli occupation of Palestinian lands is characterized by a hybrid of settlement, military occupation, displacement, and expulsion (Zureik 2020).

Israel's Settler Colonialism & Biopolitics as a Global Security Paradigm

Israel's role in the Middle East is characterized by a nexus of securitization, racialization, and settler-colonialism (Zureik and Lyon 2022). Indeed, Israel's background as a settler-colony plays an elemental role in the formation and deployment of Pegasus. Settler colonialism is a project of racial domination, based on legal and political stratified hierarchies that posit natives as backward and non- or sub-human, and the settlers as human, civilized, and progressive (Bevilacqua 2022). The colonial gaze of surveillance and observation operates as a powerful

means to dominance because the colonial observer, with an elevated vantage point, objectifies and interpellates colonized subjects in a way that situates their identities in relation to colonizers (Ashcroft, Griffiths, and Tiffin 1998). A settler society has to work to normalize itself in the midst of a native population. In order to manipulate individuals' identities, networks, social groups, and communication, they must outmaneuver the natives, study their "mentality," and learn their language. For the Israeli state, this is condensed into the practice of surveillance that has become so entrenched in this active colonial project that it is essential to its philosophies of life (Sa'di 2021). While the process of othering colonized subjects is a prerequisite, it is inherently fragile, requiring a constant stream of imagined inferiority of the Other, and therefore, is always at risk for criticism (Zureik 2011). The Israeli state argues that surveillance is a necessary tool for its security, and it is in the name of security that Israel justifies its colonization of Palestinian lands and the expansion of its military industrial complex (Zureik 2020).

Israel relies heavily on its private high-tech sector, to recruit private companies to carry out the colonial functions of military rule over Palestinians, and in their attempts to confront Iran by reshaping Israeli-Arab Gulf relations (Zureik 2020). Economically, private securitization has reaped massive profits, and the Israeli state controls core military and political aspects of contracting and privatizing security services (Zureik 2020). The proliferation of private surveillance companies also coincides with the rise of neoliberal ideologies. Neoliberalism promotes weakened government regulation and oversight over markets, including the cyber technology market. Such lack of international oversight on cyber technologies that are increasingly available in the open market can threaten democracy and empower authoritarianism (Zureik 2020). The Israeli occupation can be described as neoliberal colonization, as its economy exhibited a neoliberal restructuring leading to attacks on unions and welfare programs,

unemployment, rapid urbanization, and loss of land, directly related to its continued projects of racial and colonial domination (Clarno 2017). The Israeli experience with neoliberalism featured expanding settlements, ethnically segmenting the West Bank, and a series of ruthless military campaigns against Palestinians (Clarno 2017).

Colonialism has provided a foundation in the development of technologies of surveillance and control used in modern governance. Biopolitics, used by Michel Foucault to describe population control, or the politics of who gets to live and die, is equally relevant when it comes to intellectual discussions on surveillance and colonialism (Zureik 2011). Such logics lead to the securitization of identity, in which conditions of freedom are products of identification (Rose 1999). In an increasingly technologically adept world, surveillance and security technologies, such as sorting of population by ethnic categories using identification cards in Israel, further widen gaps to opportunity and access (Lyon 2011). Israel's control of Palestinian freedom movements lies in its control of every aspect of the Palestinian population registration (Lyon 2011). Identification is vital to surveillance, particularly in colonial contexts where political power is defined by ethnic and religious categories (Lyon 2011).

Reintroducing Foucault's logic of disciplinary technologies and societies, surveillance serves to induce fear among the surveilled, eventually creating a self-surveilling population (Foucault 1977). It is a mechanism of control appearing in five-fold measures in Israel's settler-colonial model: blockade and fragmentation of Palestinians through checkpoints, walls, fences, and bypass roads; control of movement via the permit system, enclosures, and checkpoints; use of informants, high tech satellite, and drone surveillance, and police or military raids to gather information; and lastly, bureaucratizing control and monitoring the activities of Palestinians on both sides of the internationally recognized borders known as the "Green Line"

(Zureik 2020). Additionally, there is substantial literature on highly intrusive surveillance methods on Palestinians involving the use of blackmail, extortion, and torture (Zureik 2020).

As the Israeli documentary *The Lab* highlights, the Israeli military tests its home-grown suveillance technologies on Palestinian residents in the occupied territories (Feldman 2013). With neoliberal ideologies leading to weak international oversight for the deployment of surveillance technology, the privatization of security has impeded democratic norms and threatened civil society (Zureik 2020). This is because Israeli espionage and surveillance equipment has been sold to undemocratic regimes and dictatorships, for financial gain and political alliances, with the goal of monitoring journalists, activists, dissidents, and gays in the respective nations (Zureik 2020). Arab nations lacking Israel's technological infrastructure but having the financial means, such as the Gulf States, purchase advanced surveillance technologies to repress domestic critics and neighboring enemies. Israel's goal to dominate the surveillance technology market originated in its desire to maintain control of the colonized Palestinian population (Zureik 2020). The documentation of the Israeli military testing its surveillance on Palestinian residents serves to present Israel as masters of such laboratory experiments, which eventually were marketed on a global scale (Feldman 2013). Colonialism has shaped the development and practice of surveillance and technologies of control, demonstrating a connection between the intellectual pursuits of surveillance studies and regional ethno-national conflict produced by colonialism, and proving to be a crucial factor in the Israeli state's eventual rise to the top of the global national security market (Zureik 2011).

Privatizing Israel's Security Industry: The NSO Group

Israeli surveillance industries are thoroughly integrated within the global surveillance market (Sa'di 2021). In technology studies literature, because of its sophisticated surveillance capacities, Israel is often characterized as the start-up nation surpassing other nations like the U.S. and U.K. in their per capita concentration of cyber companies (Zureik 2020). There are many factors contributing to the growth of Israel's role in the global cybersecurity market. Israel argues that surveillance is necessary for security, and in the name of security, Israel justifies the colonization of Palestinian lands. In turn, Israel relies on its private high-tech sector to recruit private companies to fulfill the colonial functions of its military occupation over Palestinians (Zureik 2020).

In 2010, Prime Minister Benjamin Netanyahu introduced a series of measures allowing veterans of Unit 8200, Israel's version of the National Security Agency, to create private businesses, subsequently resulting in the privatization of its military industries (Zureik 2020). Privatizing the occupation functions in tandem with Israel's transition into neoliberalism while also allowing the Israeli military to evade accusations of human rights violations through its shift to the private sector (Zureik 2020).

Security in Israel has a semi-sacred status, and its army signals intelligence Unit 8200 recruits and trains technical personnel that form technology companies such as the NSO group. The NSO Group, established in 2008, is an Israeli cyber spy manufacturer and among the largest high-tech companies in the spyware and espionage industry (Zureik 2020). The company Francisco Partners acquired a 70% stake in the NSO Group for $120 million dollars in 2014, and as a sign of its success, the NSO Group purchased back the company for about $1 billion dollars (Zureik 2020). The NSO Group and its counterparts in the industry claim their products are made to fight against terrorism, and that they secure prior confirmation from government clients that

their products will not be deployed in violation of human rights. However, several reports concluded that there was no evidence of the use of Pegasus associated with positive outcomes (Zureik 2020). Researchers at the Citizen Lab discovered the sale of Pegasus to over 45 countries including Algeria, Bahrain, Bangladesh, Brazil, Canada, Côte d'Ivoire, Egypt, France, Greece, India, Iraq, Israel, Jordan, Kazakhstan, Kenya, Kuwait, Kyrgyzstan, Latvia, Lebanon, Libya, Mexico, Morocco, the Netherlands, Oman, Pakistan, Palestine, Poland, Qatar, Rwanda, Saudi Arabia, Singapore, South Africa, Switzerland, Tajikistan, Thailand, Togo, Tunisia, Turkey, the UAE, Uganda, the United Kingdom, the United States, Uzbekistan, Yemen, and Zambia (Marczak et al 2018).

The report highlights the human rights abuses linked to Pegasus operations in Mexico and the countries in the Gulf Cooperation Council, noting there are three operators in Mexico, and six operators across the Arab Gulf focusing on UAE, Bahrain, Saudi Arabia, Canada, France, Greece, the United Kingdom, and the United States. The Citizen Lab also identified five operators in Africa, including one predominantly focusing on Togo, a staunch ally of Israel, in addition to an operator focusing on Morocco, Algeria, France, and Tunisia. Several operators are identified in Israel, four of which operate domestically, and another that appears to operate in Israel and other countries such as Netherlands, Palestine, Qatar, Turkey, and the USA (Marczak et al 2018). The use of NSO Group surveillance technologies in these regions have been linked to the extrajudicial killings and torture of innocent civilians, journalists, and human rights activists at the hands of government agents such as those in Mexico, and authoritarian regimes such as the UAE and Saudi Arabia (Zureik 2020).

The alliances between Israel, the US, and other western nations also allow the borrowing of surveillance capabilities and knowledge freely and often illegally (Zureik 2020). Coupled with

weak international oversight of the deployment of surveillance technology, privatization wreaks havoc by threatening civil society and democracy (Zureik 2020). Israel's settler colonial regime and neoliberal data-based capitalism has resulted in what many call a successful securitizing model, at the expense of privacy, autonomy, care, and solidarity (Sa'di 2021). Because of Israel's global standing as a surveillance state "par excellence," it makes sense to include Israel/Palestine in mainstream surveillance studies that currently focus more on western contexts (Zureik 2011: 39).

Background

The Israeli manufacturers of Pegasus spyware, the NSO Group, claims the technology is only used to "investigate terrorism and crime." The selling point is that it "leaves no traces whatsoever" (NSO Group). However, research and forensic methodology reports by Amnesty International, Citizen Lab, and Forbidden Stories detailing the use of Pegasus starting from 2014 show neither of those statements are true, dubbing the private security firm "a cyber-arms dealer" (Franceschi-Bicchierai 2016).

The use of the militarized spyware program called "Pegasus" was first made known to the public in 2016 through a failed attempt to hack the phone of Ahmed Mansoor, an Emirati human rights activist (Franceschi-Bicchierai 2016). Mansoor, at the time already having been targetted by government hackers using commercial spyware products, received a strange text message from an unknown source that read "New secrets about torture of Emiratis in state prisons" (Franceschi-Bicchierai 2016). Rather than clicking the link, Mansoor sent it to Bill Marczak, a digital rights watchdog and researcher at Citizen Lab. Upon investigation, the Citizen Lab discovered "one of the most sophisticated pieces of cyberespionage software we've ever seen." The link could remotely break into an iPhone by exploiting three different unknown vulnerabilities, or "zero-days" (Franceschi-Bicchierai 2016).

In 2014, the *Wall Street Journal* published a short profile on the NSO group, detailing how Pegasus spyware is sold all over the world, with its first customer being the Mexican government. It highlighted how this spyware even caught the interest of the CIA, and despite its now publicly known operations, remains a "complete ghost" according to co-founder Omri Lavie (2013). Now that the spyware has been exposed and even linked to the extrajudicial killings of Saudi dissident Jamal Khashoggi and Mexican journalist Cecilio Pineda Birto, it has ceased to

remain a ghost, facing retaliation from numerous sources, such as corporate lawsuits, human rights organizations, political activists, journalists, etc. The allegation of Pegasus spyware being in WhatsApp attacks linked to the murder of Jamal Khashoggi prompted two NSO group agents posing as investors to meet with the Citizen Lab Research Team (Zureik 2020).

According to a Citizen Lab Research Report (2018) on leaked NSO Pegasus documentation, the NSO Group's infrastructure initially began as a form of spear-phishing. Its initial infrastructure worked as a government operator to send a target an enhanced social engineering message (ESEM) containing an exploit link that directs to a domain name associated with the operator's Pegasus infrastructure. Each client has their own Pegasus infrastructure that does not overlap with others. After clicking on the exploit link, their device contacts the domain name, while disguising the operator's identity. Failure to infect results in a redirection to a legitimate decoy website to not arouse suspicion. If successful, the Pegasus implant on the device sends collected data back to a different domain than the one used for infection. After several redesigns of their attack infrastructure since 2016 through the use of multiple domains and servers, Pegasus attacks have evolved to include "zero-click" attacks which do not require any interaction with targets, making it incredibly difficult to detect attacks, rendering it the most advanced and sophisticated spyware technology. Zero-click attacks via Pegasus have been reported since May 2018 until now (Amnesty International 2021). These attacks can extract all the data (e.g. messages, photos, recordings, browsing histories, calendars, contacts etc.) from the target's mobile device, transforming it into a live tracking and recording device for surveillance (Mazetti et al 2022). Even the most security-conscious individuals can still be targeted, as the software exploits and leverages undiscovered vulnerabilities, such as peculiar network trafficking in commonplace apps like Photo and Music apps (Pegg and Cutler 2021). If neither

spear-phishing nor zero-click attacks work, Pegasus software can also be installed over a wireless transceiver located near a target, or manually installed if the target's phone is stolen (Pegg and Cutler 2021).

The Israeli government requires the NSO group to secure licenses before exporting the spyware. For over a decade, the NSO group sold Pegasus software to spy services, law enforcement agencies, and governments around the world (Mazetti et al 2022). Consequently, Israel gained diplomatic leverage over countries eager to purchase, such as Mexico, Saudi Arabia, and India. However, as a result of Pegasus spyware's linkage to numerous human rights abuses across the globe, governments, corporations, and target groups are taking action against the NSO Group. High-risk groups targeted by Pegasus include journalists, and upon infection, their messages and calls with sources are exposed. This makes sources far more reluctant to work with journalists, out of fear for their safety and livelihood. Journalists who suspect they are being surveilled often use encrypted messaging, refuse to publish live locations, leave phones outside of meetings, and speak in code (Zablah 2022). Technology companies and Amnesty International have sought out the NSO Group in court in efforts to revoke its license (Zureik 2020). More recently, the Biden Administration blacklisted the NSO Group, in a public stance against the abuse of spyware to target dissidents, journalists, and human rights activists (Mazzetti et al 2022).

Data and Methods

Drawing on qualitative case studies including interviews with impacted journalists, this study assesses how Pegasus is used to target journalists and how journalists retaliate and continue to report in spite of being surveilled. As journalists, their roles depend on the willingness of sources to discuss sensitive material in order to contextualize and develop a story. Therefore, surveillance of journalists works to diminish the integrity of journalism and threaten freedom of the press and democracy.

Data collection was completed over a five-month period, from December 2022 to April 2023. I reached out to journalists around the world whose targeting by Pegasus spyware was made publicly available through reports on data leaks published by Amnesty International, Citizen Lab, and Forbidden Stories. There are over 180 known journalists impacted by this spyware, and I reached out to every living and free journalist impacted whose email or social media was publicly available. After receiving 8 responses, I conducted semi-structured interviews, lasting approximately 30 minutes, with six respondents. One respondent requested that I send her the questions and subsequently sent her answers to me via email. Another respondent was not available for an interview, but provided me with a transcript of his testimony before his government's supreme court regarding the use of Pegasus. I also conducted snowball sampling, asking journalists at the end of interviews if they knew colleagues targeted by the Pegasus spyware. Then, I sent out emails in hopes of recruiting them. Because I am an undergraduate student interviewing public figures and professionals with well-established careers, the process of gaining access to these individuals was lengthy and difficult.

The primary goal of interviewing targeted journalists is to understand the ways they are impacted by surveillance, and how they are working to resist such pervasive spyware. Retaliation

and resistance to surveillance, known as counter-surveillance, can be understood as intentional, tactical means to disrupt surveillance technologies in order to challenge institutional power dynamics (Monohan 2006).

Because I interviewed public figures about a dimension of their professional lives, IRB approval is not necessary, as the only personal information collected is demographic, and I have provided the subjects with the option to be anonymous.The qualitative data obtained from the interviews was recorded and transcribed using Otter.ai, then uploaded onto Atlas.ti to organize and visualize prevalent themes. Once transcriptions were checked for accuracy, they were coded and grouped to classify possible major and minor themes. Themes include surveillance, privacy, cybersecurity, national security, ethics, journalism, government accountability and oversight, corruption, transparency, censorship, fear, paranoia, legal action, data protection, and digital safety.

Respondent Name	Country	Publication	Response Type
Julia Gavarrete	El Salvador	El Faro	Zoom Interview
Xenia Oliva	El Salvador	El Faro	Zoom Interview
Anonymous	India	No longer an active journalist	Zoom Interview
Saikat Datta	India	No longer an active journalist; CEO of Deepstrat	Testimony Transcript
Smita Sharma	India	TRT World; DW News; Professor at Kautilya School of Public Policy	Zoom Interview
Szabolcs Panyi	Hungary	Direkt36, Wesquared	Zoom Interview
Lenaig Bredoux	France	Mediapart	Email Interview
Ragip Soylu	Turkey	Middle East Eye	Zoom Interview

Data Analysis

This section analyzes the key findings of this research on surveillance, counter-surveillance, and journalism in relation to Pegasus spyware. There are four major themes present throughout the interviews and across respondents which this section aims to make sense of. Organized on a macro to micro level, these findings include the political and social climate of countries deploying Pegasus, the efficacy of the response of national and international publications and organizations to the threat of Pegasus, the impacts on the personal life and professional networks and reputation of affected journalists, and the counter-surveillance methods practiced by impacted journalists.

Political and Social Climate of Countries Deploying Pegasus

In order to contextualize the geopolitical issues of national governments that have opted to use this illegal spyware, this section assesses the political and social climates of the countries' deploying Pegasus on journalists. Respondents are suspected to be targeted by governmental forces from El Salvador, India, Turkey, Hungary, and Morocco.

High Government Control of National Media: India and Turkey

Of all the nations of the respondents interviewed, India has the lowest press freedom ranking according to the World Press Freedom Index at 150/180. Despite being "the world's largest democracy," India is governed by a Hindu nationalist right-wing government. Media ownership is 80 percent concentrated by the government, and politically dissident media and journalists are often subject to violence. While originally seen as progressive and a product of the anti-colonial movement, the Indian press drastically changed in the mid-2010s under the leadership of Prime Minister Narendra Modi who views journalists as intermediaries disrupting

the relationship between him and his constituents. A respondent who wished to remain anonymous, describes how since 2014, the climate in relation to freedom of the press in India has been on a downward spiral, and that Indian journalists are being put under "all kinds of official and unofficial pressures" by their government, elaborating, "the rankings in the freedom of the press has gone down dramatically over the last nine years. India is now down to 150 out of 180 countries, lower than some of the most horrible authoritarian states."

Smita Sharma, journalist and professor of journalism and public policy, noted that "increasing censorship and increasing clamp down on journalists is a global phenomenon. India of course, is one of the stories which is quite concerning, given that India's the world's largest democracy." She described the climate in India as characterized by a large-scale erosion of trust in media over the last few years, coupled with sharp polarization in politics. Sharma elaborated:

> There has been an extreme decline when it comes to trust in the traditional television news media, for sure. Maybe there is some degree of trust still remaining in the print media. That also reflects in conversations now with my journalism students. How do you go about fact-checking? What are the kinds of fact checking tools that you're using? How do you believe traditional media which by themselves have become such harbingers of fake news, which is actually an incorrect description, but rather are propagating alternate truths or false news. So I think these are the elements that have increasingly come up in the conversations in journalism classes.

In a highly controlled media landscape, amidst a population increasingly distrustful of news media, journalists and students of journalism struggle to navigate information, media, and facts. She described how policymakers need the media to connect with the public. That relationship should be healthy, but in recent years and especially following the news of Pegasus, it has become undeniably hostile. This hostility results in journalists being threatened with the label of "anti-national," a slogan Sharma described as very common, in turn fostering increased censorship of media.

In the case of India, a Supreme Court hearing was held to assess the Indian state's use of spyware. Saikat Datta is a former journalist and current CEO of Deepstrat, a "New Delhi-based Strategic Consultancy and Think Tank specializing in Risk Management and integrated solutions to business continuity threats across sectors" (Deepstrat 2023). Because of his expertise on issues related to the use and governance of surveillance in India as CEO of Deepstrat, Datta testified before the Technical Committee of the Supreme Court of India. In his testimony, he described a lack of clarity in India's legal definition of national security, no oversight or accountability in the purchase and use of surveillance, and no limitations in the amount of data that can be accessed through surveillance. While the Parliament has discretionary power to "provide procedures for ordering surveillance," Datta notes that there is a lack of "provisions that restrict the State from using tools and software that would infringe upon the right to privacy and threaten national security." In his testimony, he elaborated,

> Rules don't have guidelines for the State to determine safe tools for surveillance purposes. For instance, when the state uses tools like Pegasus, domain names used by Command and Control (C&C) servers resolve to cloud-based virtual private servers rented by the NSO Group, a registered private company in another country (Israel). This increases the national security risks as the Indian government doesn't have any visibility into the source code of the software and data storage policy of the cloud-based virtual private servers.

Datta also noted that the Indian state uses taxpayers money to purchase foreign softwares, which threatens the privacy of Indian citizens and overall national security because Pegasus software is controlled by a private company in Israel.

Saikat Datta, remarked in his testimony how the legal boundaries in relation to India's national security are not clearly defined:

> The terms that set the boundaries for surveillance are not well defined and understood for a number of reasons and are open to a wide interpretation and misuse. Nearly every

> action can misuse these terms to circumvent the necessity and proportionality threshold as laid down by the Hon'ble Supreme Court and thus, make the surveillance order legal…India lacks a national security strategy that could clarify the definition of national security and the government's objective in ordering surveillance.

Ultimately, journalists in India have been subjected to harsher conditions in the past decade, and the state's poorly defined notions of national security and surveillance allow it to circumvent them. India's laws are protective of the press in theory, however charges of sedition, defamation, contempt of court, and endangering national security are increasingly used against journalists critical of the government**.**

The case of Turkey is similar to that of India, with Turkey ranked right below at 149/180 by the World Press Freedom Index. Authoritarianism is gaining traction and challenging media pluralism in the country, with 90 percent of national media owned by the government (Reporters Without Borders 2022). Journalist Ragip Soylu described Turkey's surveilling capabilities as limited in comparison to other nations, with the local media being controlled by the government. Therefore, journalists working for foreign news outlets are subject to less pressure from the government than local publications. Soylu explains,

> They have a way to pressure the media groups through financial means because in most cases, those media groups have contact through businesses with the government…they're funded by the government one way or another. So it makes them susceptible to government pressure. If you're working for an oppositional media outlet, in most cases, they don't go off to individual journalists anymore, but what they do is they use the courts and basically issue access. For example, you publish an article that is really critical of the government, the Court issues a ban so you can no longer access that article.

Soylu's position as a journalist for *Middle East Eye*, a London based publication, is unique in that Soylu "has more leeway on speaking on things" than a journalist working for a Turkish national publication. Journalists working for local publications may face different kinds of

pressures, as they may be receiving government funds that could be withheld from the publication should it publish something critical of the regime.

To suppress oppositional outlets and independent journalists, Turkish agents may go through the courts to ban access to articles critical of the government. Social media is another arena where journalists can face threats, but Soylu notes the general public is more or less free to speak their mind on social media, making it a bit harder for the government to crack down on independent journalists. Ultimately, the cases of Turkey and India show media landscapes highly concentrated in governmental control.

Varied Media Landscapes: Online Harassment of Journalists in El Salvador and Hungary

While India and Turkey are countries with media landscapes almost entirely controlled by their governments, the landscapes of El Salvador and Hungary are a bit more varied, with more investigative and critical journalists. These journalists are often subject to online harassment. The World Press Freedom Index ranks El Salvador at 112/180, as journalists are among widespread victims of political violence. The nation is currently in the fourth year of Nayib Bukele's regime. Julia Gavarrete, a journalist for the Salvadorian publication *El Faro* recalls instances of physical surveillance back in 2017-2018 that her publication reported on. But, following Bukele's election in 2019, Gavarrete states:

> We are suffering many systematic attacks, not only on social media, because what Bukele does is very smart in the way that he starts these massive campaigns against journalists accused, he knows how to start attacking and then all the trolls, many people in social media, start reacting.

Whenever Salvadorian journalists conduct and publish their investigations, they are often bombarded with vitriol from online trolls, primarily on Twitter, who try to discredit their investigations and attack their journalistic integrity. Gavarrete alludes that this is the result of the

Bukele regime which has suppressed freedom of the press both through social media and legislation. She noted, “sometimes they post a lot of pictures that they create with Photoshop and put us around gang members, or in fights with gang members, or with MS-13 tattoos.”

To be accused as a gang member in El Salvador could land a journalist in prison for up to fifteen years, and to be accused as a member of the international gang MS-13 is punishable by death by firing squad, meaning these false accusations made on social media against journalists could lead to severe consequences. She says the presidency makes use of these trolls to control the narrative within Salvadorian media and portray journalists as “the bad guys.” In this sense, the impacted Salvadorian journalists continued to be victimized, even after the Pegasus leaks. Gavarrete also noted that this doesn't just happen to journalists, but activists and dissidents as well. She notes that the Bukele regime applauds itself for not executing or jailing any journalists, but that does not mean journalists live freely or without fear.

Another Salvadorian journalist, Xenia Oliva, describes how she and her colleagues anticipated surveillance, but not to the extent that the Pegasus leaks revealed. She noted how shocking it was to hear at least 30 Salvadorian journalists were affected. She remarks that while the government praises itself for not jailing any journalists,

> The way we used to work is changing. Firstly, because the sources are afraid. People are afraid to talk to us. Also, the police, the military are present when you are reporting certain topics and they are near you. They have felt encouraged by the government to harass you, to tell you to go away, to take your equipment, or erase your pictures.

Some of Oliva’s colleagues in El Salvador have been attacked both in person and on social media by government officials. Oliva also expressed her discontent with knowing that the Salvadoran government is willing to spend so much money on Pegasus because they already had surveilling capabilities, and the money could have been used to improve the circumstances of the country.

Oliva suspects that much of the efforts spent on monitoring journalists aims to stop investigations that may portray the government in a negative light while having leverage against journalists.

As another country with a more varied media landscape, Hungary is the only member of the European Union suspected of arbitrarily monitoring journalists via Pegasus. Ranked at 85/180 according to the World Press Freedom Index, Hungary has a political climate shaped by the right-wing populist government with a super-majority in the parliament. The prime minister, Victor Orban, often dubbed a press freedom predator, has created a media empire whose outlets are utterly loyal to his demands, while continually threatening independent media outlets. Szabolcs Panyi, a Hungarian journalist, said Hungary has been on a downward spiral since 2010 when it comes to freedom of the press. In explaining the political climate of Hungary, Panyi remarked,

> They have changed the Constitution, changed the whole institutional system of the country. They dismantled any kind of checks and balances, meaning that all the formerly independent institutions are controlled by cronies and comrades of the Prime Minister and of the governing party, which also means that at some point when they conquered everything, they started focusing on trying to conquer the media, because after a certain point, there was no opposition left. No effective opposition left.

Hungary's political and media climate is largely controlled by the governing party of the Prime Minister, leaving little room for critical or opposing opinions in the media, and critical journalists are susceptible to smear campaigns on social media by ruling-party supporters. Panyi describes some critical breaking news, articles, and scandals being released by investigative journalists, but the overall climate has turned against the press.

> Part of that was surveilling journalists or even trying to blackmail journalists back in late 2015. One of my immediate colleagues and one of my best friends was blackmailed. Or

> there was a blackmail attempt by the Hungarian secret police, the internal agency or "FBI." They tried to blackmail him into cooperating and revealing his sources to the government which he refused.

The Hungarian government has a history of surveilling the press that precedes Pegasus. Panyi described how a close colleague and friend was surveilled in 2015, in an attempt to blackmail him into revealing his sources, and thereby undermining the integrity of journalism. In describing his own experience prior to the Pegasus revelation, Panyi notes,

> I received some warnings. I was tipped off by some of my sources. For example, there was someone working for the Hungarian state apparatus, who canceled a meeting last minute and sent the message to a middleman saying that we couldn't meet because I'm under surveillance. And this person doesn't want to get compromised and doesn't want to be seen with me. So through these warnings, I already knew I'm under surveillance.

The threat of surveilling journalists in Hungary has persisted for years, and compromised journalists like Panyi's ability to reach sources. Sources revealing sensitive information or revelations about government operations fear the retaliation they may face from powerful state actors upon suspecting surveillance.

Cross-Country Surveillance: Moroccan Surveillance of French Journalists

Unlike the other respondents who are suspected to have been surveilled by a national entity, from what was revealed from the Pegasus leaks, the French journalists were actually surveilled by Morocco. This differs from the majority of other cases of journalists targeted by Pegasus and all the other respondents, who suspected they were targeted by their own government. While France ranks higher than most other nations in terms of press freedom at 26/180, Morocco ranks far lower, at 135/180. Moroccan journalists are continuously pressured by the authorities to follow orders, and independent journalists are subjected to harassment or even imprisonment. Lenaig Bredoux says,

> I was probably targeted because they wanted to collect information on investigations about sexual abuses in order to incriminate colleagues in Morocco. Some of them (Omar Radi for example) are in prison because they published stories which disturbed the Kingdom of Morocco.

Bredoux highlighted that the Pegasus leaks showed that even in a country like France, where freedom of speech and freedom of the press ranks higher than many other countries, journalists are still at risk of such invasive surveillance.

Domestic and International Responses to Pegasus

This chapter evaluates the efficacy of the response to the threat of Pegasus surveillance by national publications employing impacted journalists. It also assesses the response of international organizations and journalist coalitions, and how they work collectively to resist such pervasive spyware that infringes on their freedoms.

National Publications' and Domestic Organizations' Responses

All but two respondents, both from India, described feeling supported by national publications and domestic organizations amidst the discovery of surveillance of journalists via Pegasus. A respondent who wished to remain anonymous, in describing the state of Indian national publications, noted,

> The Indian journalists, Indian media relations are mostly corporate, all companies are completely aligned with the government. They behave as the normal propaganda appointed and haven't taken on the government, put it under pressure, or held the government accountable whether at the private level or at institutional level, or with the help of the Indian state, to really do something about the extensive surveillance that is carried out.

This journalist remarked that Indian publications are in complete alignment with the Indian government, resulting in media coverage echoing a lot of propaganda. Smita Sharma shared this sentiment, elaborating:

> In India, the state of the media is extremely concerning today, because a lot of the legacy media houses are the traditional media houses with money and power. Most of them today are pro-government. At least 90% of television stations are cowering to the government and to the authorities. The voices of the opposition have literally been blacked out.

As a result of the Pegasus scandal, coupled with the already highly controlled media landscape in India, Sharma explained how there was a wide-scale outcry to present the matter to the Supreme Court that did not result in any change.

> The Supreme Court framed a technical committee that looked into the investigation. Some points were handed over to the Supreme Court and in its ruling, it still leaves much to be clarified because on the one hand, the ruling said that we have found evidence of spyware and malware but we cannot say for sure, definitively, that this is Pegasus. So which by itself is very strange, because Pegasus in any case is a malware where you're not supposed to know that it's Pegasus but, some organizations like Citizen Lab have found ways of verifying whether it is Pegasus or not. Second thing, the Supreme Court said that the government has basically not really cooperated and the government continues to maintain that there has been no unauthorized surveillance. But what the Supreme Court did not do in this case was to ask the individual ministries and the top leaders involved with the central investigative central authorities, which deal with national security. They should have asked the interior ministry to give an affidavit saying in writing that we have not purchased practices from NSO. Because it is so very clearly maintained that they do not sell it to anybody who is not a government, and must be a government that does not have a stellar human rights record.

Sharma also explained how the news cycle moves quickly in India, and coupled with the polarization as a result of corporate and political influences on newsrooms, the issue of Pegasus and larger issues of surveillance, privacy, and freedom of the press have largely gone unaddressed.

Saikat Datta testified before the Technical Committee of the Indian Supreme Court that Sharma referenced. In response to a request for safeguards and laws he recommends following the Pegasus leaks, Datta echoed a similar testament as Sharma and said, “those tasked with surveillance (institutions/personnel/individuals) during the period when Pegasus was allegedly

deployed should be asked to provide sworn affidavits on its purchase, use and targets." Although, as of now, this has yet to come to fruition as no affidavits have been served. Sharma explained how this is part of being a journalist in a country lacking press freedom like India. She noted, "Everybody learns on the job. So if your device has been infected with Pegasus, it's up to you how you deal with it. No organization has your back. No organization is going to come and tell you what to do about it or fight your legal battles." Sharma highlighted how despite the NSO Group's claims that Pegasus is meant to be used for national security purposes, "this kind of malware, when used by the state, is supposed to protect citizens. But when the state wants to use these malwares in these kinds of routes, it can really be dangerous." Ultimately, the case of Indian journalists is unique to other respondents in that they did not feel protected by their national media platforms, which are instead highly controlled by government and corporate entities.

All other respondents felt supported by their publications and organizations. Julia Gavarrete, working with the Salvadorian publication *El Faro,* describes more meetings with IT services following the Pegasus attacks. Hungarian journalist Szabolcs Panyi, working with *Direkt36* and *we.squared.org,* describes being "satisfied with the reaction of journalistic institutions inside Hungary." He explains how the media coverage and publicity of the Pegasus scandal helped to generate public outrage within the country and on a global scale. However, he notes that because Hungarian press freedom is limited, especially in comparison to western European countries or the U.S., "the reaction was more moderate here. And also the consequences are lacking."

The resources provided by the respondents' respective publications are minimal in comparison to the NSO Group and the states suspected of deploying Pegasus. French journalist

Bredoux explained how the French publication *Mediapart* supported impacted colleagues, noting that, "[Mediapart] takes a lot of measures to protect our sources, and to protect ourselves. But the means we have will never be enough in front of huge military institutions or enterprises which create and sell these spywares." While national publications have demonstrated an overall support for the respondents, with the exception of those in India, their resources are not comparable to that of the powerful state, corporate, and military enterprises manufacturing and deploying Pegasus.

International Journalist & Human Rights Organizations' Responses

International journalist coalitions and human rights organizations have staunchly supported journalists victimized by Pegasus, whether by providing them with digital security courses, pushing forth legislation and lawsuits, or analyzing their infected devices. For example, Access Now, an international organization dedicated to defending and extending the digital rights of at-risk users around the world, offers a 24/7 Digital Security Helpline, providing targets of Pegasus spyware with analysis of their devices upon suspicion of surveillance. Xenia Oliva explains the process of contacting Access Now after suspecting her phone had been hacked:

> We [co-workers and friends] looked up the Access Now helpline. They told us what to do and helped me a bit to get the information I needed to send. Then they unfortunately confirmed that it was infected. A few days later, people from Amnesty International also got in touch with me. And they also did another analysis of the phone so I had this double confirmation.

Julia Gavarrete also describes getting in touch with Access Now after having issues with her phone that aroused suspicion. They analyzed her phone, as did Citizen Lab, an interdisciplinary laboratory based in the University of Toronto studying information controls related to Internet security and human rights. Reporters without Borders also provided impacted journalists like

Gavarrete with a four month digital security course in Germany following the Pegasus revelations. The program offers a limited number of journalists working in war zones or crisis areas a four-month stay in Berlin to complete a training program in digital security with the Berlin Scholarship Program. Szabolcs Panyi said that journalistic institutions like Reporters without Borders, the Committee to Protect Journalists, and other advocacy and non-governmental organizations have done a "tremendous job" in the fight against Pegasus and to protect journalists.

Many of these NGOs are involved in lawsuits against the manufacturers and deployers of Pegasus. Panyi states:

> I can't even count how many lawsuits I'm part of right now. Suing the German foreign intelligence, suing the state of Israel, suing the Hungarian government, because all these NGOs of course, saw an opportunity here that there's direct evidence of surveillance. So now they are trying to take legal action to prevent these things from happening again to other journalists, and I'm very happy to participate in these legal actions.

Other respondents like Gavarrete and Oliva are also involved in similar lawsuits. Bredoux explains how nothing will be as effective as legislation, noting, "the best way to counteract is to ask for legislations on surveillance – states have to ban these spywares."

In addition to Access Now, Amnesty International also investigated journalists' devices upon suspicion of surveillance. Lenaig Bredoux described how Amnesty International checked her phone in Berlin, which confirmed it had been infected in 2019 and 2020. Bredoux was first informed about the Pegasus attacks by another non-governmental organization, Forbidden Stories, a Paris-based non-profit organization dedicated to supporting journalists facing threats. They first revealed the news of the Pegasus attacks through a journalistic collaboration entitled

The Pegasus Project. Szabolcz Panyi had a similar experience, after he was informed about surveillance via Pegasus through Forbidden Stories,

> They requested to let my phone be analyzed by Amnesty International…We didn't know whether the surveillance was still active. So obviously, they didn't want to get compromised and they didn't want to tip off the Hungarian authorities if they are still hacking my phone, they didn't want to communicate through channels that are infected. So that's why this was a very secretive process. And also after, they asked me to use an alternative way of communicating with them not through my phone, but through some other device and channels that were deemed more safe.

The secretive process described by Panyi was a common experience among journalists who had their phones analyzed by organizations such as Amnesty International and Citizen Lab. They could not share the revelation with anyone at first, including their family and sources, so as to not tip off the people spying on them.

Turkish journalist Ragip Soylu, who reports for *Middle East Eye*, explains how foreign publications are "often targeted by non-state actors." Like other respondents, he and his impacted colleagues at the publication also received the support of international organizations, namely Amnesty International, who provided analysis of their devices. He notes,

> I think some international organizations are giving phones to their reporters for just reporting purposes so it can prevent hostile actors from accessing their private photos or private notes. I think people do what they can do. But I think there's not much that you can do. It's not possible to completely stop the spying and, you know, eavesdropping on your conversations, because they got the better hand there, they are technologically more sophisticated than we could ever be, I mean no one is going to invest that much money to stop that.

While international organizations and research labs have provided tremendous support and resources for those targeted by Pegasus, their resources do not match up to that of much wealthier and technologically sophisticated corporate and national forces that manufacture and deploy Pegasus.

Impacts on Personal Life and Professional Networks and Reputation

By assessing the personal and professional dimensions of the impact of being surveilled using Pegasus, this chapter discusses the ramifications of such intrusive surveillance on journalists' personal lives, family relationships, and professional careers and reputations.

Impact of Surveillance on Personal and Family Life

The invasive surveillance via Pegasus has left journalists stressed, anxious, and paranoid. Julia Gavarrete says,

> You live with eternal paranoia, like every time you are always thinking that someone is following you or listening to you, and that also impacts your work. Because you feel anxious or under stress, because of that, you cannot operate, like your mind cannot concentrate at all and that's why sometimes we feel that after Pegasus we, at some point we have to go to, to take therapy or to try to talk about it with a professional.

Gavarrete explained how the stress and paranoia induced by the news of Pegasus has led her and some of her colleagues to seek professional help through a therapist. Respondents also described fear not only on behalf of themselves, but also their families. Upon discovering she had been targeted via Pegasus, Lenaig Bredoux deleted all pictures of her children stored in her cell phone.

Soylu also feared the possibility of hackers downloading and leaking private photos, videos, and conversations in the initial moments of the investigations. He describes feeling "set off" at first, as for 2-3 weeks, he had not yet confirmed he was hacked and was in a state of worry. After some time passed and following the investigations, he explains

> Eventually, I think I came to terms with the fact that they already got whatever they got, and they didn't leak anything because there are some incidents and examples like for example, Arabic female presenters, their pictures were presented on social media, like they probably cover with headscarf but they leaked pictures of them without the headscarf and things like that.

Compared to other targets of Pegasus, Soylu notes that he was lucky. He uses the example of Muslim female journalists and newscasters who were also targeted. Hackers used intimate pictures and videos as blackmail and leaked them to the public, with detrimental social consequences. This was the case with Azerbaijani journalist Khadija Ismayilova, another target of Pegasus, who was subject to continued surveillance for over a decade and whose intimate videos of her and her boyfriend were released to the public after she refused to submit to blackmail (Forbidden Stories 2023). Omar Radi, a colleague of Lenaig Bredoux, was also targeted by Pegasus about a year before his imprisonment in Morocco for anti-state and rape charges.

Bredoux suspects that as a French journalist reporting on sexual violence, the Moroccan government likely spied on her to collect information on sexual abuses to imprison her colleagues, citing Omar Radi as an example. Charging journalists with sex crimes is a tactic deployed by the Moroccan government to punish journalists and eliminate public support for the accused. Previously, journalists faced with anti-state charges were seen as noble heroes, but the sex crime charges render them morally indefensible. Increasing reports by international journalist coalitions like the Center to Protect Journalists cite that being faced with false sex crime charges are a growing fear, and there aren't many journalists left working in Morocco. Most either left out of fear of being targeted or are imprisoned. Szabolcs Panyi also referenced the more drastic consequences other journalists faced in less democratic nations, noting some victims of Pegasus were killed, like Mexican journalist Cecilio Pineda. The situation of the aforementioned Azerbaijani, Moroccan, and Mexican journalists are far more drastic than those of the respondents I interviewed, but at least four respondents mentioned the cases of these particular journalists in discussing the personal impact of Pegasus.

Amidst the investigations into Pegasus by Citizen Lab, Amnesty International, and Forbidden Stories, Szabolcs Panyi described the anxieties invoked by the secrecy surrounding the investigation:

> The internal rules of the Pegasus project were pretty strict. So we couldn't even essentially tell anything to even our loved ones or relatives of what we're working on. Because, you know, there was this suspicion that maybe some of the devices around us are still hacked. So there were very strict measures. So I freaked out.

Nearly all the respondents were part of an investigation by the aforementioned organizations, and the climate of secrecy added to the stress of Pegasus surveillance. In the beginning, Panyi describes how they were very paranoid and overcautious, wondering whether they were still being spied on. This had a devastating impact on mental health, a sentiment shared by several respondents who described mental distress and seeking out professional help. While the investigation was still going on, Panyi's publication feared their internal communications may have been compromised, and ultimately found out the government had been caught off guard once the investigations were made public. When I asked how it affected his well-being, he noted that the question caused him a bit of stress, on account of other journalists in more authoritarian nations being murdered or imprisoned as a result of Pegasus surveillance.

> In the end, it made me stronger and I don't really want to complain. So I always stress whenever I'm asked how did you feel? How do I feel that there were journalists murdered, journalists torture, journalists who were jailed? There's diversity in abusers of the spyware. Not Hungary or Poland or Spain, EU countries, countries that belong to families of democracy, but Mexico or Morocco, or Azerbaijan, and other countries, so I don't really want to portray myself as a victim, to whom terrible things have happened. Because it didn't happen. I mean, it's not good. It's not a good feeling that I was surveilled. But, in the end, I just feel extremely lucky that they didn't do those things to me that they did to other journalists. And it even gave me more strength and inspiration. Who am I to be afraid to do this job? Who am I to be scared of certain stories, when other journalists had the courage to pursue investigative stories even at a huge personal cost.

Some respondents noted feelings of guilt, on behalf of people they were in contact with, such as family members or sources. Xenia Oliva describes,

> It made me reconsider if it was worth it to keep working on this because I felt guilty because of my sources and my friends and family members who had been talking to me, so maybe a lot of them had been exposed…But now that some time has passed I think I'm trying to get back on track of my work and to focus on why it's important to do what I do. So maybe not like a direct impact on my career but like an emotional impact for you as a person.

Oliva notes that Pegasus had a larger effect on her emotional and personal life than her career, because she was consumed with guilt, forcing her to reconsider her profession for a time, before ultimately realizing the importance of a journalists' work.

Upon Pegasus reaching the news headlines, with Smita Sharma and many other journalists' names publicly listed, Sharma shared how she initially received praise and congratulations from family and friends outside the journalism profession. She explains:

> Unfortunately the day the story actually broke. I was at the funeral of one of India's most prominent photojournalists, Manisha Siddiqui, the Pulitzer Prize award winner, who was killed in the front line in Afghanistan and vanished with a friend. And when the story broke, and my phone started buzzing, and I wasn't in a position to take calls, and a lot of my friends from across the world, they started sending the congratulatory texts that while you're on this super, you know, sort of sexy list that looks so like you you've made it big in journalism…because all these friends who have not bothered to ever give me your feedback for my story in the last 20 years are really sending me these congratulate projects that I've made my name into this Pegasus list. But these jokes apart, you don't want to worry your friends and your family. You don't want your family to get into the nitty gritties of what really can be the consequences. But when you sit down in the journalistic community, and especially in a country where over the last six, seven years we have seen extremely dangerous politics play out with a very sharp, depressing decline where a lot of journalists have either been financially threatened, legally intimidated, or they've been put behind bars under very draconian laws dealing with national security. …my mom actually called me up to say "Smita I am very proud of you, you have become super famous," and I was like, Good lord, other mothers are all worried and this one is

> like congratulating me. But jokes aside, they started to realize what Pegasus was really about and that this wasn't some fancy list to get on to.

After the initial praise she received from friends and family, she explained after learning of the extrajudicial killings and imprisonment of journalists and activists, and after realizing the dangers of Pegasus, they took the matter far more seriously. Sharma described the negative side of her experience experience being targeted, elaborating:

> I am used to getting trolled. I'm getting used to being abused on social media. I have my defenses. I have my network of people that I find my strength in, but they are people who just don't know how to deal with all of this. I'm a first generation journalist in the whole family. I think they definitely are very, very worried every time they see the stories. In my case, I would say I've still been very, very privileged in terms of you know, I have not faced even 10% of the kinds of stuff that so many journalists across the world today have faced including many of them who have also lost their lives who have been killed by because of state or non state actors.

Sharma shared a similar experience to the Salvadorian journalists who endured online harassment campaigns following the Pegasus scandals. These online trolls were suspected to be enabled by both government and ordinary citizens who blame journalists, on account of not understanding the importance of privacy. Sharma explained how through her shows, she has explained to people why the deployment of Pegasus is a massive violation.

> I know when my name came out in the list when I was getting all these messages on social media, and many of them were trolls because obviously my posts were critical. And many of the trolls that were enabled by the ruling party itself, and also ordinary people. The usual question I would get asked was so what if the government is listening into your conversations? How does that matter? Or, so what if your phone is hacked? What is the secret in your phone that you're wanting to hide? And I have to break it down to people that you know if you don't understand even the fundamentals and basics of how privacy works… I started asking people on my shows in Hindi, which is of course the language of the masses, why do you have curtains on your windows? Why do you have a lock on your door? Why do you have a password on your phone? When somebody is sitting in a seat next to you, during a bus ride, and they look over your shoulder and look over your messages or your photos as you're scrolling down? Does it bother you or not?

> Are you happy that strangers are just looking into your phone and into your pictures? So that's the level and sort of arguments that I'm looking at here in this country, which makes you understand where we stand when it comes to these issues.

The general public generally does not have an understanding of the fundamentals of privacy, making it that much more difficult to relay the dangers of Pegasus to the public. She experienced a sort of "victim-shaming," in the sense that she was blamed for being suspicious enough to warrant such intrusive surveillance. Sharma elaborated how Pegasus has been used to blackmail and imprison other journalists and activists under false pretenses.

> So when people don't even have an understanding of these fundamentals, how will they even understand that if Pegasus successfully impacts the phone, even through a zero click message where you actually haven't gone in and clicked on a zero message, that it can not only take everything on your phone, it can not only decrypt your so called encrypted messages, it can access your phone, your voice texts, your conversations. It can also be used to not only keep that data as a potential blackmailing tool on somebody, but for planting fabricated evidence and the Pegasus investigations across the world have pointed to the fact. The Washington Post reported on incidents in India where a lot of activists in 2018 have been put behind bars on allegations of wanting to overthrow the state. Their trial processes have become the punishment itself… When you do understand the seriousness of the depth of what a malware like Pegasus can do to you as an individual as a professional, somewhere at the back of your head, you are worried if they choose to plan some financial transactions on my banking network through my own which I have not done, and then use that to come up to me that I am on the payroll of some foreign agent. So these are real threats and real consequences we are talking about.

The lingering fear of being blackmailed or having her device planted with fabricated transactions or messages persisted within Sharma. This could manifest in real-life consequences through lengthy and unjust trial processes and imprisonment, as it already has for others.

Professional Reputation

Even though I did not ask respondents how the Pegasus leaks impacted their professional reputation, two respondents explained how Pegasus had a positive effect among their

professional networks, sources, and the general public. Despite the security and privacy threats Pegasus posed, being publicly listed as a target of Pegasus surveillance legitimized their career as journalists in a way. It is as though their work was captivating or groundbreaking enough to be worthy of such invasive surveillance. Szabolcs Panyi explains,

> This whole Pegasus thing brought me bigger name recognition - both internationally and locally in Hungary. And of course, that did help with sources, meaning that people know who I am. Some of them read my articles because they saw my name and realized this is a journalist who has been surveilled. So I think that in the end, I probably acquired more sources than I had previously, or at least in the long run. I think there's this positive effect but I can tell you that for example, another journalist who's been surveilled complained to me that some of some of his previous sources from the government outright were refusing to meet with him or to talk to him. Just pointing out the fact that you know, there was the threat of surveillance, so there's also an example in Hungary of journalists losing sources because of surveillance and it becoming news.

Panyi was the only respondent to state that the Pegasus leaks actually brought him more sources on account of the name recognition. Being publicly listed as a victim of Pegasus legitimized him to potential sources, who saw his name listed online as a target of Pegasus, and were prompted to read his work and reach out to him.

Panyi knew this was an anomaly because he followed it directly with an example of the opposite case with his colleague, who is struggling to reach sources as a result of the Pegasus surveillance becoming such widespread news. Panyi elaborates,

> This is not the type of fame that I wanted. I think every journalist is seeking a certain recognition based on the reporting that he or she is conducting. So, in my case, I think that as I said, there's a bigger name recognition. And, and it is attached to this type of controversy, or me being the subject of articles interviews. So I essentially became part of the story which is something that every scene journalist tries to avoid. Their editors tell them not to write themselves into the story because the story should be about what's happening. It should not be about the journalist or at least, this is how I see my profession as an investigative journalist. I'm reporting on the facts but when I became part of the story, then I couldn’t do anything. So I'm not that happy about this. I would rather have

> my name out there being famous because of what I did, not because of what happened to me.

While the news of Pegasus brought Panyi more name recognition, he notes that as a journalist, this was never the kind of fame he sought. Journalists want to be known for what they do, or for what they report on and write, not for something violating that happened to them. One of the primary rules that journalists must follow is to never allow themselves to become part of the story, but in the case of Pegasus, they had no control over becoming part of this international and scandalous story.

An Indian journalist who wished to remain anonymous, said that because he is no longer an active journalist, "it only helped my career because in a sense, there's a certain halo around my head. So people treat you with more respect." Being a retired journalist and pursuing an academic career, the news of the Pegasus attacks made him more respected by colleagues and others he encountered. People saw him as a legitimate journalist, as a brave victim, and as someone working toward a greater good on account of being targeted for such invasive surveillance. Had he been still actively reporting however, he notes that it could have been very damaging to his career and his sources, as India has a very tumultuous climate for journalists and press freedom overall. It is important to note that his request for anonymity, which differs from all other respondents, hints at a lingering sense of fear in an unsafe climate for people critical of the government in India.

Journalist Relations with Sources and Institutions

Similar to the ramifications of Pegasus on the personal lives of journalists, nearly all respondents noted that their sources and their ability to reach them were adversely affected

following the Pegasus leaks. Even Panyi, who described some benefits due to the name recognition the Pegasus scandals provided, explained,

> It's very interesting because on one hand, I think there are people who are not talking to me because they are afraid of my name and face being out there. They know that I've been under surveillance in the past, so there's no guarantee that I'm not currently under surveillance. But the tricky thing is that you can never tell why someone refuses to talk to you or to sit down with you. Because even before Pegasus it was extremely hard in Hungary to get a source to talk on the record. Or even to get someone working for the government to sit down with you. So that has already been a big problem.

So, even though some sources were more willing to come forward due to the name recognition and legitimacy the widespread news of Pegasus spyware brought for Panyi, there was still a hindrance in reaching other sources. However, there is no way to truly assess why sources don't come forward, nor a way to quantify how many sources have not come forward. Panyi notes how in Hungary's climate, even before the Pegasus leaks, it was difficult to reach certain sources. This demonstrates how declining press freedom inhibits sources from talking to journalists on the record, in turn shaping the stories released by the press.

The Pegasus attacks severely threatened source confidentiality, an element crucial to the integrity of journalism. Salvadorian journalist Xenia Oliva explained that "they were really unwilling to talk anymore." She elaborates how although the Bukele regime boasts about not imprisoning or executing journalists, the regime has still imposed measures that hinder journalists' ability to work.

> Even though the president brags that they haven't jailed journalists or they haven't killed any journalists, how we used to work is changing. Firstly, because the sources are afraid. People are afraid to talk to us. Also, the police and the military are present when you are reporting certain topics. They have felt encouraged by the government to harass you, to tell you to go away, or to take your equipment, or erase your picture. So this has been happening a lot in this government. So, the limits to our work have been increasing. And also regarding some coworkers, some colleagues, they have been harassed by

> government figures, both in person or on social media... So yeah, they haven't jailed someone but there have been a lot of things that have been making it harder to do our jobs.

She noted that a few sources were still willing to be in contact with the journalists immediately following the news of the Pegasus attacks, as they were accustomed to the suppressive Bukele regime and wanted to continue working with journalists to reveal human rights abuses. The respondent who is no longer an active journalist and wished to remain anonymous discussed how the inability to reach sources following the widespread news of Pegasus surveillance affects the kinds of news stories that come out.

> If I was an active journalist, maybe I would pick a different story, because my sources will not have spoken up. They may be scared to send me any document, any messages on my phone. It would have been very different had I been actively reporting…because it puts all of your sources, especially government officials, etc, under a lot of pressure.

When the news of Pegasus spyware being deployed against journalists and dissidents became public, source confidentiality was threatened. This put pressure on sources and instilled fear in them, particularly those in vulnerable positions, like government officials whose careers and safety may be threatened. Sharma explained, "as a journalist, it's not just about you. It's about the ecosystem that you're interacting with. It may not be about collecting data on you for immediate use, but it could be about keeping potential data on you that can be used at a later stage." In this sense, surveilling journalists has a ripple effect on everyone they have been in contact with. Most importantly, sources are sacrosanct to journalists, elaborated Sharma, so when that communication is threatened, the entire profession suffers.

Immediately after the news of Pegasus leaked, impacted journalists lost many sources. Turkish journalist Ragip Soylu explains the mass paranoia exhibited by journalists and sources alike:

> Initially, people were left feeling all exposed as your source because you got their names and things like that. But it eventually died out because no state scandal came out of it. Nothing major happened. So people just stopped thinking about it. I think there's an understanding among all the sources that I have, is that [surveillance] is a fact of life.

For Soylu's sources, there was only an initial hindrance in communication, noting that the fear and paranoia was mostly short-lived. This is because in Turkey, no particular state scandal was revealed via Pegasus hacking. Soylu also mentions how surveillance has become a fact of life, which he and his sources have come to understand.

Salvadorian journalist Julia Gavarrete expressed a similar sentiment, noting the initial paranoia surrounding the widespread news of Pegasus surveillance on journalists.

> Many sources were very afraid to talk since the moment that they knew about Pegasus. They said "I don't want to be in touch with you anymore." So we lost a lot of sources. But, at least there were other sources that stayed. We had to create new ways to communicate with them. So that not only puts a lot of pressure on you, but also on your source, because when you talk with them, you have to be very clear and be very specific, and that we are going to try to take care of all of our lives, but also the information that we are going to share, or the way that we are going to take it. I think many sources understand that because when you get in touch with one of them, you use safe or safer ways to communicate.

Communications with sources have been substantially hindered and altered following the Pegasus revelations. Either journalists lost their sources altogether or had to look to newer, safer ways to communicate. Gavarrete describes being much more clear, specific, and intentional in all her communications with sources, and provides them with continual reassurance that she will do everything she can to protect them and the integrity of the story. Ultimately, the Pegasus revelations not only hindered journalists' ability to reach sources, but also forced them to transform the means in which they communicate with them.

Following the Pegasus scandal, Smita Sharma explained her students' and colleagues' increasing concern surrounding the use of advanced technologies and artificial intelligence in journalism:

> So what has happened is that there is definitely a lot more emphasis now on how technology is being used in newsrooms, as well as how technology is being used to control journalists, or to intrude into their lives that has become a part of the discussions that we have. I do see students come up with a lot of questions around not just surveillance tools, but also modules of what artificial intelligence could do to newsrooms and journalism moving forward. What could ChatGBT do to editorial interventions? What could ChatGBT do to primary sources, the essential fundamentals of a reporter going to the ground and collecting that information? I just recently made my students actually take handwritten exams. Because we still do not have ChatGPT detection tools.

Advances in technology, whether it be spyware or artificial intelligence, have forced journalists to change their journalistic practices. Surveillance of journalists is not a new phenomenon, however, the difference with Pegasus is its far more invasive nature that violates every aspect of its target. Sharma recounted her past travels to countries with a high degree of surveillance and control, like Syria, Iran, and Pakistan to cover foreign policy events reporting from the ground. Over the years, before Pegasus, "we have been used to certain degrees of surveillance, through more traditional tools and methods," she elaborated:

> When you for instance, go to a country like Pakistan to report, especially as an Indian journalist, from the moment that you land at the Pakistani airport, you will have physical surveillance, there will be agents who will be tailing you constantly no matter where you go, and more often than not, these agents will actually go and not just meet up with people that you've had meetings with, but in a lot of cases also harass them. They will ask them about their proof of identity, about what the conversation was about, when they were meeting me?... Some of the people I've met over the years have been roughed up once I left the country. These are things that you are used to in countries where democracies are not strong, where there are either autocratic regimes or military takeovers. I know for instance, in Syria, I learned a lot of things on the job.

Surveillance was not foreign to Sharma in her long career as a traveling journalist reporting from high-risk countries, where she was forced to learn how to deal with surveillance on the job. In Syria, she witnessed sources asking her to remove the battery from her phone during their conversations. She explained how after coming back from a reporting assignment, she would receive calls "from spooky, odd numbers in the middle of the night with somebody saying my cousin has died, and naming somebody who is actually not a relative."

These kinds of mind games and psychological operations are meant to intimidate journalists and hinder the reports they publish. After relaying her past experiences with surveillance, Sharma assessed the difference of Pegasus surveillance, explaining:

> I think what Pegasus changed was the fact that when you find yourself named like this, it does feel like you're violated. Most importantly, it's the sense of violation. It's a sense, not just of a violation as a journalist, but as a citizen, as a woman, and as an individual. Unlike a lot of impacted ordinary citizens in India, who either do not have an idea about privacy or who really do not care about privacy because there is not much awareness. The daily struggles of bread and butter are way more extreme to be able to focus on issues of technology and privacy. So for me the fact that the state would want to listen into my conversations, that the state would want to have access to my phone camera when I'm in my drawing room, or when I'm in my bedroom, to try and get access to my private intimate conversations or my photographs, even when it would have nothing to do with the state at all or even to do with my professional life. But just as in person. I think that was not shocking, but it was definitely very, very disappointing to me. Also just the sheer fact to wrap my head around why would you want to spend millions of dollars on software.

Pegasus was a different kind of surveillance that was particularly violating for Sharma. Before, the surveillance she experienced was more or less restricted to her professional life as a journalist. But with Pegasus, her entire personhood was violated, as well as anyone she was in contact with. Any sense of privacy she may have once had was now robbed from her. In a country where the average person is more concerned with daily struggles of survival, privacy is

not a big issue for the general population, which makes it all the more outrageous that her government would throw away millions of dollars on the democracy-eroding software when the millions of dollars could have helped a struggling population.

Individual Counter-Surveillance Methods Practiced by Impacted Journalists

This section analyzes the counter-surveillance tactics employed by journalists to assess how they are changing their practices in response to being surveilled by Pegasus. All respondents now practice encryption. Gavarrete received support in learning encryption practices via Reporters Without Borders, an international non-profit and non-governmental organization which offered a four month long digital security course in Germany. Gavarrete said, "I learned a little bit more about how to encrypt my storage, my information, and how to download information that was sensible in encrypted folders." She also described feeling safer using encrypted applications on her computer for work communications and storage rather than her phone, noting how everything in a phone is vulnerable. One method of practicing encryption is the use of disappearing messages, "making it harder for them to keep track of it because they cannot connect to your phone all day. They need to distort the data from time to time," Soylu explained.

Additionally, Soylu, Sharma, and Oliva cited the use of "Signal," an app that offers an encrypted service for instant messaging, voice, and video calls via one-to-one communication between users or groups. Respondents also described avoiding the use of the landline phones in their homes and offices. Soylu explains,

> If I want to speak with [a source] on the phone, I will probably use Signal because Signal provides the best protection…it's hard for spying companies or buying actors to listen or drop in on that call. But if you're messaging with each other, it's easier for them to store and access that data. But for example, if you're speaking on Signal and you are maybe on

> WiFi and then you just turn off the WiFi and go to the regular reception. Even that change also corrupts the data and they cannot listen and so it's hard for those companies to listen.

The use of Signal encrypts data, making it difficult for those deploying spyware programs like Pegasus to interpret journalists' communications. Even turning off WiFi or using a VPN can help further corrupt that data. Sharma further explained how she was always very cautious in terms of not opening links or anything that looked suspicious.With Pegasus infections being zero-click, following this news, Sharma said,

> Now I am perhaps multiple times over more cautious about what I do. I don't like keeping any conversations on my phone for too long anymore. I have a habit of deleting my call lists every night. I have a habit of deleting most of my conversations every night. There are sensitive conversations for which I have now switched over to Signal with a lot of people that I do not rely on WhatsApp anymore.

This use of encrypted applications in professional communications was common among respondents, as well as habitually deleting the data stored on their phone. While useful, Xenia Oliva describes the barriers to using encrypted applications in El Salvador.

> For example, if I'm trying to speak with a family member of a person detained, it's hard because [sources] don't have, for example, much money to buy data for their phones. So they mostly use WhatApp because sometimes you pay $1 for data, they give you "WhatsApp pay for a day" or something. So I can't ask them to download Signal because that will imply they have to buy more data to use Signal. So yeah, we have to use WhatsApp, but in other cases, we tell the person to please use ProtonMail.

In circumstances when "Signal" is too expensive for sources to download, journalists may resort to cheaper, less safe options like WhatsApp. In some situations, journalists may advise their sources to use ProtonMail, an end-to-end encryption service that protects email content and user data before they reach servers. One of the respondents, Ragip Soylu, used ProtonMail in all communications with me. Gavarette also cited the use of Wire, an end-to-end encryption service for all messages and voice calls.

In times when digital surveillance is so pervasive, Soylu explains how face-to face interactions between journalists and sources are increasingly important. In these cases, respondents describe leaving their phones outside the room, or on airplane mode, to ensure no one is using the phone as a microphone to listen in on the conversation between a journalist and a source. Sharma echoed a similar sentiment, noting:

> There are sources within the government. There are sources which are official voices that speak to journalists under conditions of anonymity on the basis of trust. So when that starts playing in your head, you get to see some difference in behavior even if the person in front of you earlier was happily having cups of tea with you. Now perhaps he is a little hesitant in terms of meeting you constantly…Of course as a journalist, you do tend to have different levels of sources. If you're not getting information from source X, you try to reach source Y or Z and be persistent with that. But it does impact you in the sense whatever I do now, if I'm having sensitive company info, or a conversation with anyone, I would rather not have my phone anywhere nearby. I would rather want to have [the conversation] in person. I would perhaps, if I have my phone, maybe switch it off, maybe put it on airplane mode, things like this. They are there at the back of your head to keep playing you know once you you know that you've been potential target

In regards to how she handles communications with sources involving sensitive information, Sharma insists it depends on several factors. First, in looking at a body of work, sources have an understanding of whether they are communicating with a serious journalist. In times when face-to-face interaction and encrypted applications are unavailable, Sharma noted:

> I'm still using WhatsApp calls for a lot of sensitive conversations because I think there's also the realization that even if the government is wanting to snoop like in the last attempt, of course, if they didn't succeed, who's to say that they haven't tried since then? Who's to say that even if I've changed my sim card or my chip that it is not corrupted already? But that doesn't mean that you will stop doing what you need to do. So at the end of the day, you do try to be as confidential as possible. You try to take those necessary precautions. But sometimes those precautions cannot be put in place because of certain reasons: geographical distances, time zone differences, or scheduling issues. You have to take that leap of faith anyways, because that story is more important for you to tell and you can deal with the consequences later on. So I think the sources, once you've

> been in the field for a pretty long time, and if they know that you are a serious journalist, they will take that risk.

Sharma still uses WhatsApp when in-person meetings and encryption are not available, because she can never be certain that she is not being surveilled, and she recognizes the importance of her job and continues to report stories. Although surveillance may inhibit sources from coming forward, she noted that as a serious journalist, there will always be some sources who want to speak with her on issues they believe are greater than themselves.

> There may of course be a number of people who may have cold feet and who may decide to not speak to you. But more often than not, I think people who have a conscience and who want to speak up on issues they think are more important and consequential than their own individual selves. They will not stop just because they are being surveilled because it's like victim shaming also to some extent. Why should I be ashamed that I have been surveilled? Why should I be deterred? I have not done anything wrong. I am not exchanging classified secrets. I am not doling out national classified secrets to some enemy country… So if my story has to go out tomorrow and I'm not able to meet somebody in person, I will talk to that person whether it's on Signal or Telegram or WhatsApp, I will find a way there are different ways of communication today. I think that's the double edge sword of technology. There is a lot of good to it. There are also the dangers to it, but you just need to take those calculated risks depending on how urgent the story is and how important it is for that story to be told.

Sharma described how being victimized by Pegasus should not inhibit her work, as that would be a sort of victim-shaming to let her work be adversely affected, especially when she has not committed any crime. Technology is a double-edged sword when it comes to journalism, as it allows for harmful softwares like Pegasus to be manufactured, while also providing new and different methods of communication for journalists and their sources. In any communication in a post-Pegasus world, journalists and sources are taking calculated risks, on the basis of the urgency and importance of breaking a story to the public.

However, Sharma has limited her participation in WhatsApp groups, while also educating her family on digital safety practices. She explained:

> I really do not participate in WhatsApp discussions anymore, unless these are official WhatsApp groups, like for instance, the Ministry of External Affairs because I'm a reporter. I'm a part of the media group that all press releases come to, they're the official groups where I have to be a part of for dissemination of information, but I'm not a part of any WhatsApp group discussion group that would arise risk, I exited all of those groups, including my family groups. I told my family very matter of fact in categorical terms that any posts, any messages, because they are not as informed as I am, as they are not journalists. They are very ordinary people who are getting WhatsApp forwards through the day on different polarizing issues, subjects and communal issues, which they may not even be aware of that you know, if you're forwarding that to me it could result in some sort of a case against you in a lot of things, or they could be forwarding some news, which is actually not even true. So I've had to tell them and I've had to sort of educate them to not have a discussion with me on critical issues on WhatsApp or on these text platforms, because I don't want them to be touched in any way.

Because of the limitless bounds of Pegasus spyware once a device is infected, Smita Sharma's counter-surveillance practices include instilling caution in her close friends and family, to protect their safety. Even sharing a news link via WhatsApp family group message as many ordinary families do could put them at risk, especially considering Sharma's repeated targeting for surveillance in a country where press freedoms are lacking.

Bredoux explains that since the news of the Pegasus attacks, she now has two phones, one for her personal life and the other for her professional career. She stores far less things on her phone and describes being much more cautious than before in communicating with sources and storing information. Unlike the rest of the respondents who have modified their use of technology in their journalistic work, Szabolcs Panyi has opted to avoid technology almost completely. During our interview, he showed me a notebook, explaining:

> This is a notebook that I've been writing in since mid last year and this is another notebook I've been writing in since last autumn and I store everything there. I'm not

> typing down anything on my computer anymore that's more sensitive. My short-term memory has not been good, historically…But right now I feel that since I store all the information offline in handwritten notes, this is in one word, overwhelming, but this is the only way until I figure out an entirely safe method of how I can store my information digitally. Until then, I just have to rely on these notebooks and also, I'm more mindful of where I bring my phone and to put away my phone if I have any meetings.

The all-encompassing bounds of a Pegasus infection makes it quite difficult to digitally contact sources and store sensitive information in a safe way. With end-to-end encryption not widely available nor easily accessible, some journalists like Panyi have resorted to handwritten communications for the time being.

In addition to legally summoning the deployers of Pegasus, in his testimony, Saikat Datta emphasized the importance of encryption, and limitations in accessibility among the Indian population. In recommending the deployment of end-to-end encryption (E2EE), he notes, "As it stands right now encryption does not apply to most phone calls, making them vulnerable to interception…These are the first and, in many cases, the only line of defense." While several respondents received some resources from NGO's and had been taught how to encrypt data and safely contact sources, this is certainly not the case for all impacted journalists like Panyi, who continues to struggle with the use of technology in his work following the revelation of the Pegasus attacks.

Conclusion

Summary of Results

In the first chapter of the analysis, I outlined my findings on the geopolitical circumstances of select countries deploying Pegasus. First, I analyzed the case of India and Turkey as countries whose press freedom ranking is quite low and whose national media is almost entirely controlled by their respective governments. As a result, journalists in these countries, especially those employed by national publications, exhibit major pressures to write stories uncritical of the government. Then, I analyzed the case of El Salvador and Hungary as nations with more varied media landscapes, and more critical and investigative journalists despite heightened government sponsored attacks against journalists. However, journalists who are critical of the government in these nations are often subject to online harassment and political violence. Lastly, I analyzed the more unique case of cross-country surveillance of French journalists by the Moroccan government. Moroccan surveillance of French journalists is suspected to be a part of the government's tactic of charging French Moroccan journalists critical of the government with sex crimes, as numerous Moroccan journalists spied on via Pegasus are currently imprisoned in Morocco.

In the second chapter of my analysis, I assessed the efficacy of the response of both national entities and international journalistic and human rights organizations to the threat of Pegasus. Overall, all but two respondents, both from India, felt supported by their national publications following the leaks about Pegasus, describing their responses as urgent, serious, and productive. However, respondents explained that the resources of their national publications are miniscule compared to the wealthy and militarized institutions deploying Pegasus. International journalist and human rights organizations and research labs such as Reporters Without Borders,

Amnesty International, Access Now, Citizen Lab, and Forbidden Stories have provided support to journalists by analyzing impacted devices, spearheading lawsuits against the NSO Group and governments regarding the illegal use of Pegasus, and providing digital security information to assist journalists.

The third chapter assesses the impact of Pegasus spyware on respondents' personal lives and safety, professional reputation and networks, and journalist-source relations. The initial reaction of all respondents following the news of Pegasus surveillance was characterized by paranoia, fear, and guilt, on behalf of themselves, their loved ones, and their sources. As journalists they had all been used to some degree of surveillance, but Pegasus violated their entire personhood, beyond just their profession, and changed the way they conduct their work. Despite the overall negative implications of Pegasus on the journalistic profession, at least two respondents described how the widespread news of Pegasus actually had a positive impact on their professional reputation. They described being treated with more respect and seen as legitimate journalists. The news of Pegasus also hindered communications between sources and journalists, as such pervasive surveillance threatened source confidentiality and thus source safety. Respondents expressed frustrations with the fact that their governments were willing to spend so much money to violate their privacy and human rights when there are far more pressing, life-threatening issues that the money could have rather been spent on.

In the fourth chapter, I delved into the ways journalists have employed counter-surveillance methods in response to the Pegasus revelations. Journalists have had to create new ways to communicate with sources so as to protect them, their story, and the overall integrity of journalism. Many were forced to learn more secure ways of using technology and storing data, with the help of encryption practices. Others opted to reduce their use of technology

altogether in their professional communications, preferring face-to-face interactions with sources, the use of pens and notebooks, and leaving their devices outside the room or on airplane mode in professional meetings.

Contributions to the Literature

My findings use the case of journalists targeted by Pegasus spyware to expand on and support much of the prior research on surveillance, counter-surveillance, and the development and politics of Pegasus. First of all, they support and build on Agamben's theory, in which states obsessed with security as a source of legitimacy can result in the state turning itself into a terroristic entity (2002). Governments accused of surveilling my respondents – Turkey, India, Hungary, El Salvador, and Morocco – are all primarily concerned with issues of national security and controlling national press. This obsession means democracies resort to control as a means to sustain and defend themselves, even if it leads to disorder and destruction (Agamben 2002). Respondents described how the press is controlled in their countries, albeit to different degrees, either through direct government ownership of the majority of the press, or indirectly through the threat and reality of surveillance affecting journalist-source communications, in turn shaping the kinds of news stories that come out.

My findings also support theories of surveillance as a form of social control in modern societies, namely Haggerty and Ericson's conceptualization of "surveillant assemblages" (2000). The surveillant assemblage is a post-panoptic development in surveillance studies that refers to de-territorialized forms of social control, or the variety of technological systems utilized by state and nonstate actors to monitor citizens. The surveillant assemblage is also immensely vast, and Pegasus spyware is one of many discrete technological forms used to analyze and infer patterns

of behavior in the interests of social control (Haggerty and Ericson 2000). Surveillant assemblages act as recording machines, and a Pegasus infection is the most recent mechanism of recording journalists, dissidents, and government officials. Such surveillance aligns with Haggerty and Ericson description of post-panoptic surveillance as limitless, unstable, and lacking government accountability, as state and nonstate actors have manufactured and unjustly deployed this illegal spyware with little consequence. Post-panoptic surveillance is exponentially larger in its capacity with expanded functions for purposes of control, governance, and security (Haggerty and Ericson 2000). It also levels hierarchies of surveillance by monitoring new populations, and in this case, journalists. My findings on Pegasus surveillance of journalists corroborates this, as both the threat and the act of surveillance of journalists' devices initially halted journalistic investigations and in turn adversely affected source relations and storage of sensitive information. This impacts the kinds of news stories put out, and in some nations, such as Morocco or Mexico, has led to the execution and imprisonment of journalists.

Additionally, my findings support Haggerty and Ericson's concept of consumer-based surveillance (2000). Based on the information from my respondents and the analysis of impacted devices by various research labs, it was evident that Pegasus spyware was used to locate journalists and their contacts, as well as collect their communications on applications such as WhatsApp. Not only does Pegasus serve the state actors assumed to have purchased it, but also its corporate manufacturers, the NSO Group. In this sense, my findings on the manufacturing and deployment of Pegasus relates to Zuboff's conceptualization of surveillance capitalism (2016). Surveillance capitalism's dominant logic is based on data accumulation, in turn disproportionately empowering technology companies who have total control over the digital landscape. This model renders surveillance technologically dependent, and allocates technology

companies, like the NSO Group, with power that threatens individual autonomy, sovereignty, dignity, and the foundations of democracy (Zuboff 2019).

Furthermore, my findings expand on theories of dataveillance, using the specific case of journalists. As a form of surveillance based on mass data collection, dataveillance builds profiles on individual behavior and predicts their future behavior, ultimately interfering in individual decision making (Van Dijk 2014). Turning data profiles into commercial goods makes sensitive information about individuals, groups, and organizations vulnerable to third-party actors with malicious intent (Christl 2017). Such commercially motivated surveillance practices led by the NSO Group threaten civil society as a whole, but the risks and social consequences are especially high for some groups (Salzmann 2021). My findings proved this to be especially true in the case of journalists. This is because at a time when technologies and smartphones are used as work tools, and in a global climate entrenched with surveillance capitalism and dataveillance, journalists engaging in mobile journalism are at heightened risk of surveillance (Salzmann 2021). The Pegasus hackings corroborate this, as they revealed not only that hundreds of journalists around the world were subject to dataveillance, but also have changed journalists' professional conduct according to my respondents. Specifically, the role of a journalist is to investigate and report on current events. This requires contact and communication with sources, who may also be vulnerable populations, such as prisoners or high level government officials. In other words, journalists track others, and as they do so, they are being watched by third parties, translated into data, then sold to business or government markets for behavioral prediction (Salzmann 2021). As a spyware developed by a corporation and licensed exclusively to governments, Pegasus is yet another mechanism for social control, ultimately undermining news work.

My findings also support and expand upon previous studies showing how spying on journalists threatens source confidentiality and undermines journalistic work and integrity (Thorsen 2019). My respondents almost universally described how the widespread news of the Pegasus attacks made their sources distant out of fear of breach of confidentiality, in turn changing the kinds of stories that were published following the initial news of Pegasus, based on limited access to sources. Respondents explained how they and their colleagues were subject to tracking of their activities, hacking and theft of data, public shaming, online harassment, cyberstalking, confiscation or destruction of devices, and disrupting operations through account hijacking or denial of service attacks, which supports Thorsen's assessment on the ways in which digital surveillance harms journalists (2019). Respondents described how they were separated from their devices following professional analysis, or getting rid of devices all together. Additionally, respondents from around the world described being subject to online harassment campaigns. Other respondents described how operations within their publications were temporarily halted following the news of the Pegasus attacks.

Perhaps the finding most contrary to previous research was the positive impact the widespread news of Pegasus had on a journalists' professional reputations, as described by two respondents. While much of the previous literature assesses the negative impacts of surveillance of journalists, and rightfully so, two respondents explained how following the revelation, they were treated with more respect and felt as though their careers were legitimized as journalists, as if their work was worthy of such surveillance suspected to be from powerful state actors. One respondent explained his unique position in that unlike other respondents, his ability to reach sources was not adversely affected, and in turn had improved on account of the public name

recognition the Pegasus scandal brought, enabling his sources to see him as a legitimate journalist.

The surveillance of journalists in a digital landscape changes the way news is reported, but it is quantitatively impossible to assess how many stories have not been covered due to fear on the part of editors, journalists, and sources as a result of substantive or perceived surveillance powers (Mills 2018). My interviews with respondents' support this, with the exception of the aforementioned case, as most noted a severe hindrance in reaching sources immediately following the news of the Pegasus hackings. Panoptic frameworks understand both real and perceived surveillance as a mechanism of behavior modification, with the ultimate goal of making people more subservient to authority (Waters 2017). My findings show that in the case of journalists, this behavior modification is reflected in the increased difficulty in their work following the Pegasus scandals, either through hindered communication with sources, prolonged feelings of paranoia, and having to learn new methods of communication and digital security.

Previous literature outlines the psychological, professional, meso, and macro impacts of state surveillance on journalists (Mills 2018). My findings corroborate this, as all respondents described feelings of paranoia regarding personal safety and their sources. Professionally, all but two respondents described adverse effects on their investigative modes of work, either due to their own internal hesitations or that of sources. Respondents also described how entire media platforms in their countries are becoming increasingly vulnerable to pressure as a result of surveillance, with the Pegasus scandal coming at a time when press freedom rankings in their respective nations are getting lower and lower. On a macro-level, the surveillance of journalists by state and corporate actors, such as the NSO Group and governments who have purchased Pegasus, has dire implications for democracy, and the greater role of journalism in society. Many

respondents are from so-called democratic nations, who may be too self-congratulatory to realize the destructive effects of surveilling journalists on democracy (Mills 2018). The national responses of the respondents' nations further support this, as journalists have been left to themselves, their publications, and the efforts of internationalist cooperatives and organizations to fight against the use of Pegasus.

Respondents echoed previous literature in describing how privatization of such surveillance technologies with weak international oversight wreaks havoc by threatening civil society and democracy (Zureik 2020). Consequently, the majority of respondents are actively involved in lawsuits against the NSO Group, Israel, and various governments in hopes to remedy the damage by holding the perpetrators accountable. One respondent in particular testified before his nation's supreme court, emphasizing the threat imposed upon national security and privacy by the purchase and use of Pegasus from a private foreign company. Based on the experiences of the respondents in their personal lives and careers as journalists, my findings support previous studies on Pegasus stating there was no evidence of the use of Pegasus associated with positive outcomes (Zureik 2020). Even in situations where respondents gained greater notoriety following the Pegasus scandals, the overall outcome of this surveillance was negative, either through lingering paranoia, online and in-person harassment and intimidation, restructuring the ways they do their jobs, and more drastically, the imprisonment or death of them or their colleagues.

My findings also support previous literature on counter-surveillance, defined as intentional disruptions of surveillance technologies to challenge institutional dynamics (Monohan 2006). To assume technological progress as simultaneous with political progress is optimistic and flawed, as the Pegasus scandal has revealed how technology can be co-opted to depict its respective notions of justice (Stein 2021). In the case of Pegasus, it has become evident

that the nations deploying Pegasus have done so on behalf of its notion of justice, primarily concerned with national security, monopolization of the media, and suppressing and intimidating investigators or critics. As a result, discussions of surveillance should be accompanied by references to counter-surveillance, featuring privacy law and advocacy, encryption practices, sousveillance, and their limitations (Zureik 2011).

All respondents have employed counter-surveillance methods one way or another following the Pegasus scandal. Even journalists under the suspicion of surveillance may use encrypted messaging, refuse to publish live locations, leave phones outside of meetings, and speak in code (Zablah 2022). Nearly all respondents noted leaving devices outside the room during meetings, and either the respondents themselves or their media platforms practice encryption one way or another. This practice transforms data so that it is illegible to unintended audiences (Thorsen 2019). Respondents described using applications like Signal or the Wire to encrypt all communications with colleagues and sources, in addition to practicing cryptography within data storage. Some respondents were taught how to do this through their media platforms or through assistance via international organizations such as Reporters Without Borders, who provided select journalists with a digital security course. One respondent described that he tries to avoid technology altogether, and uses a notebook in all communications and writings in his journalistic work. He notes that he only uses technology in his work when he absolutely has to, in the final processes of writing and publishing a story.

My findings on journalists' encryption practices corroborate previous knowledge on encryption, namely accessibility issues (Henrichsen, Betz, Lisosky 2015). Overall, there is a lack of knowledge on how to integrate defensive digital security measures such as encryption into journalism (Posetti 2017). While my findings show that organizations like Access Now or

Reporters Without Borders have provided select journalists with digital security resources, there remains a perceived lack of usability of encryption tools. In order to better ensure source confidentiality, it is necessary to ensure both journalists and their sources fully understand data anonymization and digital security communications. While my findings show that journalists are increasingly using encryption practices in response to Pegasus, there was little information on sources' knowledge of encryption practices, and it was evident that digital security practices were not widespread enough on account of lack of resources.

However, it is important to note that most respondents expressed that despite the counter-surveillance methods they employ with the support of their national publications and international journalist and human rights organizations, it is not enough in the face of the powerful entities that manufacture and deploy Pegasus, namely the NSO Group and the countries it licensed Pegasus spyware to. This is because they are far more wealthy, resourced, and militarized. As a result, some respondents note that the most important and effective measure would be to implement legislation that makes deploying this surveillance upon journalists internationally illegal and punishable. Almost all respondents are involved in lawsuits against Israel, the NSO Group, and various national intelligence agencies and governments. These lawsuits focus on the targeted surveillance of journalists.

Bibliography

Agamben, Giorgio, and Carolin Emcke. 2002. “Security and Terror.” *Theory & Event* 5(4). doi: 10.1353/tae.2001.0030.

Amnesty International. 2023. “Forensic Methodology Report: How to Catch NSO Group's Pegasus.” *Amnesty International*. (https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/).

Ashcroft, Bill, Gareth Griffiths, and Helen Tiffin. 1998. “ Key Concepts in Postcolonial Studies.” *The Journal of Commonwealth Literature* 34(1):199–200. doi: 10.1177/00219894990340011

Beutin, Lyndsey P. 2017. “Racialization as a Way of Seeing: The Limits of Counter-Surveillance and Police Reform.” *Surveillance & Society* 15(1):5–20. doi: 10.24908/ss.v15i1.5669.

Bevilacqua, Ivana. 2022. “E-Scaping Apartheid: Digital Ventures of Zionist Settler Colonialism.” *Human Geography* 15(2):220–28. doi: 10.1177/19427786211055780.

Bigo, Didier & Anastassia Tsoukala. 2008. *Terror, Insecurity and Liberty*. London, UK: Routledge.

Bradshaw, Paul. 2016. “Chilling Effect: Regional Journalists’ Source Protection and Information Security Practice in the Wake of the Snowden and RIPA Revelations.” *Digital Journalism* 5(3):334–52. doi: 10.1080/21670811.2016.1251329.

Caluya, Gilbert. 2010. “The Post-Panoptic Society? Reassessing Foucault in Surveillance Studies.” *Social Identities* 16(5):621–33. doi: 10.1080/13504630.2010.509565.

Christl, Wolfie. 2017. *How Companies Use Personal Data Against People*. Vienna, Austria: Cracked Labs.

Clarke, Roger. 1988. “Information Technology and Dataveillance.” *Communications of the ACM* 31(5):498–512. doi: 10.1145/42411.42413

Clarno, Andy. 2017. “Neoliberal Colonization in the West Bank.” *Social Problems* 65(3):323–41. doi: 10.1093/socpro/spw055.

Dandeker, Christopher. 1990. *Surveillance, Power, and Modernity: Bureaucracy and Discipline from 1700 to the Present Day*. St. Martin's Press.

Deleuze, Gilles and Guattari Félix. 1987. *A Thousand Plateaus*. London, England: Athlone.

Deleuze, Gilles. 1992. "Postscript on the Societies of Control." 59. doi: 10.4324/9781315242002.

Durkheim, Emile. 2013. *Le Suicide, Étude De Sociologie (éd. 1897)*. Paris, France: Hachette Livre.

Ellul, Jacques. 1967. *The Technological Society*. New York: Random House.

Elmer, Greg. 2003. "A Diagram of Panoptic Surveillance." *New Media & Society* 5(2):231–47. doi: 10.1177/1461444803005002005.

Feldman, Yotam. 2013. *The Lab*. Gum Films. (https://www.gumfilms.com/projects/lab).

Foster, John Bellamy and Robert W. McChesney. 2014. "Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age." *Monthly Review* 66(3):1–31. doi: 10.14452/MR-066-03-2014-07_1

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. New York, NY: Pantheon Books.

Franceschi-Bicchierai, Lorenzo. 2018. "Inside a Demo of NSO Group's Powerful IPhone Malware." *VICE*. (https://www.vice.com/en/article/qvakb3/inside-nso-group-spyware-demo).

Fuchs, Christian. 2013. "Political Economy and Surveillance Theory." *Critical Sociology* 39(5):671–87. doi: 10.1177/0896920511435710.

Galič, Maša, Tjerk Timan, and Bert-Jaap Koops. 2017. "Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation." *Philosophy & Technology* 30(1):9–37. doi: 10.1007/s13347-016-0219-1.

Gürses, Seda, Arun Kundnani, and Joris Van Hoboken. 2016. "Crypto and Empire: The Contradictions of Counter-Surveillance Advocacy." *Media, Culture & Society* 38(4):576–90. doi: 10.1177/0163443716643006.

Haggerty, Kevin D., and Richard V. Ericson. 2000. “The Surveillant Assemblage.” *The British Journal of Sociology* 51(4):605–22. doi: 10.1080/00071310020015280.

Henrichsen, Jennifer R., Michelle Betz, and Joanne M. Lisosky. 2015. *Building Digital Safety for Journalism: A Survey of Selected Issues*. Paris, France: United Nations Educational, Scientific and Cultural Organization.

Jansen, Sue Curry and Jefferson Pooley. 2021. “Blurring Genres and Violating Guild Norms: A Review of Reviews of the Age of Surveillance Capitalism.” *New Media & Society* 23(9):2839–51. doi: 10.1177/14614448211019021

Jay, Martin. 1993. *Downcast Eyes : The Denigration of Vision in Twentieth-Century French Thought*. Berkeley: University of California Press.

Kleberg, Carl Fridh. 2015. *The death of source protection? Protecting journalists' sources in a post-Snowden age*. London, UK: LSE Polis.

Kundnani, Arun. 2014. *The Muslims Are Coming! Islamophobia, Extremism, and the Domestic War on Terror*. London, UK: Verso.

Lashmar, Paul. 2016. “No More Sources?: The Impact of Snowden’s Revelations on Journalists and Their Confidential Sources.” *Journalism Practice* 11(6):665–88. doi: 10.1080/21670811.2017.1365616

Lyon, David. 1993. “An Electronic Panopticon?: A Sociological Critique of Surveillance Theory.” *The Sociological Review* 41(4). doi: 10.1111/j.1467-954X.1993.tb00896.x

Lyon, David. 2007. “Product Review: Sociological Perspectives and Surveillance Studies: ‘Slow Journalism’ and the Critique of Social Sorting.” *Contemporary Sociology: A Journal of Reviews* 36(2):107–11. doi: 10.1177/009430610603600202.

Lyon, David. 2001. “Surveillance after September 11.” *Sociological Research Online* 6(3):116–121. doi:10.5153/sro.643

Lyon, David, ed. 2006. *Theorizing Surveillance: The Panopticon and Beyond*. Cullompton, Devon: Willan Publishing.

Mann, Steve, Jason Nolan, and Barry Wellman. 2002. “Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments.” *Surveillance & Society* 1(3):331–55. doi: 10.24908/ss.v1i3.3344.

Marczak, Bill, John Scott-Railton, and Ron Deibert. 2018. “NSO Group Infrastructure Linked to Targeting of Amnesty International and Saudi Dissident.” *The Citizen Lab.* (https://citizenlab.ca/2018/07/nso-spyware-targeting-amnesty-international/)

Marczak, Bill, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert. 2020. “Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries.” *The Citizen Lab*. (https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/).

Marx, Karl, and Friedrich Engels. 1848. *The Communist Manifesto.* London, England: The Communist League.

Mazzetti, Mark, Ronen Bergman, and Matina Stevis-gridneff. 2022. “How the Global Spyware Industry Spiraled out of Control.” *The New York Times*. (https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html).

Mills, Anthony. 2019. “Now You See Me – Now You Don’t: Journalists’ Experiences with Surveillance.” *Journalism Practice* 13(6):690–707. doi: 10.1080/17512786.2018.1555006.

Monahan, Torin. 2006. “Counter-Surveillance as Political Intervention?” *Social Semiotics* 16(4):515–34. doi: 10.1080/10350330601019769.

Morozov, Evgeny. 2019. “Capitalism's New Clothes.” *The Baffler*. (https://thebaffler.com/latest/capitalisms-new-clothes-morozov).

Norris, Clive, and Dean Wilson. 2017. *Surveillance, Crime and Social Control*. 1st ed. edited by D. Wilson and C. Norris. London, England: Routledge.

Pegg, David and Sam Cutler. 2021. “What Is Pegasus Spyware and How Does It Hack Phones?” *The Guardian*. (https://www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones).

Penney, Jonathon W.; Schneier, Bruce; 2022. “Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group.” *Berkeley Technology Law Journal* 36(1). doi: 10.15779/Z384B2X554.

Posetti, Julie. 2017. *Protecting Journalism Sources in the Digital Age*. Paris, France: United Nations Educational, Scientific and Cultural Organization.

Reporters Without Borders. 2022. “World Press Freedom Index.” *Reporters Without Borders*. (https://rsf.org/en/index).

Rose, Nikolas. 1999. “Government and Control.” *The British Journal of Criminology* 40(2):321–39. doi: 10.1177/0952695109352415

Said, Edward W. 1978. *Orientalism*. London, UK: Penguin Books.

Sa’di, Ahmad H. 2021. “Israel’s Settler-Colonialism as a Global Security Paradigm.” *Race & Class* 63(2):21–37. doi: 10.1177/0306396821996231.

Salzmann, Anja, Frode Guribye, and Astrid Gynnild. 2021. “Mobile Journalists as Traceable Data Objects: Surveillance Capitalism and Responsible Innovation in Mobile Journalism.” *Media and Communication* 9(2):130–39. doi: 10.17645/mac.v9i2.3804.

Simmel, Georg. 1971. “The Metropolis and Mental Life.” Pp. 324 in *Georg Simmel on Individuality and Social Forms*, edited by Donald Levine. Chicago, IL: Chicago University Press.

Stein, Rebecca L. 2021. *Screen Shots: State Violence on Camera in Israel and Palestine*. Stanford, California: Stanford University Press.

Thorsen, Einar. 2019. “Surveillance of Journalists/Encryption Issues.” *The International Encyclopedia of Journalism Studies* 1–7. doi: 10.1002/9781118841570.iejs0272.

Van Dijck, José. 2014. “Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology.” *Surveillance & Society* 12(2):197–208. doi: 10.24908/ss.v12i2.4776

Waters, Stephenson. 2018. “The Effects of Mass Surveillance on Journalists’ Relations With Confidential Sources: A Constant Comparative Study.” *Digital Journalism* 6(10):1294–1313. doi: 10.1080/21670811.2017.1365616.

Weber, Max and Talcott Parsons. 1947. *The Theory of Social and Economic Organizations*. London, England: Hodge.

Wilson, Dean Jonathon, and Tanya Serisier. 2010. “Video Activism and the Ambiguities of Counter-Surveillance.” *Surveillance & Society* 8(2):166–80. doi: 10.24908/ss.v8i2.3484.

Zablah, Nelson Rauda. 2022. “Pegasus Spyware Was Used to Hack Reporters' Phones. I'm Suing Its Creators.” *The Guardian*. (https://www.theguardian.com/commentisfree/2022/dec/05/pegasus-spyware-journalists-phone-hacking-lawsuit).

Zuboff, Shoshana. 2020. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

Zureik, Elia, David Lyon, and Yasmeen Abu-Laban, eds. 2013. *Surveillance and Control in Israel/Palestine: Population, Territory and Power*. London, UK: Routledge.

Zureik, Elia. 2020. “Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel.” *Middle East Critique* 29(2):219–35. doi: 10.1080/19436149.2020.1732043.

Zureik, Elia. 2016. “Strategies of Surveillance.” *Jerusalem Quarterly* 66: 12-38.

Zureik, Elia, and David Lyon. 2022. “Coronavirus Surveillance and Palestinians.” *Jerusalem Quarterly* 89: 51-62.

Appendix A: Recruitment Letter

Hello,

My name is Leila Katibah and I am an undergraduate student in the Sociology Department of the University of California, Santa Barbara. I am currently researching the implications of surveillance and counter-surveillance on freedom and democracy in relation to Pegasus spyware attacks on journalists.

I am reaching out to you because I would like for you to join me for a 30 minute remote interview about your experiences as a journalist targeted by Pegasus spyware technologies.

If you are interested and available between the months of December 2022 - April 2023, please let me know what day and time you are available, and if you prefer to meet via phone or zoom, so I could follow up with further information

Thank you!

Leila Katibah
leilakatibah@ucsb.edu

Appendix B: Interview Guide

Interviews with journalists will be semi-structured, with the following questions serving as a guideline.

- Preliminary Questions
    - May I use your real name or would you prefer to be anonymous?
- Demographic Questions
    - What publication/organization do you currently work with?
- What kind of topics do you report on?
- How did you first suspect you were being surveilled using Pegasus?
    - What was your immediate reaction? (Did you report it, clean out devices, etc. What steps did you take in response?)
    - From what you know, what was found on your devices? Did you have your device analyzed?
    - What is the climate for journalists in relation to freedom of the press in your country? Were you afraid of being spied on? Was this something you ever anticipated?
    - Why do you think the government is interested in monitoring your work?
- How has Pegasus impacted your career, if at all? How has it impacted your safety and well-being?
- How has being surveilled changed your practices moving forward? (I.e. data storage and collection)
    - How do you continue reporting in spite of being surveilled by governments using Pegasus?
    - Has the news of this targeted spyware program affected your ability to reach sources? How has this affected the willingness of sources to be in contact with you?
- Do you feel that journalistic institutions have taken adequate measures to counteract this kind of illegal surveillance?
- Do you know other journalists also targeted by Pegasus spyware who would also be willing to share their contact information with me for a potential interview?