City Research Online

City St George's, University of London

Citation: Dan, K. & Carmi, E. (2024). Keeping Pegasus on the wing: legitimizing cyber espionage. Information, Communication and Society, 27(8), pp. 1499-1529. doi: 10.1080/1369118x.2023.2245873

This is the published version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/31171/

Link to published version: https://doi.org/10.1080/1369118x.2023.2245873

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

INFORMATION, COMMUNICATION & SOCIETY
https://doi.org/10.1080/1369118X.2023.2245873

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Keeping Pegasus on the wing: legitimizing cyber espionage

Dan M. Kotliar [a] and Elinor Carmi [b]

[a]University of Haifa, Haifa, Israel; [b]City University London, London, UK

ABSTRACT

NSO Group is an Israeli cyber surveillance firm notorious for Pegasus – an intrusive malware capable of covertly taking control of smartphones and remotely extracting their contents. In 2019, after a series of unflattering reports on governments' use of Pegasus to infiltrate the phones of activists and journalists, NSO embarked on an uncharacteristically public legitimation campaign. This article focuses on this campaign and explores how this otherwise secretive spyware company publicly legitimizes its surveillance. Based on an empirical analysis of hundreds of public documents across various media, we explore NSO's legitimacy management practices and identify the audiences and contexts of this legitimation. Our analysis identified four legitimation practices: securitization, Zionist patriotism, ethics washing, and normalization. We argue that these legitimation strategies operate across two interrelated axes of legitimation: a local axis that echoes a particularly Israeli 'security-driven populism'; and a universal axis that follows Silicon Valley's ethics washing. We show that these legitimation axes are designed to simultaneously ensure the company's survivability and to sustain surveillance realism – the perception of surveillance as the only viable option This article contributes to the emerging literature on cyber surveillance firms and to the burgeoning research on the legitimation of surveillance by shedding light on the discursive infrastructures behind contemporary cyber espionage. Moreover, while surveillance is often understood as a global phenomenon, this article highlights the need to focus on the local contexts from which surveillance originates to understand its sustainability, expansion, and vulnerabilities.

ARTICLE HISTORY
Received 29 November 2022
Accepted 30 June 2023

KEYWORDS
Surveillance; legitimation; NSO; Pegasus; spyware

Introduction

On 2 October 2018, Jamal Khashoggi, a Saudi dissident and columnist for The Washington Post, entered the Saudi consulate in Istanbul, where he was brutally assassinated by agents of the Saudi government. The assassination made headlines worldwide, and shortly thereafter, an Israeli spyware company was said to have been involved – the

CONTACT Dan M. Kotliar dkotliar@soc.haifa.ac.il University of Haifa, 199 Abba Khoushy Ave., Mount Carmel, Haifa 3103301, Israel

© 2023 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (http://creativecommons.org/licenses/by-nc-nd/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

NSO Group.[1] Founded in 2010 by Israeli entrepreneurs Niv Carmi, Shalev Hulio, and Omri Lavie, NSO licenses its surveillance products to intelligence and law enforcement agencies worldwide. It is primarily known for Pegasus – an intrusive malware capable of covertly taking control over smartphones and remotely extracting their contents.

By no means was this the first scandal NSO faced. Nor was it the first time that NSO's cyber-surveillance methods were publicly revealed. Pegasus was first described by Israeli journalists in 2012 (Aspril, 2012); the first detailed report on NSO's malware was published by the University of Toronto's Citizen Lab in 2016 (Marczak & Scott-Railton, 2016), and in the two years predating Khashoggi's murder, a series of unflattering media reports repeatedly chronicled how governments use Pegasus to infiltrate the phones of activists and journalists and to effectively squash opposition. Nevertheless, Khashoggi's assassination seems to have signaled a sea change for the company. Soon thereafter, NSO stepped out of the shadows and initiated an orchestrated campaign to legitimize its activities, thus replacing years of silence with loud and public legitimation.

This article focuses on NSO's legitimation campaign and explores how this otherwise secretive spyware company publicly legitimizes its work. Based on a critical analysis of hundreds of public documents in Hebrew and English, we identify NSO's key legitimacy management practices (Suchman, 1995): securitization discourse, Zionist patriotism, ethics washing, and normalization. We argue that these legitimation strategies operate across two interrelated axes of legitimation: a local axis that echoes a particularly Israeli 'security-driven populism' (Levi & Agmon, 2021); and a universal one that follows Silicon Valley's path of ethics washing. We show that these axes of legitimation are designed to ensure the company's survivability and to, more generally, sustain surveillance realism – the perception of surveillance as the only viable option (Dencik & Cable, 2017).

While surveillance's role in contemporary life received considerable attention, only a handful of scholars empirically engaged with cyber surveillance (Iliadis & Acker, 2022; Knight & Gekker, 2020), and cyber-espionage firms like NSO were largely overlooked. Moreover, while the legitimation of surveillance has been discussed in multiple contexts (Lischka, 2017; Marciano, 2019; Schulze, 2015; Wahl-Jorgensen et al., 2017), this line of research primarily focuses on legitimation by the press. This article contributes to these lines of research by drawing attention to how cyber-espionage firms actively legitimize their work, and by shedding light on the discursive infrastructure of contemporary surveillance.

Literature review

Surveillance realism

Surveillance has been used since the dawn of ages, but in the last century, it has become an integral part of everyday life (Andrejevic, 2007; Ball et al., 2012). Accordingly, in the last decade, particularly following the 2013 Edward Snowden revelations of massive data collection by the US and its allies, people have become more aware of the scale of surveillance and its implications. Nevertheless, rather than protesting surveillance, people are becoming engulfed in what Dencik and Cable describe as *surveillance realism* – a 'perception of surveillance as the only viable option, despite widespread recognition of its fallacies and injustices' (Dencik & Cable, 2017, p. 20). As a result, people may desire to control their online data but feel unable to do so (Draper & Turow, 2019), and even

when they explicitly weigh the benefits and disadvantages of data extraction, they tend to see surveillance as a default setting they cannot change (Marwick & Hargittai, 2019). Nevertheless, this default is far from natural – it is actively manufactured and cultivated by actors using various means and practices. After all, companies and governments benefit from people's digital resignation and actively vest interest in producing it (Dencik, 2018; Draper & Turow, 2019). Hence, surveillance advocates aim to naturalize, neutralize, and legitimize their surveillance, presenting it as a 'mandatory price to pay' for their services.[2]

Legitimacy

Legitimacy is defined as a 'generalized perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions' (Suchman, 1995, p. 574). As Max Weber has famously shown, legitimation transforms power relations into authority, as people orient toward a social order that is consonant with the rules, norms, or beliefs they see as accepted by others (Weber, 1978). While some see legitimacy as a property or capacity of an entity (Suchman, 1995), and others highlight socio-cognitive aspects of legitimacy – namely, how it is perceived and evaluated by actors (Tost, 2011) – this article focuses on processes of legitimation. Legitimation theory sees legitimacy as a social process and explores how it is socially constructed through various relationships (Suddaby et al., 2017). Focusing on legitimation highlights the dynamic nature of legitimacy and the ways social actors continuously evaluate and negotiate the appropriateness of social entities (Hoefer & Green, 2016).

Legitimating surveillance

While surveillance tends to occur far from the public's eye, it is often publicly legitimized following scandals (Schulze, 2015). Notably, the 2013 Snowden revelations of the scale and scope of government surveillance have spurred much scholarly interest, predominantly focusing on legitimation by mass media. For example, focusing on UK news coverage of the Snowden revelations, Wahl-Jorgensen and colleagues have shown that newspapers tend to legitimize surveillance by highlighting national security concerns (Wahl-Jorgensen et al., 2017). Lischka (2017) similarly described how British broadcast news justifies governmental tracking using detailed terror threats. Kuehn (2018) has highlighted New Zealand's newspapers' tendency to frame mass surveillance as a political issue rather than a civic one, and Mols and Janssen (2017) have shown how Dutch discussions about the Snowden revelations displayed a tradeoff narrative that balances safety against privacy. Focusing on the creation of a national biometric database, Marciano (2019) has similarly shown how Israeli newspapers legitimize biometric surveillance by depicting it as an essential mechanism against external threats.

Legitimacy can also be promoted by those in power. Schulze, for example, argues that scandals force politicians to actively legitimize surveillance to prevent the loss of legitimacy, power, and privileges (Schulze, 2015, p. 198). Tréguer (2017) has highlighted the legalization strategies pursued by liberal states to expand domestic and foreign surveillance. Others have described how companies turn to strategies of obfuscation, such as 'dark patterns' or complex privacy policies and terms of service (Acquisti et al., 2015) to

cultivate user resignation regarding surveillance (Draper & Turow, 2019) and make privacy violations seem inevitable (Marwick & Hargittai, 2019), and how companies employ lobbyists to legislatively cement their data collection practices (Carmi, 2020).

Thus, in the last decade, research has highlighted how two impactful institutions – mass media and politicians – legitimize mass surveillance and how technology companies design their products to normalize and legitimize their intrusive practices. Nevertheless, the ways surveillance firms actively and publicly legitimize their tracking received less scholarly attention. Moreover, works on the legitimation of surveillance, like works on surveillance in general, overwhelmingly focus on governments and corporations' mass surveillance that routinely extract and mine the data of millions of citizens, noncitizens (Madianou, 2019), and 'users' worldwide. However, cyber-espionage companies like NSO operate differently. First, like other cyber surveillance companies (Iliadis & Acker, 2022; Knight & Gekker, 2020), but in opposition to most Silicon Valley corporations, NSO explicitly sells surveillance technologies. The intrusive affordances of their products are not parts of other, allegedly benign products (like social networks, search engines, or cars (Gekker & Hind, 2019)) - they are the product. NSO commodifies, markets, and sells the ability to tap into people's phones and download its content. Moreover, unlike most surveillance capitalists (Zuboff, 2019), but like some governmental bodies, NSO's products target specific individuals. These are not extensive dataveillance (van Dijk, 2014) platforms designed to manage populations or profile and affect people with ads, misinformation, or radicalizing content, but a way to extract data about specific individuals that may lead to their investigation, arrest, harassment, or worse. Accordingly, NSO's Pegasus was reportedly leased by only a few dozen customers and used on no more than a few hundred 'targets.' In other words, companies like NSO operate differently than other surveillance-based corporations, but they unquestionably play a role in today's global surveillance regime.

Accordingly, as will be shown below, it is not merely user resignation (Draper and Turow, 2019) that NSO seeks to promote. They also seek approval and complicity from politicians and regulators in Israel and abroad, the sympathy of current and future employees, their investors' loyalty, and their potential customers' acceptance. Hence, as we argue below, the sustainment of surveillance realism depends on diverse-but-interdependent factors and on simultaneously sustaining companies' dyadic ties (Schoon, 2022) with various stakeholders.

Hence, following NSO's public narrative across multiple media, we focus on their 'legitimacy management practices' (Suchman, 1995), namely, the discourses, narratives, and ideologies by which they legitimize their surveillance. We highlight the particular contexts from which such legitimation practices stem and show how these rhetorics aim to ensure the continuation and expansion of their surveillance, and the sustainment of surveillance realism. We ask: How does NSO legitimize its activities? Who are their intended audiences? What are the social contexts their strategies correspond to? And how do they aim to sustain surveillance realism? The paper unfolds as follows: We begin by discussing NSO's origin story and two foundational legitimating strategies that stem from it: the privacy/security tradeoff and the company's securitization discourse. We then turn to discuss NSO's patriotic legitimation. In the third section, we focus on NSO's use of regulatory and ethics mechanisms to legitimize their work, and then we shed light on the company's normalization tactics. Finally, we discuss the ties between NSO's legitimation and two dominant socio-political trends – right-wing

populism and silicon valley's ethics washing, and the role that discourse plays in sustaining surveillance realism.

Methods

This article is based on a Critical Discourse Analysis (CDA) (Wodak, 2014) of NSO's legitimation campaign. CDA aims to demystify 'ideologies and power through the systematic and retroductable investigation of semiotic data (written, spoken, or visual)' (Wodak, 2014, p. 303). Because this article focuses on the active legitimation of surveillance, and because legitimation revolves around exerting and transforming power (Weber, 1978), CDA's focus on how discourses reproduce power offers a good methodological fit. Hence, we compiled a comprehensive corpus of NSO's public utterances in multiple media outlets in English and Hebrew for 30 months: from the campaign's inception in January 2019 until its end in July 2022. The corpus contains 293 documents including NSO's media engagements (executives' interviews, talks at conferences, op-eds, and statements) (n = 44); NSO's social media posts (on LinkedIn and Medium) (n = 200), website entries (n = 30), reports (n = 3), and legal documents (n = 16). We also conducted an analysis of their website based on The Internet Archive Way Back Machine (Ben-David & Amram, 2018) and the Who Is documentation of their domain (www.nsogroup.com).

The authors and research assistant collected the data by repeatedly searching for NSO interviews, statements or reports on Google and MS Bing from multiple IP addresses. We also set up Google alerts with the names of the company's executives and visited their website and social media pages once a week to extract data. The inclusion criteria were direct utterances by the company, its executives, or its workers. Our research assistant transcribed TV, radio, and podcast interviews.

The data was logged into MaxQDA22 and were first analyzed by the authors using thematic analysis (Braun & Clarke, 2006). We read and reread the data to identify recurring themes, each corresponding to a different legitimacy practice (Suchman, 1995), and coded the texts using these themes. The analysis identified six themes (including technological determinism and deflection of responsibility, which appeared less frequently and proved less dominant than the other themes). Hence, for the purpose of this paper, we focus on the four most dominant themes. Following the initial coding, we selected and translated prominent quotes representative of each theme and analyzed them using critical discourse analysis (Wodak, 2014). Alongside the qualitative analysis, we also provide descriptive statistics, pointing to the frequency of the legitimation strategies across the data. References to the items mentioned in the analysis consist of the items' ordinal number, source type (IM – International media, ISM – Israeli media, LI – LinkedIn, M – Medium posts, W – NSO's website, L – legal documents, R – reports), and year. For example, 1IM16 refers to the first item in the appendix, a 2016 international media piece. The table in appendix 1 provides additional details about the items.[3]

Findings

Legitimation through securitization in NSO's origin story

NSO originated from Omri Lavie and Shalev Hulio's previous company – CommuniTake, which offered tech-support workers the ability to remotely take over and repair

customers' cellphones. According to NSO's origin story, recounted by its founders multiple times[4], a European intelligence agency found out about CommuniTake, contacted its founders, and implored them to offer a similar product that would operate without users' knowledge or consent. As Hulio recounted in an interview:

> The truth is that we didn't quite understand what they [the intelligence agency] wanted. So, we said: 'but what is your problem with gathering intelligence?' you're sitting inside the phone carrier. They said we didn't really understand and that the situation was grave. 'We are going dark. We are getting blind!' were the exact words they used. 'Help us.'[…] At the time, we knew nothing about this world […] And then the police forces and Europe's intelligence agencies told us: 'With the technology you developed, you could help us solve this problem.' So, us being Israelis and hearing we had a technology that could save lives, we immediately said: 'Tell us what you need, we'll do it (15ISM19).

Hulio's words clarify the role NSO's origin story plays in the company's raison d'être, encapsulating some of the basic legitimation strategies employed by the company. First, Hulio highlights the founders' alleged naivete as the intelligence agency approached them and explains that the idea for their intrusive product came from a legitimate actor - an intelligence officer; from a legitimate and benevolent region– Europe; and that this European agent pleaded for the Israeli entrepreneurs' help. Thus, NSO's surveillance is legitimized by association with other legitimate actors and by answering to their 'objective' security needs. Hulio dramatically describes these needs as 'darkness' or 'blindness' that have fallen upon these agencies with the widespread adoption of mobile phones and the decision to establish NSO as an act of chivalry that stems from his national identity, thus preventing these agencies' critical myopia. He further explained:

> In 2007, the first iPhone broke into our lives. It came with a set of encryption capabilities that were previously unavailable to ordinary citizens. So, [for example,] if you are now plotting a robbery, murder, acts of pedophilia or rape over a social network or an instant messaging app, the police, the Shin Bet, or any other law enforcement [agency] has no way of gathering intelligence about you and prevent this crime using previously used methods (15ISM19).

In this, and many similar NSO texts[5], the recent proliferation of encrypted communication is depicted as a dangerous and problematic turn for law enforcement agencies, as it allegedly leaves them severely handicapped. Encrypted technologies might offer customers more privacy, but as NSO executives repeatedly explain, there is a dangerous tradeoff between privacy and security (Mols & Janssen, 2017), as law enforcement can no longer surveil their targets. Thus, through its origin story, NSO's surveillance is constructed as a legitimate, even necessary assistance to law enforcement agencies that would help them reinstate the social order allegedly lost to encryption.

The privacy/security trope is closely tied to the company's central and most salient legitimation strategy –securitization. Hulio's provocative warnings against murderers, rapists, and pedophiles' use of encrypted media is an example of a discourse that repeats in 59% of the company's media engagements (26/44 documents).[6] In fact, most of their interviews begin with a mention of the security threats NSO's surveillance allegedly protects from[7], and such threats are also included in the company's most basic descriptions. For example, on the main page of NSO's website, a headline reads:

> NSO creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe.

NSO's executives similarly take pride in specific cases where their surveillance allegedly helped law enforcement prevent crime – like the capture of the Colombian drug baron 'El Chapo' (21ISM20) or help with fighting ISIS (28ISM21) – and they more generally highlight Pegasus' contribution to citizens' security. As Hulio stated in an interview:

> In just the last six months, the company's products were part of operations to thwart several very large terrorist attacks in Europe, both by car bombs and suicide bombers. So, I will modestly say that thousands of people in Europe owe their lives to the hundreds of employees of our Herzliya company (2IM19).

As Stritzel argued (2007), the construction of threats to national security aims to persuade an audience to 'tolerate violations of rules that would otherwise have been obeyed' (Stritzel, 2007, p. 361). In this case, NSO's penetrative surveillance is depicted as a legitimate, even necessary transgression of the rule due to the dangers posed by global terrorist networks. While this quote offers a global narrative with an almost universal logic, it is also specifically aimed at an Israeli audience. After all, Israel's tradition of securitization entwined with militarization (Ben-Eliezer, 1998; Kimmerling, 1993) and its longstanding preoccupation with terrorism, make Israelis inclined to accept almost any solution to such problems, as invasive as it may seem. Moreover, constructing these problems as 'European' paints a simplified, almost binary version of this story and neatly separates the in-group from the outgroup – signaling that these questionable tools are only used to help 'people like us.' It is a type of 'legitimacy through altruism' (Reyes, 2011, p. 787)– where surveillance is presented as beneficial for the in-group.[8]

While NSO's securitization discourses primarily offer pragmatic legitimation (Suchman, 1995, p. 9) that rationally explains the necessity of their product, they also include more emotionally-evocative ones. As Shiri Dolev, NSO's president, said in an interview:

> One client came to thank us for a kidnapped child who was safely returned home. Pedophilia cases like these are closest to my heart, and you cannot solve them without systems like ours because all the pedophiles are hiding behind encrypted walls (18ISM19).

Dolev adds an emotional tone to the security narratives seen above, as her narrative aims to evoke moral outrage from her audience that would legitimize NSO's product and outweigh the recurrent reports about its misuse.

Thus, NSO legitimizes its surveillance by highlighting the pragmatic and emotional needs for its encryption-breaking technology and its alleged exceptional capacity to protect an imagined benevolent collective against security threats. As we will show below, these legitimating strategies strongly resonate with contemporary Israeli security-driven populism (Brubaker, 2017; Levi & Agmon, 2021). In line with these trends, NSO also offers much more direct appeals to Israeli audiences by highlighting its belief in and exercise of Israel's core national values.

Patriotic legitimation: aligning with the norms of the nation

As legitimation scholars have shown, legitimacy is achieved when the object of legitimacy is 'culturally aligned' with audiences' expectations (Suchman, 1995). We thus first

examine how NSO explicitly constructs its identity as a Zionist company before focusing on its legitimation practices that center around three dominant Israeli cultural tropes: Holocaust remembrance, nation-building, and victimization.

In April 2021, NSO sponsored and co-organized the 'Blue and White Convention' with Calcalist, a daily business newspaper, for Israel's Independence Day. With a program appropriately decorated in the national colors, the convention revolved around the Israeli high-tech industry, including panels with prominent Israeli techies and two sympathizing interviews with NSO's Shalev Hulio (24ISM21) and Shiri Dolev (25ISM21). On the morning of the convention, Calcalist also published an op-ed by Ramon Eshkar, NSO's VP Client Executives. He wrote:

> In this op-ed, I will share with you […] how strong and pronounced the connection between such a week [that includes Israel's Memorial Day and Independence Day] and NSO is, and how deeply relevant are concepts such as Zionism, Israeliness, and values to everything that NSO does (23ISM21).

Eshkar later promises to discuss the 'very big things' NSO does. However, instead of focusing on cyber-surveillance, he describes the volunteering work that NSO employees do ('including the CEO') and, particularly, how they join search and rescue operations worldwide after major natural disasters like earthquakes or floods. He explains that: '[it is done] with no questions asked and no cost check, simply to help save lives. Because we are Israelis, and for us, values are more than just words. They are actions' (23ISM21).

Eshkar explicitly highlights the company's alleged Zionist and Israeli 'character' by tying the company to two of Israel's most revered national holidays – Independence Day and Memorial Day. Completely evading the company's main product and intrusive surveillance, he exemplifies its 'innate' Israeli values by highlighting its altruistic search and rescue missions. According to other publications, these missions stemmed from Shalev Hulio's personal military experience as an IDF search and rescue officer, and they more generally point to the deep ties between the Israeli army and its high-tech industry. Nevertheless, instead of describing this activity as his boss's altruistic hobby, Eshkar frames it as an attestation of the company's core values and its tendency to 'save lives.' This message echoes NSO's security discourse, as seen in the previous section, but here it is described as a broader, 'innately Israeli tendency' that aligns with the company's alleged identity and values. Eshkar thus signals to his Israeli readers that the company is one of their own.

NSO's patriotic legitimation also included more specific tactics. For example, on International Holocaust Remembrance Day, January 2021, NSO posted an emotional LinkedIn post. They wrote:

> During 2019, NSO Group, as a proud Israeli and Zionist company, sent six groups of 170 employees to Poland to experience the stories of those who perished and learn about the horrific crimes committed against humanity (164LI21).

In line with the previous quotes, here NSO explicitly describes itself as 'Israeli and Zionist,' and it accordingly constructs its national identity by tapping into one of Israel's most sacred national tropes – the Holocaust. As Feldman (2008) noted, organized voyages to Poland are a central way of performing the Israeli national identity. While such voyages are predominantly done in high school (ibid), NSO publicly exhibits its

employees' trips to the former sites of Nazi extermination camps as participation in an Israeli initiation ceremony that attests to the true Israeliness of their company. Moreover, while the previous section described specific security threats, here NSO contrasts its identity with much more existential threats, which hold an almost mythical significance for their Israeli audiences. Accordingly, they present their actions (and more generally, cyber-surveillance) as pertaining to a deeper moralistic pursuit. This discursive strategy mirrors Israeli right-wing politicians' discourses, particularly Netanyahu's long-time use of the Holocaust to foster existential panic in Israel for their political gain (Leslie, 2017, p. 78). That is, NSO echoes contemporary populist discourses that promise to protect an imagined bounded collectivity against external or internal, real or imagined threats (Brubaker, 2017, p. 363).

NSO similarly highlights its role in nation-building. In December 2020, the company announced opening a second branch in Israel's southeastern periphery – the arid Arava region, not far from the Jordanian border. In a press release, NSO promised to supply 100 jobs to this peripheral region and educational programs for local high schoolers, in which 'NSO experts' would teach them the 'cyber and technology professions.' With this move, NSO alludes to the Zionist myth of nation-building through expansion into the periphery and, specifically, into sparsely populated borderlands, 'making the desert bloom.' As Hulio wrote: 'We are not doing it to get PR […] we do it out of Zionism. (22ISM21).'

In his 2021 op-ed, Eshkar, NSO's VP, similarly wrote:

> What company decides to bring high-tech and equal employment opportunities to the farthest place in the country without asking 'how much does it cost?' or 'why do such a thing?' After all, this is not a [promising] economic course of action […]. The answer is – [we do it] because it is the right thing to do, because it is the Zionist thing to do, and because it is precisely what sets us apart as a company (24ISM21).

Eshkar ensures the symbolic significance of this legitimation practice will not go unnoticed and, once again, signals to the Israeli public and its legislators that the company is an altruistic entity that acts according to national interests and in light of its allegedly inherent national values. Here too, the company's technology and its economic activities are discursively sidelined in favor of NSO's alleged patriotism, and its surveillance is removed from this narrative altogether. Hence, this is an attempt to tap into yet another central Israeli founding myth and discursively place the company alongside the country's mythological founders in their attempts to expand, strengthen, and protect the homeland.

The last Zionist trope NSO turns to is that of victimization. Namely, describing the accusations against the company as an organized, anti-Israeli, or even antisemitic plot. For example, responding to the Forbidden Stories' revelation of a list of 50,000 phone numbers of alleged NSO targets, Hulio said**:**

> Hulio: It seems like someone decided to target us directly. This is not a coincidence. There is a threat to Israeli cyber [companies] in general. There are so many cyber intelligence companies worldwide, but they only focus on Israelis. […] It seems like it is deliberately done.
>
> Interviewer: By whom?
>
> Hulio: I believe that, in the end, it is either Qatar or BDS or both. […] If we were operating in the US or the UK, this story would not have happened. A large part of what we endure stems from the fact that we are Israelis (28ISM21).

Hulio suggests that the criticism against NSO stems from their national identity, not their intrusive surveillance. According to this narrative, it is Israel's so-called enemies (Qatar) and fierce political opponents (the pro-Palestinian Boycott, Divestment, and Sanctions movement) who target the company. This narrative aims to make clear that NSO is deeply Israeli – in its virtues and adversities. It also signals that NSO and its (Israeli) audiences share the threat of these adversities due to their shared national identity. Here too, in line with a populist line of thought and with Netanyahu's populist style (Leslie, 2017), NSO identifies its idiosyncratic challenges with threats to the imagined collective, demonstrating that they are deeply intertwined with it.

Hence, NSO's patriotic legitimacy highlights the company's alleged material and ideological contribution to the state, with explicitly Zionist symbolism. It is a response to the company's scandals that highlights its patriotism, national values, and intrinsic ties to Israel's national myths and grand narratives. Nevertheless, ironically, most of NSO's shares are in the hands of foreign venture capital funds, some of NSO workers reportedly work outside Israel, and most of NSO's clients are foreign governments. Nevertheless, this legitimation strategy is essential to secure NSO's survivability. After all, as will be detailed below, NSO depends on the Israeli Defense Ministry to authorize its operations, and it essentially trades in privatized intelligence services. Hence, this patriotic legitimacy signals to the Israeli public, legislators, and jurors that NSO's contribution to the state is more than financial, but it offers much deeper virtues – ones that have to do with the company's national identity and shared values.

Ethics washing

Beyond securitization and overt patriotism, NSO's legitimation campaign also operates on a more universal axis, highlighting the company's adherence to regulation, internal ethics, and allegedly unparalleled transparency.[9]

First, NSO often highlights its adherence to Israeli regulation. As a (cyber) weapons exporter, the company is subject to DECA – Israel's Defense Export Control Agency, which has oversight over their contacts and deals with their customers, as well as the power to revoke their export license and effectively terminate their activities. As part of the company's origin story, NSO's founders actively requested to be regulated by DECA from day one. As Hulio recounted in an interview:

> We want[ed] our technology to be regulated by Israel's Ministry of Defense. This meant that every sale would be under regulatory supervision. It may seem trivial today, because there is much talk around this issue, but when we founded the company in 2010, we were the first cyber-intelligence company in the world that actually demanded to be supervised (22ISM21).

Hulio explains that regulating surveillance is not only desirable in NSO's eyes, but it is something they take pride in. By highlighting their adherence to Israeli regulation, NSO allegedly delegates its responsibility to official government regulators – it is they who oversee and authorize NSO's deals, and who accordingly legitimize those deals by virtue of their official positions. This coincides with the company's ongoing attempts to closely associate itself with governments, particularly with the Israeli one.

NSO also highlights its reliance on international codes of practice. For example, in September 2019, NSO announced it had developed a Human Rights Policy 'that will

bring the company into alignment with the UN Guiding Principles on Business and Human Rights.' Here too, NSO prides itself on being 'the first company in the global cyber technology and defense sectors to seek alignment with the [UN's] Guiding Principles, cementing the company's existing industry-leading ethical business practices' (292R19). In the policy, NSO affirms its 'unequivocal respect for human rights,' their compliance with 'all laws applicable to [their] business,' they promise to integrate their 'human rights due diligence procedures' into their business plan, and more.

NSO also allegedly appointed a Governance, Risk, and Compliance Committee to oversee the implementation of the policy by conducting an 'internal risk assessment' of product sales with their potential human rights impacts in mind. Like the external DECA regulator, this committee was allegedly authorized to reject sales or request an investigation into misuse of the products. NSO also published a Whistle Blower Policy that covers 'all employees, contractors, partners, officers, and directors of the NSO Group' (291R19).

As legitimation researchers have shown, organizations often respond to normative pressures by adhering to standards and norms set by external actors (such as professional organizations, trade associations, or regulators) (Suddaby et al., 2017, p. 19). By creating an in-house regulatory mechanism and by publicly adopting the UN's Human Rights discourse, NSO aims to performatively adhere to such standards, achieve 'regulative legitimacy' (Johnson et al., 2006, p. 59) and appease its critics with an image of a law-abiding company.

Alongside external and internal regulation, NSO also highlights its transparency. As Hulio provocatively said in a podcast interview:

> How many cyber companies would agree to sit down and speak with you freely and transparently in a podcast? I believe I'm the only one. And the reason we are getting all the heat is that we want to be transparent (36ISM22).

As Hulio's words remind us, NSO's entire campaign is based on the tension between its inherent secrecy as a cyber-espionage firm and its unconventionally public acts of transparency. In this and in similar utterances[10], NSO treats the mere fact that their campaign is uncharacteristically public as an indication of its legitimizing potential. In this quote, Hulio highlights the singularity of his company's exposure compared to other surveillance firms and ironically argues that NSO's openness is the reason for their scandals, not the other way around.

NSO's transparency was accordingly formalized in June 2021 with the publication of its Transparency and Responsibility Report. As Hulio wrote in the opening paragraph:

> [W]e very much see today's release as a newly added necessity to the complex, ongoing international debate over electronic surveillance. We are opening our processes to even deeper scrutiny in an effort to inspire our peers while also opening new avenues of interaction with our fiercest critics (293R21).

This is one of the rare occasions whereby NSO explicitly mentions the term surveillance. By that, they seem to highlight the allegedly candid and genuine way they approach the subject of transparency. Like their legitimation campaign in general, NSO uses this report to capitalize on its alleged transparency: operating in a highly secretive field, they laud themselves for publicly discussing their affairs and inviting external actors to scrutinize

their actions even further. That is, transparency is primarily seen as an opportunity for the company to reject its image of secrecy and subterfuge and highlight its unique agreeableness compared to its competitors.

In the transparency report itself, NSO similarly writes that they 'will engage in good faith with any credible independent expert, including human rights defenders and others from civil society organizations […]' but do not mention which ones, what these engagements entail, and how NSO takes them into consideration. Hence, the transparency NSO takes pride in is conveniently accompanied by concealment and obfuscation – their numerous interviews and lengthy reports never reveal the identities of their collaborators or customers, nor the exact affordances and limitations of their product.

Moreover, with their Transparency and Responsibility Report, NSO follows Silicon Valley's tech giants in their so-called 'ethics washing' (Wagner, 2018). Such corporations have recently highlighted their self-regulation mechanisms (for example, Facebook's Oversight Board, Google's Ethical AI team, or the plethora of corporate-based AI ethics guidelines) to make external regulations redundant. Similarly, NSO aims to legitimize its actions by highlighting its proficiency in contemporary tech ethics discourses and willingness to collaborate with external auditors (Haupt, 2021), and it also follows the footsteps of Silicon Valley tech giants by turning its CEO into a public figure (Creech & Maddox, 2022). However, by omitting crucial details from this report, their actions remain conveniently (and ironically) opaque. After all, companies' 'transparency initiatives' often stem from public relations efforts (Crain, 2018), and transparency alone cannot create accountable systems (Ananny & Crawford, 2018). In the case of NSO, transparency seems like its means of gaining legitimacy, not an end in itself.

NSO also signals that its ethics have much deeper organizational roots by performing its 'day-to-day ethics' on LinkedIn. For example, they post about their employees volunteering with at-risk youth (177LI21), their activities for 'the International Day for the Elimination of Violence against Women' (150LI20), their NSO-branded truck-full of donated food for the 'less fortunate' (148LI20), or by publicly marking Earth Day (186LI21), World Autism Day (179LI21), or Good Deeds Day (238LI22). These posts are solely in English, and they signal that NSO's ethics are not only formalized but are also inherent to this company's organizational structure. In other words, these online performances add a normative legitimacy to their regulatory one (Johnson et al., 2006, p. 59), and it is also part of NSO's efforts of normalization, as will be discussed below.

'NSO is a technology company' – legitimation by normalization

In January 2022, NSO posted a series of LinkedIn posts, each busting an alleged myth about the company (248-254LI22). The last post read as follows:

> ✕#Fiction: Pegasus is called Pegasus because it acts like a war horse
>
> ✓#Fact: NSO Group's employees came up with this name because they wanted to be a unicorn … one day! (248LI22)

This short and playful post offers a reinterpretation of the etymology behind NSO's notorious product. While the name of the mythical winged horse invokes the idea of other mythical horses, specifically Trojan ones, this post tries to make clear that there

is nothing belligerent about this product (and, by extension, this company). Naming their main product after a winged horse merely signifies that, like any start-up, NSO's employees dream of it becoming a 'unicorn' – a company valued at over US$1 billion. Mythical or not, Pegasus never had a horn, but describing it as such, presents NSO as a typically ambitious company whose employees predictably fantasize about financial prosperity. This etymological tale elucidates one of NSO's key legitimating strategies– normalization. As we will demonstrate below, NSO uses various discursive strategies, predominantly on social media, to create a self-image of an ordinary, universally generic tech company, far removed from the image of a secretive and malevolent cyber-espionage firm.[11] As Hulio said in an interview:

> It's not that we are an intelligence company as you often read in the papers. Absolutely not. We are a company that produces technology, we give this technology to law enforcement agencies that use these technologies to catch pedophiles and criminals (29ISM21).[12]

Using the term 'technology' three times in one sentence, Hulio explains that in stark contrast to NSO's public image, his company is merely a technological one, and it is only responsible for the production of its products, not for how they are used. This argument mirrors gun advocates' arguments that focus on the ones who pull the trigger rather than the ones who manufacture the weapons. Hence, Hulio attempts to shake off the dark connotations of cyber surveillance and depict this company as just another standard tech company.

NSO's normalization strategy was particularly salient in NSO's social media posts. While NSO's competitors rarely have active social media accounts, NSO uses its LinkedIn page to publicly perform its normalcy. NSO's LinkedIn posts are strictly in English, and they often include hiring opportunities (197-198LI21, 225LI22), holiday greetings (155LI20, 235LI22, 256LI22) or pictures of their employees at conferences (222LI22, 236LI22). The posts also include pictures of company parties (170LI19, 187LI21, 190LI21), workshops and hackathons (156LI20), or other special events (pride-colored ice cream for Pride Day [212LI21] or pies for Pi Day [241LI22]), posts about remote work during the COVID-19 lockdowns (89LI20, 93LI20), and more). Such posts not only signal to potential employees that NSO is an attractive employer but also signal to wider audiences that it is, in fact, just as normal and just as legitimate as any other tech company.

NSO's normalization attempts also included the diversification of their line of products. For example, in February 2020, the company announced the acquisition of Convexum, an anti-drone start-up, and in June of the same year they launched it as their drone defense system – Eclipse. While NSO rarely mentioned Pegasus on its LinkedIn page, Eclipse was continuously featured there, as the company dedicated almost 20% of its 2020 posts to this new product (for example, 200LI21, 213LI21, 111LI20). The company also posted video demonstrations of Eclipse, invited media outlets to cover it, and incidentally positioned the new system in the background of some of their executives' TV interviews (25ISM21). This new product offered NSO a crucial addition – unlike Pegasus, it can easily be construed as a non-intrusive, purely defensive technology.

Similarly, in the last years, NSO attempted to add various products to their portfolio, including a COVID-19 contact-tracing app (Yadlin & Marciano, 2022) (97-98LI20, 101-103LI20, 274W20) and a data analytics tool that allegedly turns 'every life pattern into a

mathematical vector' (12IM22). The logic behind this diversification is evident in how the company described itself in a 2021 report:

> NSO is a technology company with a range of products, including those designed to augment data analytics capabilities by law enforcement and intelligence agencies, improve search and rescue efforts, [and] implement effective counter-measures against incursions by drones (293R21).

Thus, NSO attempts to promote a public image of itself as a flexible 'technology company' with a diverse portfolio whose sum is much larger than that of its most notorious part – Pegasus. According to this self-description, the basic denominator of NSO's products is not surveillance but security and safety, and this benevolent aim is achieved in various, mostly non-invasive ways.

NSO also distances itself from the image of a secretive surveillance firm by humanizing and deanonymizing its employees. For example, in a series of LinkedIn posts, NSO presented 'employee stories' – pictures of individual employees, with their full names, roles at the company, the time they have worked at NSO, and their quotes (90LI20, 106LI20, 109LI20, 116LI20, 118LI20). In 2021, NSO similarly ran a social media campaign under the hashtag #IAMNSO, in which employees took pictures of themselves and their families wearing NSO T-shirts and posted them to social media sites with the appropriate hashtag (206-207LI21 and on employees' private profiles). This campaign was a direct response to one of NSO's most serious scandals – the Forbidden Stories revelations, and it seemed to have aimed to humanize the company, give its employees concrete faces, and show that they are not a shadowy, secretive firm, they are just normal techies.

Discussion

This article exposed how the NSO Group legitimizes its surveillance by analyzing this cyber-espionage company's public utterances across media. We asked: How does NSO legitimize its activities? Who are their intended audiences? What are the social contexts their strategies correspond to? And how do they aim to sustain surveillance realism? We have shown that NSO used four key legitimacy management practices (Suchman, 1995) in its quest for legitimacy: securitization, Zionist patriotism, ethics washing, and normalization. We argue that each of these strategies was communicated with particular audiences in mind, and together they aim to create an impression that NSO is a benevolent, patriotic, cooperative, transparent, and normative actor who is far removed from the image of secrecy and subterfuge attributed to it by its critics. Particularly, the first two legitimation strategies (securitization discourse and Zionist patriotism) primarily operate on a localized legitimation axis, one that is aimed at Israeli audiences and echoes a particularly Israeli 'security-driven populism' (Levi & Agmon, 2021). The last two strategies (ethics washing and normalization) revolve around a universal axis, with more international audiences in mind and following Silicon Valley's precedents. These two axes of legitimation are designed to simultaneously ensure the company's survivability and aim to more generally, sustain surveillance realism - the feeling that surveillance is an essential part of contemporary life with deep roots in various social structures. Nevertheless, these axes' reach is far from identical.

As an Israeli company that is highly reliant on Israeli regulators and politicians, NSO has concentrated much of its legitimation efforts on its local axis and on Israeli audiences:

75% of its media appearances were on Israeli media outlets (33/44), and its messages are meticulously designed with distinct Israeli symbolism and cultural tropes. With repetitive references to the Holocaust, Zionist nation-building, and to terror threats, NSO turns to discourses that echo dominant themes from today's political zeitgeist (Brubaker, 2017) and that specifically prove effective among Israeli politicians, media, and citizens alike (Levi & Agmon, 2021; Panievsky, 2021). This line of legitimation is understandable, given that Israeli politicians and regulators have the power to restrict or even halt NSO's activities. Indeed, while in the last years, some Israeli journalists grew critical of NSO, Israeli politicians, regulators, and jurists seemed largely unfazed by the reports. Thus, for a time, NSO's local legitimation axis seemed to have successfully fended off multiple scandals, preserving the legitimacy and survivability of the company and sustaining surveillance realism – at least locally.

However, as Suchman argued, 'legitimacy is resilient to particular events, yet it is dependent on a history of events' (1995:, p. 5), and indeed, by the end of 2021, and following some major global events, NSO's luck, and legitimacy, seemed to have run out. In November 2021, the US Commerce Department had blacklisted NSO – prohibiting American firms from selling technology to NSO or its subsidiaries. This dramatic move was more than another descriptive report about the company; it was a harsh response from an American regulatory agency. Subsequently, by August 2022, and further burdened by that year crisis in tech, NSO reportedly fired 100 workers; Hulio, the company's CEO who also spearheaded the company's legitimation campaign, resigned, and NSO was reportedly nearing bankruptcy. This was a legitimation crisis with global origins, but one that NSO's universal, world-facing legitimation axis could not avert. Thus, NSO's efforts to discursively secure its survival seemed to have failed, and their attempts to present cyber-surveillance as a taken-for-granted-yet-essential fact of life proved fruitless.

In the last decade, surveillance scholars have shown how companies and governments actively sow digital resignation, passivity, and complacency among citizens and 'users' – making surveillance a taken-for-granted, unavoidable fact of life (Dencik, 2018; Draper & Turow, 2019; Marwick & Hargittai, 2019). Nevertheless, the efforts to sustain surveillance realism (Dencik & Cable, 2017) go beyond governments' and corporations' mass surveillance and their relationships with their 'users.' Cyber-espionage companies like NSO might not target the masses, but their interest in sustaining surveillance realism is clear. The legitimacy, legality, and survivability of such companies depend on how multiple stakeholders see and understand surveillance, and as we have shown above, they actively strive to sustain it with various stakeholders in mind.

Sociologist Eric Schoon (2022) has recently described legitimacy as a dyadic process - one that inherently includes two nodes and a tie - an object of legitimacy, an audience, and the relationship that connects the two. As Schoon explains, nodes in a dyad are not limited to individuals, and they can be any social entity. Indeed, NSO's legitimation campaign is not only aimed at cultivating user resignation, but it mainly seeks approval and complicity from politicians and regulators in Israel and abroad; the sympathy of current and future employees; their investors' loyalty; their potential customers' acceptance, and more. It is on these stakeholders that this company's survivability, and surveillance's place in today's life, depends. Hence, as NSO's legitimation campaign reveals, the nurturing of surveillance realism depends on diverse-but-interdependent factors and on

simultaneously sustaining companies' multiple dyadic ties (Schoon 2022) with various stakeholders.

Thus, focusing on how NSO actively legitimates their surveillance also reveals the discursive foundations surveillance firms build to sustain their surveillance empires. It serves as a reminder that cyber-surveillance is more than the computers, the code, and the data that runs between them. It is also more than the funds that flow between those who surveil and those who supply the technology for this surveillance. Such intrusive practices also rely on words, local symbolism, cultural tropes, and on the degree of fit between these firms and their various audiences.

Moreover, while surveillance is often understood as a global power, this article highlights the need to focus on the local contexts from which surveillance emanates and operates. As we have shown above, considering the local factors behind such firms can better elucidate the ties between surveillance and society and highlight the social structures that sustain it to become surveillance realism (Dencik & Cable, 2017). Such an approach can also flesh out the specific sensibilities, frictions, and cultural tropes that make specific societies more receptive to surveillance, and hence reveal the weaknesses in such firms' legitimation and consequently 'immunize' (van der Linden, 2022) relevant stakeholders and audiences most susceptible to the companies' pleas. Hence, highlighting surveillance firms' active legitimation attempts in their contexts can not only shed light on today's surveillance, but also offer ways of resistance.

Conclusion

This paper examined NSO Group's legitimation practices, and how they construct and sustain the discursive infrastructure of contemporary surveillance. We have shown that NSO simultaneously uses local and universal tropes to ensure its survivability and to help sustain surveillance realism - the perception of surveillance as the only viable option (Dencik & Cable, 2017, p. 20).

While surveillance firms often operate in the dark, this research joins recent works (Iliadis & Acker, 2022; Knight & Gekker, 2020) in showing that they in fact leave considerable traces for social scientists to study. This article also contributes to surveillance studies by shedding light on cyber espionage companies; by highlighting how surveillance companies actively legitimize their surveillance; and by highlighting the discursive sustainment of surveillance realism. Our findings also offer a path towards identifying vulnerabilities in such companies' narratives by highlighting their local and universal origins, and thus 'immunize' publics and stakeholders against their legitimation attempts.

Studying cyber surveillance companies is inherently limited by the secrecy of such companies and the relative scarcity of data about them. The opacity of their actions and tools also limits our ability to verify their arguments, and observe their internal legitimation efforts - with their customers, investors, and employees. Future works should explore how other spyware companies in other contexts legitimize their practices. Research should also explore how media outlets and politicians legitimize, resist, and at times cooperate with such companies and delve into the ties between surveillance firms and nation-states. These lines of research can help better elucidate the role of surveillance in contemporary life and perhaps help ground the next Pegasus before it takes flight.

Notes

1. From here on will be called NSO.
2. While research on surveillance realism predominantly focuses on users' perspective, this article highlights surveillance firms' discursive attempts to actively construct and sustain it.
3. The analysis stems from a constructivist perspective, focusing on how NSO discursively legitimize their work, rather than the veracity of their claims. Moreover, while the analysis focused on NSO's direct utterances, these are in no way seen as natural or "unmediated" texts. Taken individually, each utterance was at least partially framed by the specific journalist, editor, or media outlet in which it appeared (Scheufele, 1999) and was presumably created with the help of various consultants, lobbyists, or spinsters. However, as we detail below, collectively and across media, these utterances create a coherent set of legitimation strategies that go beyond the framings of specific media outlets.
4. NSO's origin story is mentioned in 34% of its media engagements (15/44 documents). For example, 15ISM19, 22ISM21, 33ISM21.
5. This theme was discussed in 27% of NSO's media engagements (12/44).
6. The term 'terror' (in all its forms) appeared 504 times in 79 documents. The term 'crime' (in all its forms) appeared 483 times in 69 documents; And the term 'pedophile' in all its forms appeared 77 times in 21 documents.
7. Interestingly, the list of crimes prevented with Pegasus never contains white collar crimes such as corruption, tax evasion, or embezzlement.
8. Accordingly, NSO repeatedly claims that it only sells Pegasus to governments, thus aiming to reassure its audiences that their product is in legitimate hands who legitimately use it to prevent ominous consequences. In fact, foreign governments are mentioned in 46% of NSO's media engagements, and it is also their main line of defense in the WhatsApp v NSO Group Lawsuit, as part of their claim for a 'foreign sovereign immunity' (59-60L22).
9. This theme appeared in 43 of NSO's media engagements (19/44).
10. See 28ISM21, 29ISM21, 34ISM22.
11. This theme appeared in 24% of the company's Linkedin posts, and in 20% of the total documents.
12. See also 28ISM21, 4IM21, 268W19, 269W20, and more.

Acknowledgement

We thank Alex Gekker, Anat Ben-David, and Asaf Darr for their invaluable comments on previous versions of this article. We also thank ICS's anonymous reviewers for their insightful suggestions and Einav Stapleton for her help in collecting and making sense of NSO's data.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Dr. Elinor Carmi is a Senior Lecturer in Data Politics and Social Justice at the Sociology & Criminology Department at City University, London, UK. Dr. Carmi is a digital rights advocate, feminist, researcher and journalist who has been working, writing and teaching on data politics, data literacies, feminist approaches to media and data, data justice and internet governance.

Dr. Dan M. Kotliar is a lecturer (assistant professor) at the Department of Sociology, University of Haifa, Israel. Dr. Kotliar's work revolves around critical algorithm studies focusing on algorithmic production in Israel and Silicon Valley, cyber surveillance firms, AI ethics, AI hype, data infrastructures, and more.

ORCID

Dan M. Kotliar http://orcid.org/0000-0001-7028-1678
Elinor Carmi http://orcid.org/0000-0003-1108-2075

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the Age of information. *Science*, *347*(6221), 509–514. https://doi.org/10.1126/science.aaa1465

Ananny, M., & Crawford, K. (2018). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. *New Media & Society*, *20*(3), 973–989. https://doi.org/10.1177/1461444816676645

Andrejevic, M. (2007). *iSpy: Surveillance and power in the interactive era*. University Press of Kansas.

Aspril, S. (2012). We have a listener on the line. *Calcalist* 18 October [Hebrew]. Retrieved from: https://www.calcalist.co.il/local/articles/0,7340,L-3585117,00.html.

Ball, K., Haggerty, K., & Lyon, D. (eds.). (2012). *Routledge handbook of surveillance studies*. Routledge. https://doi.org/10.4324/9780203814949.

Ben-David, A., & Amram, A. (2018). The internet archive and the socio-technical construction of historical facts. *Internet Histories*, *2*(1-2), 179–201. https://doi.org/10.1080/24701475.2018.1455412

Ben-Eliezer, U. (1998). *The making of Israeli militarism*. Indiana University Press.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brubaker, R. (2017). Why populism? *Theory and Society*, *46*(5), 357–385. https://doi.org/10.1007/s11186-017-9301-7

Carmi, E. (2020). *Media distortions: Understanding the power behind spam, noise, and other deviant media*. Peter Lang International Academic Publishers.

Crain, M. (2018). The limits of transparency: Data brokers and commodification. *New Media & Society*, *20*(1), 88–104. https://doi.org/10.1177/1461444816657096

Creech, B., & Maddox, J. (2022). Thus spoke zuckerberg: Journalistic discourse, executive personae, and the personalization of tech industry power. *New Media & Society*, *0*(0).

Dencik, L. (2018). Surveillance Realism and the Politics of Imagination: Is There No Alternative? *Krisis: Journal for Contemporary Philosophy*, *1*, 31–43. https://doi.org/10.14361/dcs-2016-0205

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the Snowden leaks. *International Journal of Communication*, *11*, 763–781.

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, *21*(8), 1824–1839. https://doi.org/10.1177/1461444819833331

Feldman, J. (2008). *Above the death pits, beneath the flag: Youth voyages to Poland and the performance of Israeli national identity*. Berghahn Books.

Gekker, A., & Hind, S. (2019). Infrastructural surveillance. *New Media & Society*, *22*(8), 1414–1436. https://doi.org/10.1177/1461444819879426

Haupt, J. (2021). Facebook futures: Mark Zuckerberg's discursive construction of a better world. *New Media & Society*, *23*(2), 237–257. https://doi.org/10.1177/1461444820929315

Hoefer, R. L., & Green Jr. S. E. (2016). A rhetorical model of institutional decision making: The role of rhetoric in the formation and change of legitimacy judgments. *Academy of Management Review*, *41*(1), 130–150. https://doi.org/10.5465/amr.2014.0330

Iliadis, A., & Acker, A. (2022). The seer and the seen: Surveying Palantir's surveillance platform. *The Information Society*, *38*(5), 334–363. https://doi.org/10.1080/01972243.2022.2100851

Johnson, C., Dowd, T. J., & Ridgeway, C. L. (2006). Legitimacy as a social process. *Annual Review of Sociology*, *32*, 53–78.

Kimmerling, B. (1993). Patterns of militarism in Israel. *European Journal of Sociology*, *34*(2), 196–223. https://doi.org/10.1017/S0003975600006640

Knight, E., & Gekker, A. (2020). Mapping interfacial regimes of control: A qualitative analysis of America's post-9/11 security technology infrastructure. *Surveillance & Society*, *18*(2), 231–243. https://doi.org/10.24908/ss.v18i2.13268

Kuehn, K. M. (2018). Framing mass surveillance: Analyzing New Zealand's media coverage of the early Snowden files. *Journalism*, *19*(3), 402–419. https://doi.org/10.1177/1464884917699238

Leslie, J. G. (2017). Netanyahu's populism: An overlooked explanation for Israeli foreign policy. *SAIS Review of International Affairs*, *37*(1), 75–82. https://doi.org/10.1353/sais.2017.0006

Levi, Y., & Agmon, S. (2021) Beyond culture and economy: Israel's security-driven populism. *Contemporary Politics*, *27*(3), 292–315. https://doi.org/10.1080/13569775.2020.1864163

Lischka, J. A. (2017). Explicit terror prevention versus vague civil liberty: how the UK broadcasting news (de)legitimatise online mass surveillance since Edward Snowden's revelations. *Information, Communication & Society*, *20*(5), 665–682. https://doi.org/10.1080/1369118X.2016.1211721

Madianou, M. (2019). Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises. *Social Media + Society*, *5*(3), https://doi.org/10.1177/2056305119863146

Marciano, A. (2019). The discursive construction of biometric surveillance in the Israeli press: Nationality, citizenship, and democracy. *Journalism Studies*, *20*(7), 972–990. https://doi.org/10.1080/1461670X.2018.1468723

Marczak, B., & Scott-Railton, J. (2016). The million dollar dissident: NSO group's IPhone zero-days used against a UAE human rights defender. Citizen Lab Research Report. University of Toronto. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

Marwick, A., & Hargittai, E. (2019). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, *22*(12), 1697–1713. https://doi.org/10.1080/1369118X.2018.1450432

Mols, A., & Janssen, S. (2017). Not interesting enough to be followed by the NSA: An analysis of Dutch privacy attitudes. *Digital Journalism*, *5*(3), 277–298. https://doi.org/10.1080/21670811.2016.1234938

Panievsky, A. (2021). Covering populist media criticism: When journalists' professional norms turn against them. *International Journal of Communication*, *15*, 2136–2155.

Reyes, A. (2011). Strategies of legitimization in political discourse: From words to actions. *Discourse & Society*, *22*(6), 781–807. https://doi.org/10.1177/0957926511419927

Scheufele, D. A. (1999). Framing as a theory of media effects. *Journal of Communication*, *49*(1), 103–122. https://doi.org/10.1111/j.1460-2466.1999.tb02784.x

Schoon, E. W. (2022). Operationalizing legitimacy. *American Sociological Review*, *87*(3), 478–503. https://doi.org/10.1177/00031224221081379

Schulze, M. (2015). Patterns of surveillance legitimization. The German discourse on the NSA scandal. *Surveillance & Society*, *13*(2), 197–217. https://doi.org/10.24908/ss.v13i2.5296

Stritzel, H. (2007). Towards a theory of securitization: Copenhagen and beyond. *European Journal of International Relations*, *13*(3), 357–383. https://doi.org/10.1177/1354066107080128

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *The Academy of Management Review*, *20*(3), 571–610. https://doi.org/10.2307/258788

Suddaby, R., Bitektine, A., & Haack, P. (2017). Legitimacy. *Academy of Management Annals*, *11*(1), 451–478. https://doi.org/10.5465/annals.2015.0101

Tost, L. P. (2011). An integrative model of legitimacy judgments. *Academy of Management Review*, *36*(4), 686–710. https://doi.org/10.5465/amr.2010.0227

Tréguer, F. (2017). Intelligence reform and the Snowden paradox: The case of France. *Media and Communication*, *5*(1), 17–28. https://doi.org/10.17645/mac.v5i1.821

van der Linden, S. (2022). Misinformation: Susceptibility, spread, and interventions to immunize the public. *Nature Medicine*, *28*(3), 460–467. https://doi.org/10.1038/s41591-022-01713-6

Van Dijck, J. (2014). Datafication, dataism, and dataveillance: Big data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Wagner, B. (2018). Ethics as an escape from regulation. From "ethics-washing" to ethics-shopping? In being profiled: Cogitas ergo Sum: 10 years of profiling the European citizen. Amsterdam University Press.

Wahl-Jorgensen, K., Bennett, L., & Taylor, G. (2017). The normalization of surveillance and the invisibility of digital citizenship: Media debates after the Snowden revelations. *International Journal of Communication*, *11*, 740–762.

Weber, M. (1978 (1924)). *Economy and society*. University of California Press.

Wodak, R. (2014). Critical discourse analysis. In C. Leung & B. V. Street (Eds.), *The Routledge companion to English studies* (pp. 302–316). Routledge.

Yadlin, A., & Marciano, A. (2022). COVID-19 surveillance in Israeli press: Spatiality, mobility, and control. *Mobile Media & Communication*, *10*(3), 421–447. https://doi.org/10.1177/20501579211068269

Zuboff, S. (2019). *The Age of surveillance capitalism: The fight for a human future at the New frontier of power*. Public Affairs.

Appendix 1

No.	Code	Type	Year	Title	Date	Source	Link
1	1IM16	International media	2016	Meet NSO Group, The New Big Player in The Government Spyware Business	8/25/2016	Vice	https://www.vice.com/en/article/wnxpjm/nso-group-new-big-player-in-government-spyware
2	2IM19	International media	2019	Interview with CEO of NSO Group – Israeli spyware-maker	5/14/2019	CBS	https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/
3	3IM20	International media	2020	The man who built a spyware empire says it's time to come out of the shadows	8/19/2020	MIT TR	https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/
4	4IM21	International media	2021	Israel's Invisible Dome Can Stop Drones & Terrorist Attacks | Insights: Israel & the Middle East	6/19/2021	TBN	https://www.youtube.com/watch?v=ltA1WLBSkfs
5	5IM21	International media	2021	Private Israeli spyware used to hack cellphones of journalists, activists worldwide	7/18/2021	Wapo	https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/
6	6IM21	International media	2021	list of countries using oegasus totally incorrect some not even clients international conspiracy says NSO group in an interview to ANI	7/19/2021	ANI	https://www.aninews.in/news/national/general-news/list-of-countries-using-pegasus-totally-incorrect-some-not-even-clients-international-conspiracy-says-nso-group-in-an-interview-to-ani20210719123022/
7	7IM21	International media	2021	'Somebody has to do the dirty work': NSO founders defend the spywear they built	7/21/2021	WaPo	'Somebody has to do the dirty work': NSO founders defend the spyware they built - The Washington Post
8	8IM22	International media	2021	Shalev Hulio, NSO, and Pegasus	9/2/2021	Forbes	https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-pegasus-project-hacking-allegations/?sh=5015b10a472d
9	9IM21	International media	2021	Israel's Cyber Security: The Invisible War	2/3/2022	TBN	https://www.youtube.com/watch?v=3t-wlXhh72Y
10	10INM22	International media	2022	The Battle for the World's Most Powerful Cyberweapon	1/28/2022	NYT	https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html
11	11IM22	International media	2022	NSO Never Engaged in Illegal Mass Surveillance	2/24/2022	WSJ	NSO Never Engaged in Illegal Mass Surveillance - WSJ

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
12	12IM22	International media	2022	How Democracies Spy on Their Citizens. The New Yorker	4/18/2022	New Yorker	https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens
13	13ISM12	Israeli media	2012	יש לנו מאזין על הקו	10/18/2012	Calcalist	https://www.calcalist.co.il/local/articles/0,7340,L-3585117,00.html
14	14ISM15	Israeli media	2015	פרק 29: סייבר עם שלו חוליו	4/20/2015	Cyber Podcast	https://www.shavua.net/episodes/29
15	15ISM19	Israeli media	2019	אצלי הכל בסייבר	1/9/2019	YA	https://www.yediot.co.il/articles/0,7340,L-5444102,00.html
16	16ISM19	Israeli media	2019	שירי דולב, נשיאת NSO. גיל: 43 | מצב משפחתי: נשואה ואם לשלושה | תואר ראשון בהנדסת חשמל	7/28/2019	Globes	https://www.globes.co.il/news/article.aspx?did=1001300462
17	17ISM19	Israeli media	2019	כשחברה מצליחה להשיג אימפקט כה גדול בזמן כה קצר, יש מי שמנסה לנצל את זה"	9/30/2019	Globes	https://www.globes.co.il/news/article.aspx?did=1001301294
18	18ISM19	Israeli media	2019	שירי דולב - Mind The Tech 2019	11/25/2019	Calcalist	https://www.youtube.com/watch?v=3_MA7rQzWu0
19	19ISM20	Israeli media	2020	חמ"ל בהיי-טק: הכירו את החברות שמינו "קציני קורונה"	4/3/2020	Ynet	https://www.ynet.co.il/economy/article/BJGpDAZvL
20	20ISM20	Israeli media	2020	הודף את NSO רבים מהפרסומים עלינו – שגויים": מייסד הביקורת	4/6/2020	13	https://13tv.co.il/item/news/domestic/nso-interview-1042525/
21	21ISM20	Israeli media	2020	חברת הסייבר שמוכרת מערכות ריגול פתחה שלוחה בערבה	12/7/2020	Ynet	https://www.ynet.co.il/economy/article/SJ81J65jw
22	22ISM21	Israeli media	2021	כנס האינטרנט של קשת	2/14/2021	Mako	https://www.mako.co.il/special-conferences/Article-9b08edaa5578771027.htm
23	23ISM21	Israeli media	2021	NSO זה לא רק סייבר מודיעיני	4/11/2021	Calcalist	https://www.calcalist.co.il/conference/articles/0,7340,L-3904074,00.html
24	24ISM21	Israeli media	2021	ועידת כחול לבן - חוליו 2021	4/20/2021	Calcalist	https://www.youtube.com/watch?v=_KDYb86YKy0
25	25ISM21	Israeli media	2021	ועידת כחול לבן – שירי דולב	4/20/2021	Calcalist	https://www.youtube.com/watch?v=yK88BMZRcpY
26	25ISM21	Israeli media	2021	נכ"ל NSO: "רשימת 50 אלף מספרי הטלפון לא קשורה אלינו" (Document)	7/20/2021	Ynet	https://www.ynet.co.il/news/article/rkgdzv40d
27	27ISM21	Israeli media	2021	ריאיון ראשון עם מנכ"ל NSO: "אין לנו רשימת מטרות" - וואלה! חדשות	7/20/2021	Walla	https://news.walla.co.il/item/3449244
28	28ISM21	Israeli media	2021	מישהו החליט ללכת לנו על הראש. יש עליהום על הסייבר הישראלי" (ישר	7/22/2021	IH	https://www.israelhayom.co.il/magazine/hashavua/article/3540783
29	29ISM21	Israeli media	2021	מנכ"ל NSO: "בחרנו שלא לפעול נגד מספרים ישראלים ואמריקנים"	7/22/2021	GLZ	https://glz.co.il/גלצ/תוכניות/אילנה-דיין/אילנה-דיין0801-22-07-2021/מנכל-nso-שלא-בחרנו-לפעול-נגד-מספרים-ישראלים-ואמריקנים

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
30	30ISM21	Israeli media	2021	'If You're Not A Criminal, Don't Be Afraid'	7/22/2021	Forbes	https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-pegasus-project-hacking-allegations/?sh=fb1f584472d8
31	31ISM21	Israeli media	2021	NSO Group Executives Discusses Pegasus, Says Company Has Nothin	7/25/2021	i24	https://www.youtube.com/watch?v=ObW31P7VUsU
32	32ISM21	Israeli media	2021	מנכ"ל NSO מגיב לסערה בראיון לפורבס: "רק פושעים צריכים לחשוש מאיתנו	7/25/2021	Forbes IL	https://forbes.co.il/nso-ceo-intereview-forbes/
33	33ISM21	Israeli media	2021	Omri Lavie at the 20 Minute Leaders Podcast	7/28/2021	20m Leaders podcast	https://www.audible.com/pd/Ep505-Omri-Lavie-Co-Founder-CEO-Orchestra-Group-Podcast/B09BC9HV2C
34	34ISM22	Israeli media	2022	ריאיון עם מנכ"ל NSO: "פה כדי להישאר"	1/29/2022	Mako	https://www.mako.co.il/news-channel12?subChannelId=5664a3056f87d710VgnVCM200000650a10acRCRD&vcmid=4cc1ce7c727ae710VgnVCM200000650a10acRCRD
35	35ISM22	Israeli media	2022	NSO chief calls blacklisting by US 'an outrage,' rejects 'hypo	1/30/2022	Times of Israel	https://www.timesofisrael.com/nso-chief-calls-blacklisting-by-us-an-outrage-rejects-hypocritical-criticism/
36	36ISM77	Israeli media	2022	The Man at the Center of the Storm	2/11/2022	Times of Israel	https://www.timesofisrael.com/spotlight/the-man-at-the-center-of-the-storm/
37	37ISM22	Israeli media	2022	מנכ"ל NSO מגיב לראשונה אחרי התחקיר המטלטל mako.co.il) (Documen)	2/11/2022	Mako	https://www.mako.co.il/nexter-news/Article-a82d051cb35ee71027.htm
38	38ISM22	Israeli media	2022	N12 - NSO תובעת את כלכליסט: "פרסום חד-צדדי, מוטה וכוזב" (mako.c)	2/27/2022	Mako	https://www.mako.co.il/news-israel/2022_q1/Article-d22c22a325a3f71027.htm
39	39ISM22	Israeli media	2022	חברת NSO הגישה תביעת לשון הרע נגד 'כלכליסט'	2/27/2022	Calcalist	https://www.calcalist.co.il/local_news/article/bkmqbykl5
40	40ISM22	Israeli media	2022	אחד ממייסדי חברת הסייבר NSO ירד מתחת לרדאר. איתרנו אותו בשווייץ	3/4/2022	Globes	https://www.globes.co.il/news/article.aspx?did=1001404102
41	41ISM22	Israeli media	2022	"ללא יכולות סייבר, תהיה פגיעה ביכולת של גופי הביטחון"	3/29/2022	103fm	https://103fm.maariv.co.il/programs/media.aspx?ZrqvnVq=IJLLHJ&c41t4nzVQ=FJF
42	42ISM22	Israeli media	2022	מנכל אן אס או: פעולה ללא יכולות סייבר פוגעת בחקירת גופי הביטחו	3/29/2022	103fm	https://103fm.maariv.co.il/programs/media.aspx?ZrqvnVq=IJLLHJ&c41t4nzVQ=FJF
43	43ISM22	Israeli media	2022	Document) "ההפתעה לה זכה חתן "חתונה ממבט ראשון" (168), Pos. 1)	5/23/2022	Maariv	https://tmi.maariv.co.il/celebs-news/Article-919875
44	44ISM22	Israeli media	2022	Report: Israel pushing US to remove scandal-ridden NSO Group fr	6/11/2022	Times of Israel	https://www.timesofisrael.com/report-israel-pushing-us-to-remove-scandal-ridden-nso-group-from-blacklist/

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
45	45L19	Legal documents	2019	בית משפט השלום	2019		
46	46L19	Legal documents	2019	NSO-Motion-to-Dismiss	2019		
47	47L20	Legal documents	2020	WhatsApp Inc. v. NSO Grp. Techs. Ltd., 2020 U.S. App. LEXIS 327	2020		
48	48L20	Legal documents	2020	WhatsApp Inc. v. NSO Grp. Techs. Ltd., 2020 U.S. Dist. LEXIS 64	2020		
49	49L20	Legal documents	2020	WhatsApp Inc. v. NSO Grp. Techs. Ltd., 2020 U.S. Dist. LEXIS 71	2020		
50	50L20	Legal documents	2020	WhatsApp Inc. v. NSO Grp. Techs., 2020 U.S. Dist. LEXIS 79901	2020		
51	51L20	Legal documents	2020	WhatsApp Inc. v. NSO Grp. Techs., Ltd., 472 F. Supp. 3d 649	2020		
52	52L20	Legal documents	2020	Whatsapp Inc. v. NSO Grp. Techs. Ltd., 2020 U.S. Dist. LEXIS 24	2020		
53	53L20	Legal documents	2020	Whatsapp Inc. v. NSO Grp. Techs. Ltd., 491 F. Supp. 3d 584	2020		
54	54L20	Legal documents	2020	Whatsapp Inc. v. Nso Group Techs., 2020 U.S. Dist. LEXIS 247690	2020		
55	55L20	Legal documents	2020	NSO's appeal to U.S. District Court for's decision	2020		
56	56L20	Legal documents	2020	Trinh et al. - BRIEF FOR AMICI CURIAE MICROSOFT CORP., CISCO SY	2020		
57	57L21	Legal documents	2021	US Court of Appeals 9th	2021		
58	58L22	Legal documents	2022	Ghada Oueiss v. Saud, 2022 U.S. Dist. LEXIS 80547	2022		
59	59L22	Legal documents	2022	WhatsApp Inc. v. NSO Grp. Techs. Ltd., 17 F.4th 930	2022		
60	60L22	Legal documents	2022	Whatsapp v. Nso Group Techs., 2022 U.S. App. LEXIS 408	2022		
61	61LI19	LinkedIn	2019	2019- ISS World Europe	2019		
62	62LI19	LinkedIn	2019	May 2019- Security Conference Miami	2019		
63	63LI19	LinkedIn	2019	2019- ISS World Prague	2019		
64	64LI19	LinkedIn	2019	2019- Shiri Dolev	2019		
65	65LI19	LinkedIn	2019	2019- ISS World North America	2019		
66	66LI19	LinkedIn	2019	2019- Tom Ridge Article	2019		
67	67LI19	LinkedIn	2019	2019- Shiri Dolev	2019		
68	68LI19	LinkedIn	2019	2019- Milipol Paris	2019		
69	69LI19	LinkedIn	2019	2019- Official response to the lawsuit filed by Facebook	2019		
70	70LI19	LinkedIn	2019	2019- Milipol Paris	2019		

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
71	71LI19	LinkedIn	2019	2019- Calcalist mind the tech conference	2019		
72	72LI19	LinkedIn	2019	2019- Holiday Season	2019		
73	73LI20	LinkedIn	2020	2020- New Year	2020		
74	74LI20	LinkedIn	2020	2020- Come Join Us	2020		
75	75LI20	LinkedIn	2020	2020- 10 Years Anniversary	2020		
76	76LI20	LinkedIn	2020	2020- Come Join Us	2020		
77	77LI20	LinkedIn	2020	2020- A reason Shiri Dolev is proud to work at NSO	2020		
78	78LI20	LinkedIn	2020	2020- European Police Congress	2020		
79	79LI20	LinkedIn	2020	2020- Convexum	2020		
80	80LI20	LinkedIn	2020	2020- HR Meet Up	2020		
81	81LI20	LinkedIn	2020	2020- Come Join Us	2020		
82	82LI20	LinkedIn	2020	2020- Security and Policing Event	2020		
83	83LI20	LinkedIn	2020	2020- Come Join Us	2020		
84	84LI20	LinkedIn	2020	2020- Security Policing 2020	2020		
85	85LI20	LinkedIn	2020	2020- Security Policing 2020	2020		
86	86LI20	LinkedIn	2020	2020- Women In Tech	2020		
87	87LI20	LinkedIn	2020	2020- Purim	2020		
88	88LI20	LinkedIn	2020	2020- NSO family	2020		
89	89LI20	LinkedIn	2020	2020- Work in the time of Corona	2020		
90	90LI20	LinkedIn	2020	2020- Employee Story	2020		
91	91LI20	LinkedIn	2020	2020- ZOOM screenshot	2020		
92	92LI20	LinkedIn	2020	2020- PRO women zoom meeting	2020		
93	93LI20	LinkedIn	2020	2020- NSO studio	2020		
94	94LI20	LinkedIn	2020	2020- Online Standup	2020		
95	95LI20	LinkedIn	2020	2020- Shalev Hulio Interviews on 13News	2020		
96	96LI20	LinkedIn	2020	2020 - Fighting Coronavirus	2020		
97	97LI20	LinkedIn	2020	2020- Fleming	2020		
98	98LI20	LinkedIn	2020	2020- Fleming	2020		
99	99LI20	LinkedIn	2020	April 2020- Yom Hazikaron	2020		
100	100LI20	LinkedIn	2020	April 2020- Independence Day	2020		
101	101LI20	LinkedIn	2020	2020- Fleming	2020		
102	102LI20	LinkedIn	2020	2020- Fleming	2020		
103	103LI20	LinkedIn	2020	2020- Fleming	2020		
104	104LI20	LinkedIn	2020	May 2020- International day of families	2020		
105	105LI20	LinkedIn	2020	May? 2020- World Telecommunication Day	2020		
106	106LI20	LinkedIn	2020	2020- Employee Story	2020		
107	107LI20	LinkedIn	2020	2020- Transparency	2020		

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
108	108LI20	LinkedIn	2020	2020- Gifts For Employees	2020		
109	109LI20	LinkedIn	2020	2020- Employee Story	2020		
110	110LI20	LinkedIn	2020	2020- Career at NSO	2020		
111	111LI20	LinkedIn	2020	2020 - Eclipse	2020		
112	112LI20	LinkedIn	2020	2020- Eclipse	2020		
113	113LI20	LinkedIn	2020	July? 2020- Pride Month	2020		
114	114LI20	LinkedIn	2020	2020- Eclipse	2020		
115	115LI20	LinkedIn	2020	2020- Eclipse	2020		
116	116LI20	LinkedIn	2020	2020- Employee Story	2020		
117	117LI20	LinkedIn	2020	2020- Eclipse	2020		
118	118LI20	LinkedIn	2020	2020- Employee Story	2020		
119	119LI20	LinkedIn	2020	2020- Court's Rejections of Amnesty International's Petition	2020		
120	120LI20	LinkedIn	2020	2020- Eclipse	2020		
121	121LI20	LinkedIn	2020	2020- Eclipse	2020		
122	122LI20	LinkedIn	2020	2020- Process Transparency	2020		
123	123LI20	LinkedIn	2020	2020-Eclipse	2020		
124	124LI20	LinkedIn	2020	2020- Drones	2020		
125	125LI20	LinkedIn	2020	August 2020- International Dog Day	2020		
126	126LI20	LinkedIn	2020	2020- Eclipse	2020		
127	127LI20	LinkedIn	2020	2020- Eclipse	2020		
128	128LI20	LinkedIn	2020	2020- Rosh Hashanah	2020		
129	129LI20	LinkedIn	2020	Breast Cancer Awarness	2020		
130	130LI20	LinkedIn	2020	2020- Brasilia	2020		
131	131LI20	LinkedIn	2020	2020- "Best High Tech Companies" Ranking	2020		
132	132LI20	LinkedIn	2020	2020- Reason #1	2020		
133	133LI20	LinkedIn	2020	2020- Reason #2	2020		
134	134LI20	LinkedIn	2020	2020- Reason #3	2020		
135	135LI20	LinkedIn	2020	2020- Reason #4	2020		
136	136LI20	LinkedIn	2020	2020- Reason #5	2020		
137	137LI20	LinkedIn	2020	2020- Reason #6	2020		
138	138LI20	LinkedIn	2020	2020- Reason #7	2020		
139	139LI20	LinkedIn	2020	2020- Reason #8	2020		
140	140LI20	LinkedIn	2020	2020- Reason #9	2020		
141	141LI20	LinkedIn	2020	2020- Reason #10	2020		
142	142LI20	LinkedIn	2020	2020- Reason #11	2020		
143	143LI20	LinkedIn	2020	2020- Reason #12	2020		

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
144	144LI20	LinkedIn	2020	2020- Reason #13	2020		
145	145LI20	LinkedIn	2020	2020- Reason #14	2020		
146	146LI20	LinkedIn	2020	November 2020- "SHEvyon"	2020		
147	147LI20	LinkedIn	2020	2020- Employees Individual Needs	2020		
148	148LI20	LinkedIn	2020	2020- Donating	2020		
149	149LI20	LinkedIn	2020	2020- Voulnteering	2020		
150	150LI20	LinkedIn	2020	2020- International Elimination of Violence Day	2020		
151	151LI20	LinkedIn	2020	2020- Donating	2020		
152	152LI20	LinkedIn	2020	2020- Eclipse	2020		
153	153LI20	LinkedIn	2020	2020- New Branch Offices	2020		
154	154LI20	LinkedIn	2020	2020- Human Rights Day	2020		
155	155LI20	LinkedIn	2020	2020- Hanukkah	2020		
156	156LI20	LinkedIn	2020	2020- Hackathon Lior Boker	2020		
157	157LI20	LinkedIn	2020	2020- NSO's search & Rescue Team	2020		
158	158LI20	LinkedIn	2020	2020 Christmas	2020		
159	159LI20	LinkedIn	2020	2020 - VR experiences - Employees	2020		
160	160LI21	LinkedIn	2021	Eclipse	2021		
161	161LI21	LinkedIn	2021	Empowering team members	2021		
162	162LI21	LinkedIn	2021	32 most desirable workplace in Israel	2021		
163	163LI21	LinkedIn	2021	Intl dayy of education	2021		
164	164LI21	LinkedIn	2021	Holocaust Remembrance Day	2021		
165	165LI21	LinkedIn	2021	Data privacy day	2021		
166	166LI21	LinkedIn	2021	Cancer day	2021		
167	167LI21	LinkedIn	2021	#SaferInternetDay	2021		
168	168LI21	LinkedIn	2021	Family Day	2021		
169	169LI21	LinkedIn	2021	TOHACon conference	2021		
170	170LI21	LinkedIn	2021	Purim 2021	2021		
171	171LI21	LinkedIn	2021	COVID19 vaccination	2021		
172	172LI21	LinkedIn	2021	Eclipse	2021		
173	173LI21	LinkedIn	2021	Beach Cleanup	2021		
174	174LI21	LinkedIn	2021	DIY workshop	2021		
175	175LI21	LinkedIn	2021	Intl women's day	2021		
176	176LI21	LinkedIn	2021	IDC	2021		
177	177LI21	LinkedIn	2021	Good deeds day	2021		
178	178LI21	LinkedIn	2021	Passover	2021		
179	179LI21	LinkedIn	2021	World Autism Day	2021		
180	180LI21	LinkedIn	2021	memorial day	2021		

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
181	181LI21	LinkedIn	2021	Memorial day	2021		
182	182LI21	LinkedIn	2021	ועידת כחול לבן	2021		
183	183LI21	LinkedIn	2021	Memorial Day	2021		
184	184LI21	LinkedIn	2021	Independence day	2021		
185	185LI21	LinkedIn	2021	Eclipse	2021		
186	186LI21	LinkedIn	2021	Earth Day	2021		
187	187LI21	LinkedIn	2021	NSO "Non Stop Festival"	2021		
188	188LI21	LinkedIn	2021	Eclipse	2021		
189	189LI21	LinkedIn	2021	December 2021- Hanukkah	2021		
190	190LI21	LinkedIn	2021	Nov- Dec 2021- Employee Party	2021		
191	191LI21	LinkedIn	2021	Nov- Dec 2021- Black Friday	2021		
192	192LI21	LinkedIn	2021	Nov- Dec 2021- Lior Raz	2021		
193	193LI21	LinkedIn	2021	Nov- Dec 2021- Charity	2021		
194	194LI21	LinkedIn	2021	Nov-Dec 2021- Issac Benbenisti	2021		
195	195LI21	LinkedIn	2021	Nov- Dec 2021- Lonely Peleg	2021		
196	196LI21	LinkedIn	2021	October 2021- Breast cancer awarness	2021		
197	197LI21	LinkedIn	2021	October 2021- Job Openings (Document (230), Pos. 1)	2021		
198	198LI21	LinkedIn	2021	October 2021- Job Openings	2021		
199	199LI21	LinkedIn	2021	October 2021- International Security Expo	2021		
200	200LI21	LinkedIn	2021	Sep-Oct 2021- Eclipse	2021		
201	201LI21	LinkedIn	2021	September 2021- 9/11	2021		
202	202LI21	LinkedIn	2021	September 2021- cybar security	2021		
203	203LI21	LinkedIn	2021	September 2021- Talent acquisition	2021		
204	204LI21	LinkedIn	2021	August- Sep 2021- New School year	2021		
205	205LI21	LinkedIn	2021	July- August 2021- Benbenisi Co-President	2021		
206	206LI21	LinkedIn	2021	July- August 2021- #IAMNSO	2021		
207	207LI21	LinkedIn	2021	July- August 2021- #IAMNSO	2021		
208	208LI21	LinkedIn	2021	July- August 2021- transparency	2021		
209	209LI21	LinkedIn	2021	June- July 2021 enough is enough	2021		
210	210LI21	LinkedIn	2021	June- July 2021- Transparency	2021		
211	211LI21	LinkedIn	2021	June- July 2021- Transparency and responsibility report	2021		
212	212LI21	LinkedIn	2021	June 2021- Israel pride day	2021		
213	213LI21	LinkedIn	2021	June 2021- Eclipse	2021		
214	214LI21	LinkedIn	2021	June 2021- Women Engineering day (Document	2021		
215	215LI21	LinkedIn	2021	June 2021- Cyber Security (Document (212), Pos. 1)	2021		

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
216	216LI21	LinkedIn	2021	June 2021- New Book Club	2021		
217	217LI21	LinkedIn	2021	June 2021- ShieldAfrica21	2021		
218	218LI21	LinkedIn	2021	Mid-June 2021- HackIDC21	2021		
219	219LI21	LinkedIn	2021	2022 - Spreading the love	2021		
220	220LI21	LinkedIn	2021	2021 New Year	2021		
221	221LI21	LinkedIn	2021	Cyber Nation 2021	2021		
222	222LI22	LinkedIn	2022	June 18th, 2022 ISS WORLD	2022		
223	223LI22	LinkedIn	2022	June 16th, 2022	2022		
224	224LI22	LinkedIn	2022	June 4th, 2022	2022		
225	225LI22	LinkedIn	2022	June 2nd, 2022- Hiring	2022		
226	226LI22	LinkedIn	2022	May 2022	2022		
227	227LI22	LinkedIn	2022	Mid-May 2022- חתונה ממבט ראשון	2022		
228	228LI22	LinkedIn	2022	Mid-May 2022	2022		
229	229LI22	LinkedIn	2022	May 2022 Unistream	2022		
230	230LI22	LinkedIn	2022	May 2022 יום העצמאות	2022		
231	231LI22	LinkedIn	2022	April- May 2022 יום הזיכרון	2022		
232	232LI22	LinkedIn	2022	End of April 2022- Maestro	2022		
233	233LI22	LinkedIn	2022	End of April 2022- Holocust Memorial Day	2022		
234	234LI22	LinkedIn	2022	12.4.2022- New Generation of PythoNSO	2022		
235	235LI22	LinkedIn	2022	15.4.2022- Passover	2022		
236	236LI22	LinkedIn	2022	4.4.2022- HIT Panel	2022		
237	237LI22	LinkedIn	2022	31.3.2022- TIME100	2022		
238	238LI22	LinkedIn	2022	30.3.2022- Good Deeds Day	2022		
239	239LI22	LinkedIn	2022	March 2022- Ope Positions	2022		
240	240LI22	LinkedIn	2022	March2022- Purim	2022		
241	241LI22	LinkedIn	2022	March 2022- Pi Day	2022		
242	242LI22	LinkedIn	2022	March 2022- International Women Day	2022		
243	243LI22	LinkedIn	2022	March 2022- NSO CS Academy	2022		
244	244LI22	LinkedIn	2022	Feb-March 2022- Innovation NSO	2022		
245	245LI22	LinkedIn	2022	Feb-March 2022- Pegasus	2022		
246	246LI22	LinkedIn	2022	Feb-March 2022- 36Hour Hackathon	2022		
247	247LI22	LinkedIn	2022	Feb2022- Celebrating Health	2022		
248	248LI22	LinkedIn	2022	January 2022- 7 myth #7	2022		
249	249LI22	LinkedIn	2022	January 2022- 7 myth #6	2022		
250	250LI22	LinkedIn	2022	January 2022- 7 myth #5	2022		
251	251LI22	LinkedIn	2022	January 2022- 7 myth #4	2022		
252	252LI22	LinkedIn	2022	January 2022- 7 myth #3	2022		

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
253	253LI22	LinkedIn	2022	January 2022- 7 myth #2	2022		
254	254LI22	LinkedIn	2022	January 2022- 7 myth #1	2022		
255	255LI22	LinkedIn	2022	January 2022- 2022	2022		
256	256LI22	LinkedIn	2022	Dec- Jan 2022- Holiday Grettings	2022		
257	257LI22	LinkedIn	2022	Dec- Jan 2022- ISS	2022		
258	258LI22	LinkedIn	2022	Dec- Jan 2022- ISS	2022		
259	259ME19	Medium posts	2019	Evolve or Die. Cyber Security challenges post COVID-19 by Omri	9/29/2019		
260	260ME22	Medium posts	2022	Cyber Intelligence Here to stay. by Omri Lavie Medium	2/21/2022		
261	261W18	NSO website	2018	NSO-Statement-17-September-2018	9/17/2018		
262	262W18	NSO website	2018	NSO-Statement-17-September-2018	2018		
263	263W19	NSO website	2019	CEO Shalev Hulio talks for the first time	1/9/2019		
264	264W19	NSO website	2019	Brazilian firefighters and more than 100 Israelis rescue fighte	1/29/2019		
265	265W19	NSO website	2019	NSO_Group_Acquired_by_its_Management	2/14/2019		
266	266W19	NSO website	2019	NSO Group Announces New Human Rights Policy and Governance Fram	9/10/2019		
267	267W19	NSO website	2019	Law enforcement's encryption dilemma	9/19/2019		
268	268W19	NSO website	2019	If We Could Share What NSO Really Does, Media Discourse Would	11/26/2019		
269	269W20	NSO website	2020	NSO_Ltr_to_David_Kaye_-June	2020		
270	270W20	NSO website	2020	NSO is shocked and appalled by the story that has been publishe	1/22/2020		
271	271W20	NSO website	2020	NSO acquires Convexum	2/12/2020		
272	272W20	NSO website	2020	The truth about digital tracking to fight coronavirus	3/25/2020		
273	273W20	NSO website	2020	NSO Group appoints Asher Levy as Executive Chairman (Document (	4/6/2020		
274	274W20	NSO website	2020	"Fleming" is a new program developed by NSO Group (Document (24	5/13/2020		
275	275W20	NSO website	2020	NSO responds to David Kaye	2020		
276	276W20	NSO website	2020	NSO Group Launches Drone Defense System, Eclipse (Document (22	6/11/2020		
277	277W20	NSO website	2020	NSO Group welcomes the court's rejection of Amnesty Internation	7/13/2020		
278	278W20	NSO website	2020	NSO group presents its life-saving search & rescue solutions at	10/21/2020		

(*Continued*)

Continued.

No.	Code	Type	Year	Title	Date	Source	Link
279	279W20	NSO website	2020	NSO Group has been ranked #14 on the Dun & Bradstreet (Israel)	10/26/2020		
280	280W20	NSO website	2020	NSO Expands to Arava Region - NSO Group (Document (17), Pos. 1)	12/8/2020		
281	281W21	NSO website	2021	NSO Entering Drone Market with Eclipse-Advanced and Innovative	9/5/2021		
282	282W21	NSO website	2021	NSO Group has been named one of the 50 most-desirable workplace	1/21/2021		
283	283W21	NSO website	2021	NSO Group's Commitment to Transparency and Solid Governance (D	4/29/2021		
284	284W21	NSO website	2021	NSO GROUP UNVEILS THE INDUSTRY'S FIRST "TRANSPARENCY AND RESPON	6/30/2021		
285	285W21	NSO website	2021	Following the publication of the recent article by Forbidden St	7/18/2021		
286	286W21	NSO website	2021	Enough is enough!	7/21/2021		
287	287W21	NSO website	2021	In response to recent publications	11/3/2021		
288	288W21	NSO website	2021	Following today's media reports, NSO Group wishes to clarify th	12/3/2021		
289	289W21	NSO website	2021	הודעה על פרסום דוח שקיפות	2021		
290	290W22	NSO website	2022	BIG NEWS! NSO GROUP NAMED TIME'S LIST OF 2022 TIME100 MOST INFL	4/11/2022		
291	291R19	NSO's reports	2019	External Whistleblowing Policy	9/1/2019	NSO	
292	292R19	NSO's reports	2019	Human Rights Policy	9/1/2019	NSO	
293	293R21	NSO's reports	2021	Transparency and responsibility report	6/30/2021	NSO	