DECEMBER 2022

Meta Policy Recommendations for Tackling the Surveillance-for-Hire Industry

December 15, 2022
David Agranovich, Director, Threat Disruption
Eneken Tikk, Security Policy Manager for Security Governance

Meta

Introduction

Meta builds technologies that help people connect, find communities and grow businesses. To keep people safe and build positive social experiences online, it is essential for us to keep their accounts secure and enable them to make choices around how their data is used.

We've been investigating and taking action against commercial spyware vendors, the so-called surveillance-for-hire industry, for years. Since we published our first threat research about this challenge last year, we have taken down more of these entities and, whenever possible, worked with researchers and our industry partners to tackle this growing challenge from multiple angles. Our goal has been threefold: first, to protect people using our services; second, disrupt surveillance-for-hire across our apps; and third, to enable cross-industry and cross-societal response to the problem by sharing detailed technical threat indicators to enable additional security research.

Surveillance-for-hire technology undermines the privacy of targeted individuals and can be used to violate fundamental civil and human rights. The industry creating these tools has grown exponentially over the past two decades. Reporters Without Borders highlighted the growth of online surveillance as a danger for journalists, bloggers, citizen-journalists and human rights defenders in 2013.[1] Since then, several companies have taken action against cyber mercenaries.[2][3][4]

Today, we published our second threat report focusing on the spyware industry, where we share a number of updates including the latest trends and tactics that stood out to us in our investigations and disruptions of these private surveillance entities in 2022. In addition to sharing our threat research findings in the report, we're also publishing this Policy Paper where we provide a broad set of recommendations on what levers and approaches different stakeholders – the governments, the surveillance-for-hire industry, civil society and technology platforms whose products and services are targeted – can take to increase security, safety and trust online.

---

[1] http://surveillance.rsf.org/en/wp-content/uploads/sites/2/2013/03/enemies-of-the-internet_2013.pdf
[2] See WhatsApp's "Why WhatsApp is pushing back on NSO Group hacking", October 2019, available at https://www.washingtonpost.com/opinions/2019/10/29/why-whatsapp-is-pushing-back-nso-group-hacking/
[3] See Microsoft's "Response to the United Nations (UN) Working Group on the Use of Mercenaries," October 2021, available at https://www.ohchr.org/sites/default/files/Documents/Issues/Mercenaries/WG/CyberMercenaries/MSFT-Response.pdf
[4] See Microsoft's "Cyber mercenaries don't deserve immunity," December 2020, available at https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/

These recommendations are grounded in our investigations conducted over the years and describe a set of the interventions we believe would meaningfully constrain the abuse by these types of spyware services.

The Adversarial Threat Disruption Model

Since 2017, Meta has taken down more than 200 covert influence operations, in addition to cyber-espionage campaigns, spam and scam networks, mass reporting and brigading operations, and adversarial networks seeking to abuse our services. These takedowns are part of a strategy we first deployed against Russia's clandestine influence activity in 2017 that combines on-platform enforcement actions like network takedowns, legal action, public disclosure and attribution, and cross-industry information sharing to enable a wider defense response.

A key part of this strategy involves using investigations by Meta's security teams to inform threat research by other technology companies, open source researchers and governments, with each having distinct measures and dedicated teams to counter and deter adversarial activity.

Our December 2021 Surveillance-for-Hire report was designed to apply this model to a new class of threat actors: spyware vendors selling sophisticated surveillance and hacking capabilities to anyone willing to pay. In this Policy Paper on the spyware industry, we're building on the impact of our initial enforcements and analysis to expand the focus and consider a broad spectrum of levers our society can use to constrain and meaningfully regulate the abuses of this industry.

Combatting the Surveillance-for-Hire Industry

Private social media companies, including Meta, can take a series of measures to tackle the problem of global surveillance. These include:

- **Investigations and threat disruptions:** Our security teams identify and counter adversarial networks that seek to target people on our apps with spyware and other abusive targeting.
- **Technical safeguards against scraping and other abusive activities.** Our dedicated team of more than 100 people includes data scientists, analysts and engineers, and is focused on combating unauthorized scraping across our services, including detecting, blocking and deterring scraping.
- **Public reporting:** We publish our findings to enable our industry peers, researchers, governments and the public to improve our collective understanding of threat actor behavior and to raise costs on spyware vendors. By including technical indicators - including malware hashes, victimology and malicious web domains - we hope to enable our industry peers and open-source researchers to build on this work and find threat actors across the internet. Our disclosures serve a second, critical purpose: forcing bad actors that try to hide their activity into the light, and blow the cover on clandestine operations attempting to abuse ours and others' services. We want threat actors to think twice about the cost of being discovered, should they target people through our technologies.
- **Alerts and education:** Whenever appropriate, we alert people who we believe were targeted by spyware networks that we take down to help them take steps to protect their accounts on our apps. Our goal is to raise awareness about how these activities may manifest online so that people, particularly among the most targeted groups like journalists, activists and dissidents, can change their security posture against spyware.
- **Legal action:** We've issued cease and desist letters to entities that violate our terms and policies, putting them on notice that their continued targeting of our people who use our technologies is not acceptable.
- **Expert briefings and testimony:** We share our analyses and findings into this constantly evolving threat with security researchers, industry peers and policymakers to help ensure that regulation and legislation in this area is informed by expert perspectives.

- **Transparent pathways for legal requests for information by law enforcement:** We maintain authorized channels where government agencies can submit lawful requests for information, rather than resorting to the surveillance-for-hire industry that indiscriminately sells these services to anyone willing to pay, including known bad actors. These channels are designed to safeguard due process and we report the number and the origin of these requests publicly so that people worldwide have the full picture.
- **Cooperation with industry peers:** The cross-societal nature of the problem means that no single player can solve this issue on their own, which requires stronger defenses to protect people across the internet. Where appropriate, we share information with industry peers on surveillance threats and collaborate with our industry peers on the development of principles to guide the regulation of this space.
- **Partnering with civil society:** We work with and welcome broader partnerships with civil society, including security and privacy researchers and digital rights scholars, on joint strategies to protect people from being targeted by spyware. These strategies focus on educating the public on how to identify and protect against spyware and investing in accessible technical tools to help people secure their accounts and devices, including non-experts.

We also have seen a number of notable emerging policy frameworks by governments and multinational organizations aimed at addressing the risks posed by spyware.

For instance, in 2021, the US Department of State adopted a framework for US companies to consider the potential that a product or service can be misused to violate or abuse human rights. This framework guides companies to implement the UN Guiding Principles on Business and Human Rights, as well as the Organization for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises. In particular, these guidelines are directed at companies willing to undertake a human rights review where the US government does not require an authorization for export.[5]

In addition, the European Parliament's Pegasus Inquiry issued several recommendations for improving regulation and oversight of the surveillance-for-hire industry.

[5] Department of State, Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities, October 2020, https://www.state.gov/wp-content/uploads/2020/10/DRL-Industry-Guidance-Project-FINAL-1-pager-508-1.pdf

Policy Recommendations For a Wider Response

Surveillance-for-hire is an inherently cross-societal problem that demands a whole-of-society approach. While the levers we've outlined above have allowed us collectively to make progress, as a society we need to see greater engagement by a wider range of responders, including regulators and governments, tech platforms and civil society, and the surveillance companies and their clients themselves if we're to make more advances in protecting people online from indiscriminate abuse. Our recommendations include:

GOVERNMENT OVERSIGHT & REGULATION OF PRIVATE SFH INDUSTRY

- Regulate the activities of surveillance-for-hire companies, including through imposing restrictions or bans on the sale of surveillance software such as malware.
- Establish accountability frameworks for surveillance-for-hire companies, such as those principles within the EU data protection laws, which would require private surveillance-for-hire companies to notify surveilled individuals and require review and oversight of compliance.
- Establish institutions and proceedings that help targets of the surveillance-for-hire vendors to seek legal recourse from these companies.
- Use export control lists and dual-use regimes to limit the export of domestic technology to the surveillance-for-hire industry.
- Leverage existing authorities, such as the Magnitsky Act, to impose consequences on the development or use of surveillance-for-hire technology to conduct or enable human rights violations.[6]
- Build multi-stakeholder alliances to raise awareness of the surveillance-for-hire threats and develop cooperation and coordination mechanisms (e.g., Export Controls and Human Rights Initiative) for governments, industry and civil society to counter the spyware industry.
- Develop and publish restrictions on government procurement, use and testing of surveillance-for-hire technologies.
- Increase transparency by creating a process for citizens to obtain information on surveillance targeting and regularly disclosing details of government procurement, use and testing of surveillance-for-hire technologies.

[6] Magnitsky Act, https://www.wyden.senate.gov/imo/media/doc/Global%20Magnitsky%20Sanctions%20Letter%20to%20Sec.%20Yellen%20&%20Blinken.pdf

SURVEILLANCE-FOR-HIRE INDUSTRY

- Adopt “know your customer” protocols and non-sale lists to limit the sale of spyware tools to entities with a high risk of abuse.
- Provide transparency into the use of spyware services, including who the customers are and how they deploy these tools, to enable accountability and inform regulation.

PHILANTHROPY AND CIVIL SOCIETY

- Advocate for meaningful regulation of surveillance-for-hire technology and the companies that develop it.
- Develop and fund campaigns raising public awareness of the importance of preventing device and online account compromise.
- Increase accessibility to forensic tools for suspected compromised devices, including by making existing services more user-friendly for non-experts.