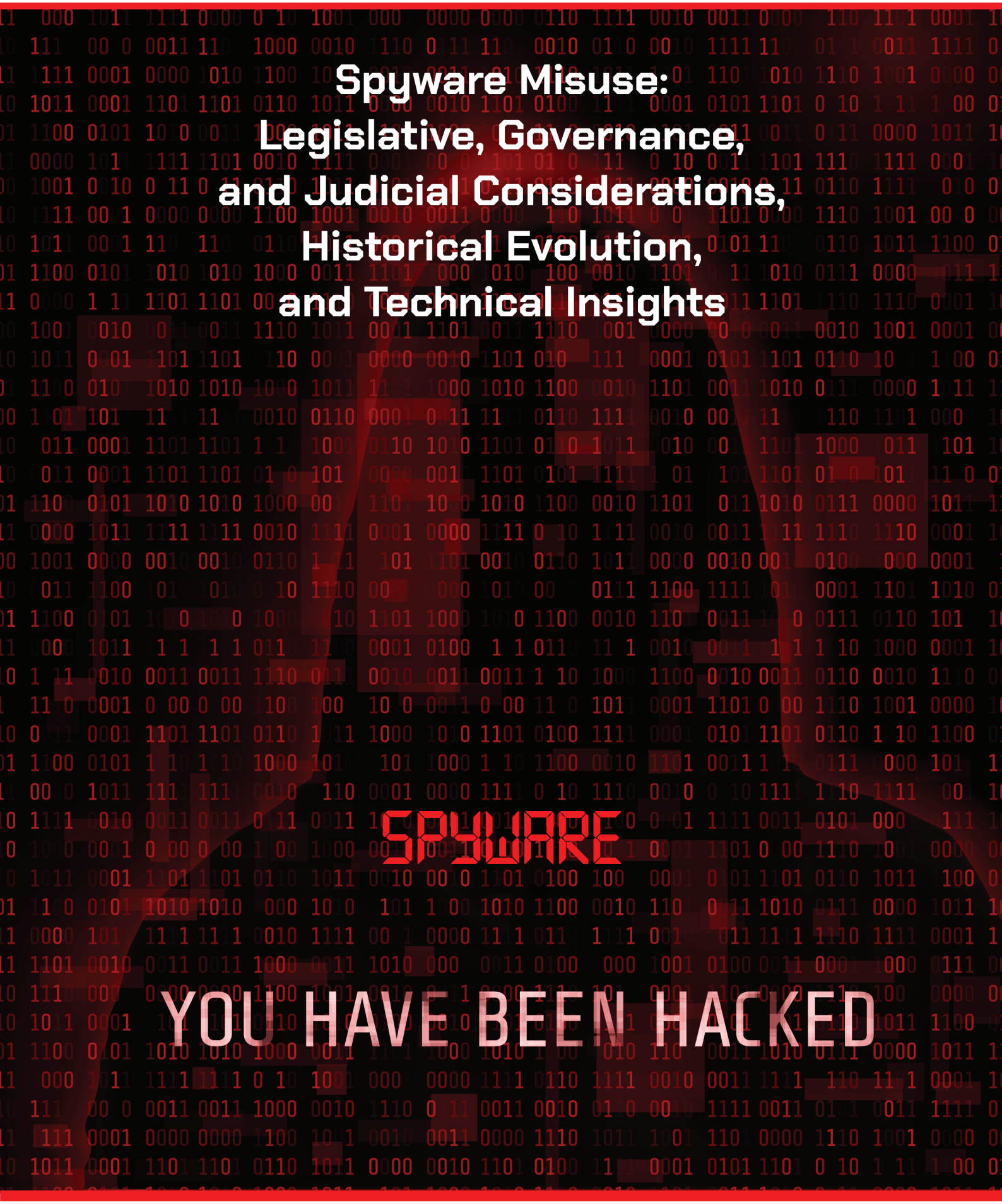
CGS
CENTRE FOR GLOBAL STUDIES

A Program of Parliamentary Assembly of the Mediterranean

Spyware Misuse: Legislative, Governance, and Judicial Considerations, Historical Evolution, and Technical Insights



www.cgspam.org

Report:

Spyware Misuse: Legislative,

Governance, and Judicial Considerations,

Historical Evolution, and Technical Insights

San Marino, 10 December 2025

Disclaimer: This document is prepared by the researchers of the Centre for Global Studies (CGS) of the Parliamentary Assembly of the Mediterranean (PAM) in San Marino in their personal capacity. The opinions expressed in the note are the authors' own and may not reflect the views of PAM.

Index

Index of Figures and Tables

Executive Summary

The report "Spyware misuse: Legislative, Governance, and Judicial considerations, Historical evolution, and Technical insights" prepared by the Center for Global Studies (PAM-CGS), addresses the threat represented by the misuse of spyware technologies in the general context of illegal surveillance activities and cyber intrusions. CGS is a special program of the Parliamentary Assembly of the Mediterranean (PAM), operating in cooperation with the Counter-Terrorism Executive Directorate (CTED) of the United Nations Security Council.

Spyware has recently emerged as a prominent topic in geopolitical discourse, surpassing earlier monitoring methods by enabling the manipulation of communications and records to incriminate and extort targets. This report, primarily directed at legislators and government officials, examines the impact of the misuse of spyware technologies, originally designed to enhance counter-terrorism efforts, on individuals. It provides a comprehensive analysis of the evolution of these technologies, their consequences, and the ongoing regulatory framework governing them.

On 14 January 2025, the members of the United Nations Security Council convened, for the first time, an Arria-formula meeting, entitled "Commercial Spyware and the Maintenance of International Peace and Security," to address the threat posed by commercial spyware.[1] The current historical phase is particularly delicate and the meeting examined how malware is infiltrating diplomats' devices. According to the US Representative, in the States, the National Defense Authorization Act[2] for fiscal year 2025 includes a measure to better protect diplomats from spyware technology. The Polish Representative emphasized the legislative initiatives in his country: a commission of the Polish Senate[3] declared that the government's use of spyware is illegal. The Greek Representative mentioned the law that reorganizes the secret services in his country and prohibits the sale of spy software.[4] Shane Huntley, senior director of Google's Threat Analysis Group, told the participating diplomats that his group is currently actively monitoring about 40 commercial surveillance system providers: Huntley said that 20 of the 25 zero-day exploits (infections that take advantage of previously unreported software bugs) that Google's Threats Analysis Group discovered in 2023 were used by spyware companies.[5] John Scott-Railton, a researcher at the University of Toronto's Citizen Lab, pointed out that Europe is the epicenter of spyware abuse and is home to an increasing number of spyware

[1] United Nations. (14 January 2025). Security Council Arria-formula meeting on commercial spyware and the maintenance of international peace and security [Video]. UN Web TV. Retrieved from https://webtv.un.org/en/asset/k1j/k1jteho6fm

[2] U.S. Congress. (23 December 2024). H.R.5009 – Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025. Congress.gov. Retrieved from https://www.congress.gov/bill/118th-congress/house-bill/5009/text

[3] Franceschi-Bicchierai, L. (8 September 2023). Polish Senate says use of government spyware is illegal in the country. TechCrunch. Retrieved from https://techcrunch.com/2023/09/08/polish-senate-says-use-of-government-spyware-is-illegal-in-the-country/

[4] Smith, H. (9 December 2022). Greece passes intelligence bill banning the sale of spyware. The Guardian. https://www.theguardian.com/world/2022/dec/09/greece-passes-intelligence-bill-banning-the-sale-of-spyware

[5] Huntley, S. (6 February 2024). Buying spying: How the commercial surveillance industry works and what can be done about it. Google. https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/

companies: a recent TechCrunch investigation[6] showed how Barcelona has become a hub for spyware companies recently.

The panorama of spyware technologies shows the need to strengthen multilateral cooperation at the inter-state, regional and global levels. The growing complexity of the tools, the market numbers and the impacts of the malicious use of spyware technologies require a cooperation that tends to reinforce the good practices introduced by European legislation and the operational principles that characterize the evolving Pall Mall Process, within the framework of the United Nations Charter and in line with the work carried out in recent years by the United Nations and other international organizations; in particular, it is crucial to mention the process, which PAM contributes to strengthen, of the Pact for the Future[7] adopted by the United Nations on 22 September 2024. The impacts of spyware go beyond the borders of nation states and affect all institutional, economic and social spheres within individual countries: if it is necessary to reiterate the importance of safeguarding the human rights of individuals and populations, coordination between police forces, judicial and intelligence systems is very important. Likewise, it is crucial to study the evolution of spyware ecosystems at a global level. Dialogue with and between parliaments is strategic for coordinating increasingly effective legislative and governance actions.

As espionage tools evolve, legislation must also evolve accordingly. On 15 May 2025, the Dutch Government approved a new law that expands existing espionage regulations, making the disclosure of state secrets a criminal offence. Under the new law, the disclosure of sensitive unclassified information that harms Dutch interests may also lead to criminal charges.[8]

Issues relating to the misuse of spyware are being reported to the judicial authorities. On 6 May 2025, a federal jury in California ordered NSO Group, the maker of Pegasus, to pay Meta $167.25 million for hacking 1,400 users on WhatsApp. Meta's complaint dates back to 2019. Apple has also sued NSO Group for targeting iPhone users with Pegasus.[9] Meta said that this decision represents a fundamental deterrent.[10]

This report includes a very robust technical annex that helps to understand how spyware tools work. The pervasiveness of such tools requires technologies that are constantly being adapted. After exploring the recent history of spyware, the report highlights: the importance of digital security in the

[6] Franceschi-Bicchierai, L. (13 January 2025). How Barcelona became an unlikely hub for spyware startups. TechCrunch. https://techcrunch.com/2025/01/13/how-barcelona-became-an-unlikely-hub-for-spyware-startups/

[7] United Nations. (22 September 2024). Pact for the Future. https://www.un.org/en/summit-of-the-future/pact-for-the-future

[8] Alexander Martin. (20 May 2025). Netherlands Law Criminalizes Cyber-Espionage. The Record. https://therecord.media/netherlands-law-criminalizes-cyber-espionage

[9] Robertson, A. (13 May 2025). Meta wins lawsuit against NSO Group over Pegasus WhatsApp hack. The Verge. https://www.theverge.com/news/662242/meta-nso-group-pegasus-whatsapp-hack-damages

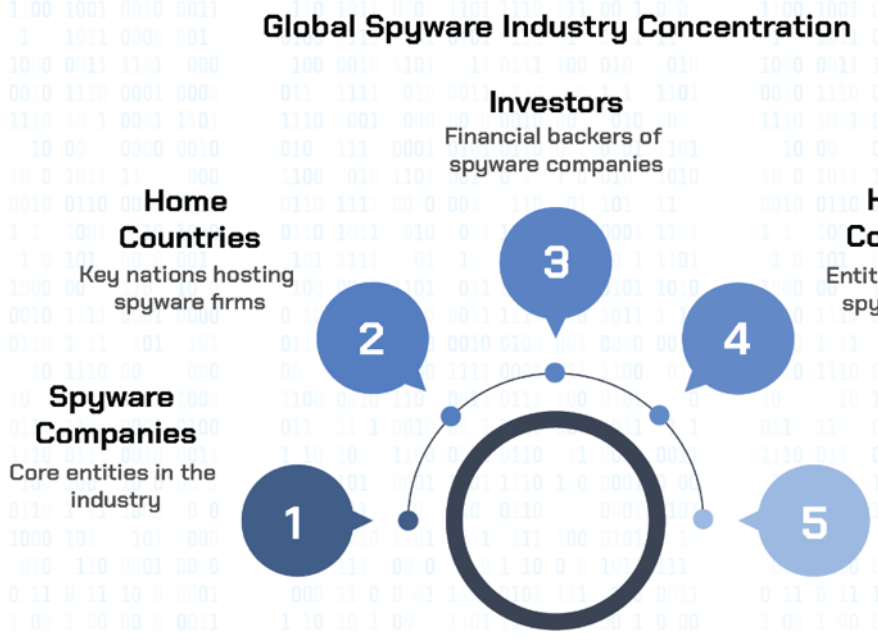
[10] Meta. (6 May 2025). Winning the fight against spyware merchant NSO. https://about.fb.com/news/2025/05/winning-the-fight-against-spyware-merchant-nso/

digital age (in particular, the need for robust data protection measures); the need for continuous vigilance and proactive measures to protect against the ever-evolving threat of spyware; and the risks associated with various forms of spyware, including keyloggers, adware and mobile spyware. It also explores the dangers posed by social media, online gaming and outdated mobile devices. The section on hidden cameras and security cameras highlights the vulnerabilities and potential misuse of these devices for unauthorized surveillance, the proliferation of affordable tracking devices and their implications for privacy. It includes a case study on the misuse of Ring cameras, emphasizing the importance of robust security measures; the emerging trend of smartwatches and rings and their potential for unauthorized tracking; recommendations for protection against spyware, including best practices for mobile security, email security and the use of antivirus programmes. It emphasizes the importance of multi-factor authentication (MFA) and offers detailed guidelines for improving device security.

Introduction

1. In recent years, there has been a rapid and exponential development of the technological capabilities of governments and companies to intercept, extract, filter, store, analyze, and disseminate strategic data produced by individuals exposed in relevant public roles and institutions. Tools for analyzing information have improved as a result of machine learning and algorithmic design. These are technological advances in which misuse represents a direct threat to the guarantees that protect the right to privacy, as well as other human rights. Faced with these risks, the legal debate has intensified on the role of international law, and in particular international human rights law and international humanitarian law, in responding to these applications.
2. Research by the Georgetown Law Technology Review (January 2024)[11] defines spyware as a *secretive, new weapon that is steadily challenging the global balance of power*. And emphasizes that *authoritarian and democratic regimes alike are clamoring for commercially available "spyware" technologies that enable them to surreptitiously track and monitor the private communications of almost anyone, anywhere in the world*.

Figure 1: Geographical Distribution of Private Spyware Companies[12]



[11] Silberman, M. (January 2024). Policing Pegasus: The promise of U.S. litigation for commercial spyware accountability. Georgetown Law Technology Review. Retrieved from https://georgetownlawtechreview.org/policing-pegasus-the-promise-of-u-s-litigation-for-commercial-spyware-accountability/GLTR-01-2024/

[12] Figure 1: Graph and sources compiled by the GCS research team. Note. Adapted from "The Global Surveillance Industry," by Privacy International, (7 December 2016). Retrieved from https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

3. In several countries, the misuse of spyware is generating problems at a systemic level and can lead to critical situations within state institutions and between some of them: this misuse crosses over into almost all institutional and economic spheres. A recent position statement by the Italian Data Protection Authority[13] emphasizes the seriousness and sensitivity of the misuse of spyware technologies: there is a need for strict regulations governing the progress and use of powerful surveillance tools, as well as investment in ethical governance and transparency, and public awareness campaigns. The misuse of spyware technologies must lead national governments to identify, also through adequate regulation, the right balance between security and privacy.[14]
4. Originally adopted as tools to strengthen national security and to counter terrorism more effectively, spywares are often used to attack political dissidents, activists, human rights defenders, journalists, diplomats, representatives of the armed forces,[15] politicians, institutional representatives, and public officers. With particular reference to activists, dissidents or human rights defenders abroad, a study by the British Institute of International and Comparative Law[16] analyzes the practice of transnational digital repression: the impact is particularly serious because this practice erodes human rights, the spaces of democracy, the rule of law, and the targeted communities. An aspect that is not given much consideration, with many ethical and legal consequences, concerns the use of digital surveillance in the enforcement of immigration laws: a blog by the Immigration and Human Rights Law Review of the University of Cincinnati[17] considers the issue from the point of view of the potential violation of constitutional protections.
5. According to Carnegie's global inventory of commercial spyware and digital forensics,[18] between 2011 and 2023, seventy-four governments have entered contracts with commercial companies to obtain spyware or digital forensics technology.

[13] Asokan, A. (18 February 2025). Italian privacy agency warns against unlawful spyware use. Archyde. Retrieved from https://www.archyde.com/italian-privacy-agency-warns-against-unlawful-spyware-use/.
[14] Erhayel, H. (24 July 2024). Striking the balance between privacy and security: The case of spyware. Future Europe Journal. Retrieved from https://feu-journal.eu/issues/issue-5/striking-the-balance-between-privacy-and-security-the-case-of-spyware/
[15] NextGov (2024, December 9). FY2025 NDAA targets spyware threats to U.S. diplomats, military devices. Retrieved from: https://www.nextgov.com/cybersecurity/2024/12/fy2025-ndaa-targets-spyware-threats-us-diplomats-military-devices/401538/
[16] Anstis, S. (12 December 2023). Regulating transnational dissident cyber espionage. International and Comparative Law Quarterly. Retrieved from https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/regulating-transnational-dissident-cyber-espionage/8662095ACD8DB0BB32392E1BAD7DEFF6
[17] Fernandez, K. (17 January 2025). ICE, spyware, and the Constitution: A call for reform in immigration enforcement. Immigration and Human Rights Law Review. Retrieved from https://lawblogs.uc.edu/ihrlr/2025/01/17/ice-spyware-and-the-constitution-a-call-for-reform-in-immigration-enforcement/
[18] Feldstein, S., & Kot, B. C. H. (14 March 2023). Why does the global spyware industry continue to thrive? Trends, explanations, and responses. Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en

A strategic overview

6. In a report dated 15 February 2022, the European Data Protection Supervisor[19] emphasized the impact of the misuse of spyware technologies, in particular on the rights to privacy and data protection. From the introduction: *As the specific technical characteristics of spyware tools like Pegasus render controlling over their use very difficult, we must rethink the entire existing system of safeguards established to protect our fundamental rights and freedoms, which are endangered by these tools.*
7. The report "United Nations Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism. Global Regulation of the Counter-Terrorism Spyware Technology Trade: Scoping Proposals for a Human-Rights Compliant Approach,"[20] dated April 2023, emphasized that *recent leaks-most notably in respect of the widespread use of the Pegasus spyware technology-show that, whatever the justification for the intended application of this technology, something is fundamentally wrong in practice. Intrusive secret technology that monitors people's digital communications and other information, like where they are, how long they communicate, who they talk to, and more, has spread worldwide without proper oversight and threatens human rights significantly.*
8. In May 2023, the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent spyware (PEGA) adopted its final report and recommendations[21] after a year-long investigation into the abuse of spyware in the EU. MEPs condemned spyware abuses that aim to intimidate political opposition, silence critical media, and manipulate elections. On 15 June 2023, the European Parliament adopted a resolution on the reforms needed to curb the abuse of spyware.[22] Guidelines can be found in Table 1.[23]

[19] European Data Protection Supervisor. (15 February 2022). Preliminary remarks on modern spyware. European Data Protection Supervisor. Retrieved from https://www.edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf

[20] United Nations Special Rapporteur on Counter-Terrorism. (April 2023). Position paper on global regulation of counter-terrorism spyware technology trade. Office of the High Commissioner for Human Rights. Retrieved from https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf

[21] European Parliament. (June 2023). PEGA Committee final report. Media Freedom Resource Centre. Retrieved from https://www.rcmediafreedom.eu/Resources/Reports-and-papers/PEGA-Committee-final-report

[22] European Parliament. (15 June 2023). Spyware: MEPs call for full investigations and safeguards to prevent abuse. European Parliament News. Retrieved from https://www.europarl.europa.eu/news/en/press-room/20230609IPR96217/spyware-meps-call-for-full-investigations-and-safeguards-to-prevent-abuse

[23] This table, presented on page 13, summarizes the key guidelines adopted by the European Parliament in its June 2023 resolution on reforms to prevent the abuse of spyware within the EU. These recommendations stem from the final report of the PEGA Committee (Committee of Inquiry to investigate the use of Pegasus and equivalent spyware) and aim to ensure that spyware use is strictly regulated, transparent, legally justified, and subject to independent oversight. Each guideline is grouped by thematic category for clarity and policy relevance.

9. In February 2024, the Annual Threat Assessment of the U.S. Intelligence Community[24] clearly addressed the issue of the misuse of spyware: *During the next several years, governments are likely to exploit new and more intrusive technologies including generative AI for transnational repression. From 2011 to 2023, at least 74 countries contracted with private companies to obtain commercial spyware, which governments are increasingly using to target dissidents and journalists.*
10. The report "Buying Spying: How the commercial surveillance industry works and what can be done about it" by Google's Threats Analysis Group[25] (February 2024) notes that, even if the use of spyware normally only affects a small number of human targets at a time, its impact spreads to society because it increases the threats to freedom of speech, freedom of the press, and the integrity of elections all over the world.
11. The report "Mythical Beasts and Where to Find them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights," produced by the Atlantic Council (4 September 2024)[26] aims to help fill a gap in the public debate on the proliferation of spyware by identifying the connections between 435 entities in forty-two countries in the global spyware technology market. The network is complex: the suppliers are in fact related to investors, holding companies, and partners often belonging to different jurisdictions. The report "Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights" provides an analysis of the data (from 1992 to 2023, therefore not exhaustive). Some trends remain constant: 1) serial entrepreneurship among multiple suppliers; 2) partnerships between spyware and surveillance hardware suppliers; 3) regularly changing supplier identities; 4) strategic leaps across jurisdictions; and 5) cross-border capital flows that feed this market.
12. In September 2024, several civil society organizations have pointed out[27] that the European Media Freedom Act[28] does not provide the necessary legal basis to counter the misuse of spyware technologies against journalists. The same civil society organizations have been calling for greater

[24] Office of the Director of National Intelligence. (5 February 2024). 2024 annual threat assessment of the U.S. intelligence community. Office of the Director of National Intelligence. Retrieved from https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf
[25] Huntley, S. (6 February 2024). Buying spying: How the commercial surveillance industry works and what can be done about it. Google Threat Analysis Group. Retrieved from https://blog.google/threat-analysis-group/commercial-surveillance-vendors-google-tag-report/
[26] Roberts, J., Herr, T., Bansal, N., & Messieh, N., with Taylor, E., Le Roux, J., & Gelava, S. (4 September 2024). Mythical beasts and where to find them: Mapping the global spyware market and its threats to national security and human rights. Atlantic Council. Retrieved from https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/
[27] Center for Democracy and Technology. (3 September 2024). Civil society joint statement on the use of surveillance spyware in the EU and beyond. Center for Democracy and Technology. Retrieved from https://cdt.org/insights/civil-society-joint-statement-on-the-use-of-surveillance-spyware-in-the-eu-and-beyond/
[28] European Union. (15 April 2024). Regulation (EU) 2024/1083 of the European Parliament and of the Council of 15 April 2024 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. EUR-Lex. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1083

verification of member states compliance with the ePrivacy[29] and Law Enforcement[30] directives and the Dual-Use Regulation,[31] with infringement proceedings for countries where the use of spyware violates them. On 13 December 2024, the Electronic Privacy Information Center, together with 13 civil society organizations, sent a letter[32] to the Polish Presidency of the Council of the European Union to demand decisive action against the misuse of spyware technologies.

13. Many states have sought to control exports of spyware to help prevent transfers of cyber-surveillance tools, including software, that could allow human rights violations or pose a threat to national security. These controls have been introduced through the Wassenaar Arrangement,[33] the European Union and national control lists,[34] and comprehensive control in the EU dual-use regulation. In October 2024, the European Union published a new set of guidelines[35] to help exporters comply with the controls.
14. In its 2024 report (March 2025), the "Platform to promote the protection of journalism and safety of journalists" of the Council of Europe raised the issue of freedom of the press and digital security of journalists being threatened by the use of advanced spyware technologies:[36] *Media freedom and the digital security of journalists across Europe continued to be threatened by the ongoing use of advanced spyware technology to surveil journalists and media actors. In 2023, new cases involving journalists being spied on were documented, while accountability for previous use of surveillance technology against media continues to prove evasive. While a landmark report by the European Parliament's Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance*

[29] European Union. (19 December 2009). Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). EUR-Lex. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02002L0058-20091219

[30] European Union. (27 April 2016). Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data. EUR-Lex. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L0680

[31] European Union. (20 May 2021). Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 on the control of exports, brokering, technical assistance, and transit of dual-use items. EUR-Lex. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32021R0821

[32] Electronic Privacy Information Center. (13 December 2024). EPIC, coalition urge EU Polish presidency to prioritize action against spyware misuse. Electronic Privacy Information Center. Retrieved from https://epic.org/epic-coalition-urge-eu-polish-presidency-to-prioritize-action-against-spyware-misuse/

[33] Control lists - The Wassenaar Arrangement. (5 December 2024). The Wassenaar Arrangement. https://www.wassenaar.org/control-lists/

[34] European Commission. (2 October 2024). Regulation (EU) 2024/1143 of the European Parliament and of the Council on geographical indications for wine, spirit drinks and agricultural products, as well as traditional specialties guaranteed and optional quality terms for agricultural products, amending Regulations (EU) No 1308/2013, (EU) 2019/787 and (EU) 2019/1753. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52024XC05881&qid=1736440924065

[35] European Commission. (16 October 2024). Regulation (EU) 2024/2659 of the European Parliament and of the Council on the application of Article 101 (3) of the Treaty on the Functioning of the European Union to categories of vertical agreements and concerted practices. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202402659

[36] Council of Europe. (5 March 2025). Safety of Journalists platform 2024 report: Serious concern about the use of spyware against journalists, abusive lawsuits, and journalists in exile. Council of Europe. Retrieved from https://www.coe.int/en/web/portal/-/safety-of-journalists-platform-2024-report-serious-concern-about-the-use-of-spyware-against-journalists-abusive-lawsuits-and-journalists-in-exile

spyware (PEGA) shone a spotlight on the use of spyware technology across the bloc and provided first-of-a-kind recommendations for tackling the abuse of the technology, investigations within certain EU member states into spyware use against journalists both lacked transparency or legal clarity and/or failed to provide remedy to journalists for the abuse. On that occasion, the former Secretary General of the Council of Europe, Marija Pejčinović Burić, declared, *the Safety of Journalists Platform report shows the increasing risks and obstacles that journalists and media face in Europe. Determined action from states is necessary to protect journalists and counter threats to media freedom, such as abusive lawsuits and illegal surveillance.*

Table 1: European Parliament's Structured Guidelines on the Responsible Use and Oversight of Spyware (June 2023 Resolution)

No.	Guideline	Category
A. Use and Authorization of Spyware		
1	Spyware should only be used to protect national security and must get approval from a fair and independent judge beforehand.	Use & Authorization
2	Approval for using spyware must only be for national security and must also come from a fair and independent judge beforehand.	Use & Authorization
3	The approval must clearly state how long and what devices can be accessed, and it should not last longer than necessary to get useful information for the investigation.	Use & Authorization
4	Authorization must specifically cover the scope and duration for each device accessed and may not exceed the time required to obtain a result useful to the investigation.	Use & Authorization
5	States must identify a specific list of serious crimes that pose a real threat to national security, and spyware can only be used against people who have committed these crimes.	Use & Authorization
B. Legal Protections and Sensitive Data		
6	Particularly sensitive data in certain categories or relating to specifically protected relationships (for example, lawyer-client privilege) or rules on the determination and limitation of criminal liability relating to freedom of the press or freedom of expression must not be obtained through spyware unless there are grounds relating to involvement in criminal activities or matters of national security.	Legal Limits & Protections
C. Transparency and Public Oversight		

7	States must publish the number of approved and rejected surveillance requests, with the type and purpose of the investigation, and record each case anonymously in a national register with a unique identifier.	Transparency & Reporting
8	The EU should work together openly to ensure the safety of its citizens, and the reliability of evidence collected through spyware in cases that cross borders.	Transparency & Reporting
D. Rights and Remedies for Individuals		
9	The right to information of the person under surveillance must be guaranteed, as well as that of third parties who were not the direct target of the surveillance, but who have suffered its effects (interception of personal data via spyware).	Rights of Individuals
E. Independent Oversight and Accountability		
10	Effective, binding, and independent ex-post surveillance by responsible and autonomous bodies is necessary.	Oversight & Accountability
11	Individuals who have been directly or indirectly subjected to surveillance must be guaranteed effective means of recourse from independent supervisory bodies. In the event of violations, the application of adequate sanctions must be envisaged.	Oversight & Accountability
F. Data Management		
12	During the surveillance, the authorities must delete any data not relevant to the authorized investigation. At the end of the surveillance, all data collected, and any related documents must be deleted.	Data Handling & Deletion
G. Access and Use Restrictions		
13	The information obtained through spyware must be accessible only to authorized authorities and exclusively for the purposes of a specific operation.	Access Control
H. EU Legal Compliance and Marketing		
14	Can be developed, used and marketed within the Union only spyware designed in accordance with European Union law.	Legal Compliance
I. Procurement and Use by Public Authorities		

15	This software can only be purchased by public authorities, identified within a closed list, whose responsibilities include investigations into crimes or the protection of national security for which the use of spyware can be authorized.	Procurement Control
J. Defining National Security Boundaries		
16	The concept of national security must be circumscribed, in order to prevent abuses that would justify a disproportionate use of spyware, also based on the case law of the Court of Justice of the European Union according to which the reference to national security cannot be interpreted as an unlimited derogation from the application of EU rules and should in any case require a clear justification.	Definition & Scope
K. Implementation of Existing Laws		
17	The application of current legislation must be improved, considering its lack of or incomplete implementation (in particular, the anti-money laundering directive, the directive on data protection in police and judicial activities, the rules on procurement and the directive on the protection of whistleblowers).	Implementation
L. EU-US Strategic Cooperation		
18	The European Parliament proposes the adoption of a joint EU-US strategy on spyware, including a blacklist of spyware vendors whose tools have been misused or are at risk of misuse by foreign governments to maliciously surveil government officials, journalists, and members of civil society and who operate against the security and foreign policy of the Union.	International Strategy

International Efforts

15. In general terms, much work has been done at the international level on combating cybercrime. A decisive step forward was the Council of Europe's Budapest Convention, which has been in force since 2001.[37]
16. Starting in 2021, UN OHCHR has called on States to impose a global moratorium on surveillance technologies (sale and transfer) until an effective regulatory framework is established to ensure that these technologies are used in accordance with international human rights standards.[38]

[37] Council of Europe. (July 2025). The Budapest Convention on Cybercrime. Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention

[38] United Nations. (12 August 2021). Spyware scandal: UN experts call for moratorium on sale of 'life threatening' surveillance tech. OHCHR. https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening

17. On 4 October 2023, at the 54th session of the UN Human Rights Council, the United States presented a statement entitled "Heightened Risks Associated with Surveillance Technologies and the Importance of Safeguards in the Use of these Tools." The statement, signed by 59 countries, emphasizes that: *the use of technologies associated with surveillance, including commercial spyware, should not enhance the capacity to violate or abuse human rights and target human rights defenders, journalists, activists, workers, union leaders, political opposition members, and other perceived critics. Such tools should not be used in an arbitrary or unlawful manner to infringe privacy, curb dissent, restrict access to information, or limit the freedoms of expression, peaceful assembly, and association. We call on governments to take steps to ensure the use of these technologies is lawful and responsible, in accordance with states' domestic law and international obligations and commitments. Governments should also establish safeguards that apply to the collection, handling, and disclosure of personal information obtained using these technologies to uphold universal human rights and the rule of law. Governments may incorporate principles such as lawfulness, necessity, proportionality, or reasonableness. Governments should foster transparency, oversight, and accountability and mitigate unlawful or unintended bias in their use of these tools.*[39]
18. On 6 February 2024, on the initiative of the United Kingdom and France, the Pall Mall Process was launched. The final declaration, "The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities,[40] was signed by 27 countries and international organizations, 14 large companies, and 12 representatives of civil society and academia." The declaration indicates that: *The Pall Mall Process will establish guiding principles and highlight policy options for states, industry, and civil society in relation to the development, facilitation, purchase, and use of commercially available cyber intrusion capabilities. This process builds on the whole-of-society approach to cyberspace and acknowledges the importance of public-private partnership and multi-stakeholder in the pursuit of a more secure cyberspace.* The Pall Mall process is a work in progress. On 3 and 4 April 2025, its second conference promoted by the French and British governments, was held in Paris. The Joint Communiqué states: *to date, 21 participating governments have endorsed a Code of Conduct for States, which sets out political commitments and practical recommendations to address the irresponsible use of commercial cyber*

[39] U.S. Mission to International Organizations in Geneva. (4 October 2023). Joint statement on surveillance technologies at the 54th Session of the Human Rights Council. https://geneva.usmission.gov/2023/10/04/joint-statement-on-surveillance-technologies-hrc54/
[40] Foreign, Commonwealth & Development Office. (6 February 2024). The Pall Mall Process: tackling the proliferation and irresponsible use of commercial cyber intrusion capabilities. GOV.UK. https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-c

intrusion capabilities and to promote responsible behavior across the cyber intrusion market.[41] While this Code represents a tangible sign by some countries of their commitment to ensuring effective regulation of digital surveillance tools such as spyware, it does not establish a binding legal standard for States to prevent spyware abuse in their domestic law, nor does it provide a roadmap for ensuring accountability and redress for victims of spyware abuse.[42]

19. The Code of Practice for States, introduced as part of the Pall Mall Process,[43] emphasizes several strategic points. First and foremost, the issue of respect for human rights by both states and private companies is decisive: *We further recall that the United Nations Guiding Principles on Business and Human Rights sets out that States have a duty to protect human rights, that business enterprises have a responsibility to respect human rights, and that States must take appropriate steps to ensure that when business-related human rights abuses occur within their territory and/or jurisdiction, those affected have access to effective remedy, including during the development, facilitation, purchase, transfer and use of CCICs*. Another point regards the complexity and growth of the market for commercial cyber intrusion capabilities (CCICs), which include spyware: *The market for CCICs encompasses a wide variety of cyber intrusion companies offering products and services that are continually evolving and diversifying. The market includes an interconnected ecosystem of researchers, developers, brokers, resellers, investors, corporate entities, operators, and customers, including States. The emergence of new technologies, such as artificial intelligence, although they can enhance cyber defensive capabilities including the detection, response and remediation of malicious cyber incidents, are likely to increase the availability of cyber intrusion tools and services and the threat stemming from their irresponsible use, whilst making them more difficult to monitor and regulate. This growing market vastly expands the potential pool of state and non-state actors with access to CCICs and increases the opportunity for irresponsible use, making it more difficult to mitigate and defend against the threats they pose. These threats, including to security, respect for human rights and fundamental freedoms and the stability of cyberspace, are expected to increase over the coming years*. The Code of Conduct makes a fundamental reference to the relevant international legal framework: *We recall that all United Nations Member States have affirmed by consensus that international law, including customary international law and the principles of sovereignty and non-intervention, apply to the*

[41] Foreign, Commonwealth & Development Office. (4 April 2025). Joint Communiqué of France and the United Kingdom on the Paris Conference of the Pall Mall Process. GOV.UK. https://www.gov.uk/government/publications/joint-communique-of-france-and-the-united-kingdom-on-theparis-conference-of-the-pall-mall-process

[42] Ní Aoláin, F. (9 May 2025). One step forward? Agreement on spyware regulation in the Pall Mall Process. Just Security. https://www.justsecurity.org/113115/agreement-spyware-regulation-pall-mall-process/

[43] Foreign, Commonwealth & Development Office. (n.d.). The Pall Mall Process: Code of Practice for States. GOV.UK. https://assets.publishing.service.gov.uk/media/67f8f85b04146682e61bc867/The-Pall-Mall-Process-Code-of-Practice-for-States.pdf

conduct of States in cyberspace, including in the context of States' regulation and use of CCICs. The pertinent international legal frameworks where applicable in relation to States' regulation of the development, transfer and use of CCICs include, but are not limited to: the United Nations Charter;[44] *international human rights law, including but not limited to the right to freedom of thought, conscience and religion, the right to freedom of opinion, the right to freedom of expression, the right of peaceful assembly with others, the right to freedom of association, and that no one should be subjected to arbitrary or unlawful interference with his privacy, as set out in the International Covenant on Civil and Political Rights*[45] *and other applicable international and regional treaties; international treaties, alongside other applicable regional conventions; and international humanitarian law, with respect to cyber activities carried out with CCICs in the context of an armed conflict*. The attention paid to overcoming the digital divide is very important, as is the focus on global trust and cooperation to strengthen cyber capacity building and resilience: *The actions foreseen under this document sit alongside our common objective to close all digital divides. We recognize the role confidence building measures can play to enable information sharing to address this issue, the importance of cooperation on cyber capacity building, and the necessity of cyber resilience in identifying, preparing, mitigating, responding, recovering, and learning from destructive or disruptive malicious cyber activities. We strongly encourage States, industry, civil society, academia, members of the technical community, and individuals to continue to build greater global cyber capacity for defensive purposes, in line with the cyber capacity building principles set forth in the 2021 OEWG Final Substantive Report.*[46]

20. On 18 March 2024, during the third Summit for Democracy, which was held in Seoul, Republic of Korea,[47] more than 20 countries approved the "Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware." The statement ends with this wish: *Our efforts will allow us to work collectively for the first time as we develop and implement policies to discourage the misuse of commercial spyware and encourage the development and implementation of responsible use principles that are consistent with respect for universal human rights, the rule of law, and civil rights and civil liberties.*[48] During the Arria-formula meeting promoted by the

[44] United Nations. (n.d.). Charter of the United Nations. https://www.un.org/en/about-us/un-charter/full-text
[45] United Nations. (16 December 1966). International Covenant on Civil and Political Rights. OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
[46] United Nations. (10 March 2021). Final report of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security. UNODA. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
[47] International Institute for Democracy and Electoral Assistance. (18–20 March 2024). *The 3rd Summit for Democracy*. International IDEA. https://www.idea.int/events/3rd-summit-democracy
[48] The White House. (18 March 2024). Joint statement on efforts to counter the proliferation and misuse of commercial spyware. https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/

United Nations Security Council on 14 January 2025, Slovenia announced its adherence to the joint declaration promoted by the United States.

21. The use of spyware by state actors or affiliated companies during armed conflicts, including those operating under the label of private military and security firms (PMSCs) within the framework of international humanitarian law (IHL), raises significant legal concerns.[49] When such digital tools are used to infiltrate the command systems of opposing forces, target journalists, or interfere with civilian infrastructure, they risk breaching the principles of distinction and proportionality. A clear example is activists or journalists are deceived into installing commercial spyware, enabling actors to identify, track, or neutralize them in ways that directly endanger civilian life. This lack of accountability among cyber-mercenaries, using commercially available spyware further complicates questions of state responsibility and attribution under both the law of state responsibility and IHL.[50]

Considerations for Parliamentarians and Public Officials

22. PAM and its CGS propose, as already done for the malicious of AI, to set up a Euro-Mediterranean and Gulf Parliamentary Observatory on cybersecurity and spyware misuse, as well as a network for the Prevention and Contrast of the Misuse of Spyware Technologies. Guarantees of human rights and fundamental freedoms, the safeguarding of peace and national and international security, the resilience of institutional and economic systems, and the integrity of information environments (within the framework of the United Nations Global Principles for Information Integrity)[51] are all threatened by the growing misuse of spyware technologies. Their use must be compatible with international law, in particular international humanitarian law and international human rights law. This is particularly true given the growing role of spyware and surveillance technologies in armed conflicts and the increasing involvement of private contractors in military intelligence, targeting and cyber operations. Furthermore, the rise of "cyber mercenaries" calls for a rethinking of the scope of international humanitarian law (through a better-defined articulation of the functions that cannot be delegated by States in the digital sphere and the development of new legal regimes to regulate commercial surveillance actors in conflict contexts). PAM considers dialogue and

[49] Korzak, E. (March 2025). Managing commercial spyware through export controls: Lessons learned from the Wassenaar experience. Center for Long-Term Cybersecurity, UC Berkeley. https://cltc.berkeley.edu/wp-content/uploads/2025/03/Managing_Commercial_Spyware_Export_Controls.pdf

[50] Gallagher, R. (10 October 2012). *Ahmed Mansoor, UAE activist, allegedly tricked by phoney WikiLeaks into downloading Hacking Team spyware*. Slate. https://slate.com/technology/2012/10/ahmed-mansoor-uae-activst-allegedly-tricked-by-phoney-wikileaks-into-downloading-hacking-team-spyware.html

[51] United Nations. (2024). United Nations Global Principles for Information Integrity. United Nations. https://www.un.org/en/information-integrity

parliamentary diplomacy to be fundamental tools for dealing with the misuse of spyware technologies, given the humanitarian and systemic implications that derive from them.

23. PAM suggests that states adopt "The Pall Mall Process Code of Practice for States," which proposes voluntary good practices. Although important, voluntary adoption of this Code may not be decisive. A process of progressively articulating binding international legal obligations is needed for truly effective governance and, given the number of actors involved, a multi-stakeholder approach (including states, private sellers, civil society and multilateral institutions) is required.
24. The wrong use of spyware technologies needs better protection, especially by finding the right balance between security and ensuring privacy for sensitive groups like political dissidents, activists, human rights defenders, journalists, diplomats, military representatives, politicians, government officials, and public servants. In terms of responsibility, actions are needed to hold accountable those states that are not in line with international human rights law and the non-state actors that operate within them.
25. It is crucial, at the national, regional, and global level, that the development, purchase, and use of commercial spyware technologies are effectively regulated, while their legitimate use must be safeguarded to counter criminal and terrorist organization. Without any tolerance for the misuse of commercial spyware tools, an objective risk must be addressed: in the absence of stable legal frameworks that consider the importance of spyware in combating serious crime and terrorism, it is possible that states will choose mandatory access regimes as the best alternative, through private platforms to redefine their security architecture in ways that can seriously damage the encrypted communications ecosystem. That said, it is necessary to monitor the growth and diversification of a market that risks spreading potentially destructive capabilities in cyberspace and to improve the oversight activities. International efforts to control existing exports of spyware technologies and national actions in this regard need to be strengthened:
    - States must work for a harmonized legal definition of national security as much as possible, considering the real and serious threat posed by the misuse of spyware technologies. In this context, it is very important to consider the conceptual and doctrinal ambiguities surrounding the commercial spyware sector, which could threaten the consistency of any emerging governance regime;
    - States must promote public-private partnerships between political institutions, judicial systems, intelligence services, police forces, private companies, academia, and civil society organizations. The whole of society needs to approach cyberspace to make it safer, investing

in better global IT capacity for defensive purposes to seize the enormous opportunities offered by digital technologies. Promoting an organic participatory process from the bottom up, encouraging strategic dialogue among all involved actors, and incorporating the concept of human rights into this process is fundamental;

- States have a responsibility to prevent the proliferation of malicious ICT tools and techniques and the use of malicious covert functions. States must also improve the responsible reporting of ICT vulnerabilities.

26. Regarding the acquisition of spyware technologies, given the changing identities of suppliers and the volatility of supply chains, national governments should impose 'Know Your Vendor' (KYV) requirements, requiring the disclosure of relationships with suppliers and investors. Naturally, appropriate feasibility and potential impact assessments must be carried out in relation to this instrument.
27. Recent SaaS spywares are found to be going more on a 'spyware-as-a-service' (SaaS) approach, with one stage in the spyware's life cycle, like the development of those exploits, or server hosting, or the obfuscation of the infrastructure, being outsourced to a network of specialized actors. Scalability is also possible with this outsourced modular architecture, which provides an added advantage of being able to scale quickly in addition to the fact that the responsibility is obfuscated, rendering attribution and enforcement to be much more difficult. Service-based ecosystems typically include grey-market intermediaries and offshore providers of infrastructure that are outside the conventional legal domain. The regulative policies, accordingly, should change; instead of focusing on the giant spyware corporations, they must establish policies to resolve the system risk of distributed and service-based systems fueling the current commercial spyware actions.[52]
28. Government-run company registries are a crucial resource in terms of responsibility: they would play a significant role in better addressing cross-border circulation or investments in spyware providers. These registries would also be an important source of information for due diligence by potential investors, as well as providing better visibility of commercial entities operating in their respective jurisdictions.
29. In order to limit extraterritorial jurisdictional arbitrage by spyware vendors (and others seeking to evade regulatory controls), states should raise the barriers for vendors associated with an export license for electronic surveillance technologies, including spyware, to leave a single jurisdiction and impose reporting of new branches and subsidiaries.

[52] Amnesty International Security Lab. (1 May 2024). A web of surveillance: Unravelling a murky network of spyware exports to Indonesia. Amnesty International. https://securitylab.amnesty.org/latest/2024/05/a-web-of-surveillance/

30. States must guarantee open reporting. There is a worrying trend of threats to undermine this reporting, as some spyware providers are implementing legal strategies against public participation (SLAPP, Strategic Lawsuits Against Public Participation).
31. States must strengthen export licensing requirements by safeguarding human rights considerations beyond the geopolitical positioning of the country.
32. States, ensuring accountability for abuses, must protect the victims of spyware and eliminate as many bureaucratic obstacles as possible to obtaining justice.

Conclusions

33. The pervasiveness of spyware tools poses a decisive and constantly evolving challenge to democratic institutions. The risks associated with the misuse of illegal espionage tools, in particular spyware, are transforming thanks to technological developments and are jeopardizing the guarantee of fundamental rights of citizens and democratic resilience. At a time when deregulation is being pushed very strongly, national, regional and global rules on the proliferation and use of spyware are increasingly necessary. This report has attempted to highlights the potential, as well as the limitations of existing legislative and governance tools (such as the strategic guidelines developed by the United Nations system, by the European Parliament and the Code of Conduct for States proposed in the Pall Mall Process negotiations), emphasizing the importance of parliamentary dialogue.
34. What is clear is the need for public-private partnerships that include all relevant actors and mitigate as much as possible the negative effects of spyware misuse through cooperation, exchange of intelligence information's and best practices.
35. This report is a first step, and in-depth research on the strategic impacts of spyware misuse in the context of relentless technological evolution must continue. As part of the *Global Parliamentary Observatory on AI and Emerging Technologies* based in San Marino, PAM and its CGS propose to work on study and research projects aimed at understanding the impact of new frontiers in artificial intelligence on the evolution of spyware technologies. How will autonomous surveillance agents work without continuous human input, and what risks will this entail?

Report:

Annex

Spyware Explored: Historical Development, Definitions, and In-Depth Technical Insights

San Marino, 10 December 2025

Disclaimer: This document is prepared by the researchers of the Centre for Global Studies (CGS) of the Parliamentary Assembly of the Mediterranean (PAM) in San Marino in their personal capacity. The opinions expressed in the note are the authors' own and may not reflect the views of PAM.

Index

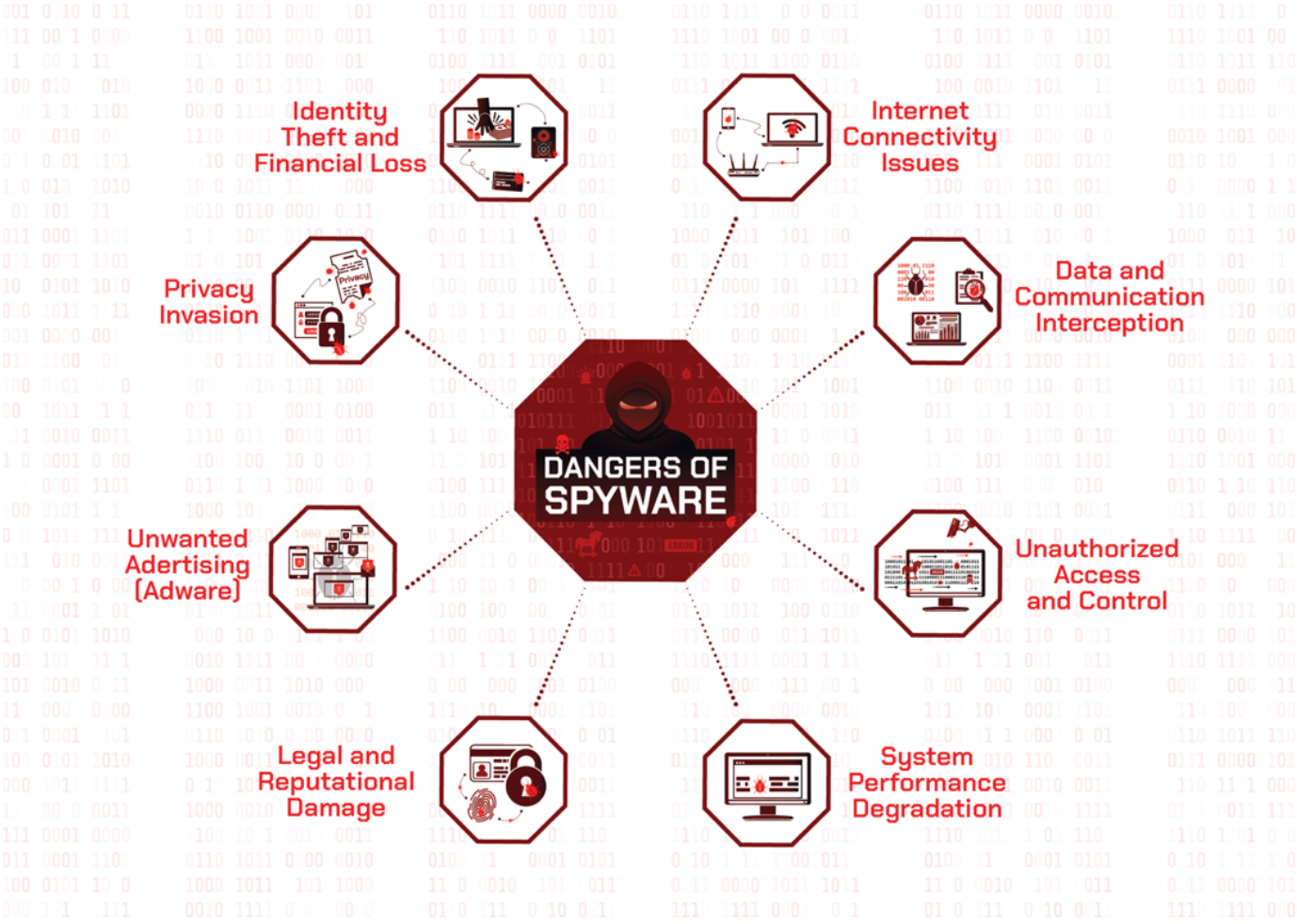
Introduction

1- Modern technological progress during the digital age shapes every aspect of human living, working, and communication. The technological advancements have produced critical challenges, especially with regard to cybersecurity. Spyware is a type of malicious software that secretly monitors and collects information from devices that affects private users just as much as it affects business entities because of its widespread and dynamic nature. This report explains the historical development and current state of spyware, along with its severe impact on privacy protection and safe operations. Furthermore, in favor of parliamentarians and public officials, the report looks at the legislative aspects of a growing phenomenon and is prepared by the Center for Global Studies (CGS), a special program of the Parliamentary Assembly of the Mediterranean (PAM) and, in cooperation with the Counter-Terrorism Committee Executive Directorate (CTED).

2- The development of malicious software named spyware, which observes user devices secretly without permission, has shifted substantially throughout history. Spyware experienced a development from simple adware through various stages until it evolved into advanced tools that cybercriminals use for espionage. Modern cybersecurity demands knowledge about all types of spyware as well as their infection methods and available protective measures.

3- The misuse of spyware technology creates dangerous challenges that protect both the rights of citizens and ensure law enforcement remains lawful. The use of these technologies has become a threat against political dissidents, activists, journalists, and diplomats who need strict regulations along with ethical governance to prevent unfavorable cyber intrusions and illegal surveillance. A complete review of spyware exists in this report while exploring both its social effects and the need for strong protective measures for digital security.

Figure 2: Dangers of Spyware[53]



Importance of Data Security

4- In the digital era, securing data has become paramount for parliaments, organizations, and companies. The increasing reliance on technology for daily operations and communication has made data a valuable asset that needs robust protection. Ensuring data security helps prevent unauthorized access, data breaches, and potential espionage.

5- Apple OS and iOS are widely regarded as more secure compared to Android and Windows because they are closed-source operating systems. Like Apple's, do not share their code publicly, making them harder to hack[54] Open-source systems, like Android allow anyone to view and modify the code, which can lead to security vulnerabilities. While this openness fosters innovation and customization, it also increases the potential for security flaws to be identified and exploited. The

[53] Figure 2: Graph and sources compiled by the GCS research team. This figure illustrates the trends in spyware usage over the past decade, highlighting key data points and sources. Bloxberg, D. (n.d.). What is spyware? Secure privacy & halt theft. VIPRE. https://vipre.com/glossary-terms/what-is-spyware/?srsltid=AfmBOoqSC24_jGU6K5hW7l4PKc1RjJYdspzTFaslkTEB793Jj2uaBJaU

[54] Knezevic, O. (28 June 2024). Android vs iPhone security: which is safer? Norton. https://us.norton.com/blog/mobile/android-vs-ios-which-is-more-secure

controlled environment of closed-source systems like Apple OS and iOS ensures tighter security measures and more rigorous vetting of applications, contributing to their enhanced safety.[55]

6- **Device Ports and Security**: The third port on devices used through Apple, Android, and Google products poses significant security implications. These ports can be potential entry points for malicious software if not properly secured.[56] It is crucial to implement stringent security measures to safeguard these access points.[57]

7- **Camera Security**: With the integration of advanced camera features in devices, securing these components has become essential. Unauthorized access to cameras can lead to privacy breaches and unauthorized surveillance.[58] Ensuring that camera features are secure and regularly updated is vital for maintaining privacy and security.[59]

8- **Precautionary Measures**: To mitigate the risk of unauthorized access, it is advisable to turn off cameras during meetings at home or in the office.[60] This precaution helps ensure that sensitive discussions are not inadvertently recorded or monitored by compromised devices.[61]

Early History of Spyware

9- Spyware has a long and complex history, dating back to the early days of personal computing. The term "spyware" was first used publicly in October 1995 on Usenet, an early internet discussion system. Initially, it referred to "snoop equipment" like hidden cameras. However, it soon came to describe software that secretly monitors and collects information from users' computers.[62]

10- In 1999, Steve Gibson of Gibson Research detected advertising software on his computer, which he suspected was stealing his confidential information. designed to detect and remove spyware, called OptOut. This marked the beginning of efforts to combat spyware.[63]

---

[55] Kaspersky. (22 April 2023). Android vs. iOS security comparison 2023. Retrieved from https://www.kaspersky.com/resource-center/threats/android-vs-iphone-mobile-security

[56] Shetty, S. (5 December 2024). Firewall configuration for Cyber Device Manager MDM. Codeproof. Retrieved from https://support.codeproof.com/mobile-device-management/mdm-servers-ports-for-firewall-config

[57] Google. (2025). Device management security checklist. Retrieved from https://support.google.com/cloudidentity/answer/7422256?hl=en

[58] Devasia, A. (28 December 2024). Video surveillance laws by state: Comprehensive guide. Safe and Sound Security. Retrieved from https://getsafeandsound.com/blog/video-surveillance-laws-by-state/

[59] Reconeyez. (18 September 2024). Understanding privacy laws for security cameras and CCTV. Retrieved from https://reconeyez.com/us/updates/security-camera-privacy-laws/

[60] Tsipursky, G. (7 May 2024). Cameras on during meetings: The pros and cons. Disaster Avoidance Experts. Retrieved from https://disasteravoidanceexperts.com/cameras-on-during-meetings-the-pros-and-cons/

[61] Cybersecurity and Infrastructure Security Agency (CISA). (17 January 2020). Cybersecurity publications. Retrieved from https://www.cisa.gov/resources-tools/resources/cybersecurity-publications

[62] inPixio. (2023). The history of spyware. Retrieved from https://support.inpixio.com/hc/en-us/articles/4408050108564-The-History-of-Spyware

[63] Gibson, S. (2010). OptOut: Internet spyware detection and removal. Gibson Research Corporation. Retrieved from https://www.grc.com/optout.htm

The Echelon Affair (1999-2002)

11- The Echelon Affair was a significant event in the history of global surveillance. The Echelon network was a global interception system developed and managed by the states that signed the UKUSA agreement. It was capable of intercepting private and economic communications.[64]

12- During the late 1990s, press and media reports revealed the existence of the Echelon network. This led to investigations by the European Parliament, including the STOA (Scientific and Technological Options Assessment) studies. The European Parliament responded with questions, debates, and the establishment of a temporary committee to investigate the network. The final position adopted by the Parliament highlighted the need for transparency and accountability in surveillance practices.[65]

13- The Echelon Affair had a significant impact on international relations and public opinion, drawing parallels with later revelations by Edward Snowden and Julian Assange.[66]

Evolution of Spyware Post-2002

14- After 2002, spyware evolved significantly, becoming more sophisticated and dangerous. Here are some key developments:

- **Anti-Spyware Software Market**: The commercial spyware sector was valued at around $12 billion in 2023,[67] while the anti-spyware software market was valued at $2.9 billion and is expected to reach $7 billion by 2032. This highlights the growing demand for both spyware and anti-spyware solutions.[68]
- **Adware and Browser Hijackers**: In the early 2000s, adware and browser hijackers became prevalent. Programs like CoolWebSearch (2003) redirected users' browsers to unwanted websites and displayed intrusive ads.[69]
- **Key-loggers and Info-stealers**: Spyware evolved to include key-loggers and info-stealers, which captured sensitive information like passwords and financial data. These programs became more advanced, often hiding deep within the system to avoid detection.[70]

---

[64] Publications Office of the European Union. (2015). Competition policy for the digital era. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/c5f2f42f-3db7-4023-8cb5-f30d5242bab2/language-en

[65] European Parliamentary Research Service. (4 November 2014). Artificial intelligence: From ethics to policy. Retrieved from https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU%282014%29538877

[66] Monbelli, I. (n.d.). The Echelon affair: History of an international investigation. Historical Archives of the European Union. Retrieved from https://www.eui.eu/Documents/Research/HistoricalArchivesofEU/FriendsofArchives/FriendsHAEUConfMonbelli.pdf

[67] Chin-Rothmann, C. (4 September 2024). Cyber mercenaries: Limiting government use of commercial spyware. Georgetown Journal of International Affairs. Retrieved from https://gjia.georgetown.edu/2024/09/04/cyber-mercenaries-limiting-government-use-of-commercial-spyware/

[68] Business Research Insights. (7 April 2025). Anti spyware software market size & growth report. Retrieved from https://www.businessresearchinsights.com/market-reports/anti-spyware-software-market-103433

[69] Infosec Institute. (4 June 2014). A history of malware: Part four, 2000-2005. Retrieved from https://www.infosecinstitute.com/resources/general-security/history-malware-part-four-2000-2005/

[70] Urianza, J. (10 October 2023). How keyloggers have evolved from the Cold War to today. Dark Reading. Retrieved from https://www.darkreading.com/vulnerabilities-threats/how-keyloggers-have-evolved-from-the-cold-war-to-today

- **FinFisher or FinSpy (2010)**: Utilized primarily by governments for surveillance, FinFisher infiltrated systems across 32 countries. Researchers identified 33 likely government users of this spyware.[71]
- **Regin (early 2010s)**: A sophisticated malware targeting various countries, Regin infected computers predominantly in Russia and Saudi Arabia.[72]

Common Infection Methods

15- Mobile spyware can infiltrate devices through several methods:

- **Malicious Apps**: Spyware is often disguised as legitimate apps, which users unknowingly download and install.[73]
- **Phishing Attacks**: Attackers may use phishing emails or messages to trick users into clicking on malicious links that install spyware.[74]
- **Exploiting Vulnerabilities**: Some spyware exploits security vulnerabilities in the operating system or apps to gain access to the device.[75]
- **Wi-Fi Network Spyware**: Spyware can also infiltrate devices through compromised Wi-Fi networks. Attackers can set up rogue Wi-Fi hotspots or exploit vulnerabilities in legitimate networks to intercept data and install spyware on connected devices. It is crucial to be cautious when connecting to public Wi-Fi networks and to use secure, encrypted connections whenever possible.[76]
- **Advanced Persistent Threats (APTs)**: Spyware became a tool for APTs, which are long-term attacks by skilled hackers who target specific organizations or individuals. These attackers use sophisticated methods to maintain access to systems for extended periods, often for espionage.[77]

[71] Moes, T. (January 2024). Spyware examples: The 5 worst attacks of all time. SoftwareLab. Retrieved from https://softwarelab.org/blog/spyware-examples/
[72] Ibidem
[73] Doffman, Z. (26 November 2024). Delete these 15 dangerous apps on your phone—8 million installs so far. Forbes. https://www.forbes.com/sites/zakdoffman/2024/11/26/delete-these-15-dangerous-apps-on-your-phone-8-million-installs-so-far/
[74] Stouffer, C. (3 October 2022). 20 types of phishing attacks + examples and prevention tips. Norton. https://us.norton.com/blog/online-scams/types-of-phishing
[75] Cybersecurity and Infrastructure Security Agency. (10 March 2025). CISA adds five known exploited vulnerabilities to catalog. CISA. https://www.cisa.gov/news-events/alerts/2025/03/10/cisa-adds-five-known-exploited-vulnerabilities-catalog
[76] Stouffer, C. (14 June 2023). How to tell if someone hacked your router: 10 warning signs. Norton. https://us.norton.com/blog/privacy/how-to-tell-if-someone-hacked-your-router
[77] Baker, K. (04 March 2025). What is an advanced persistent threat (APT)? CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/advanced-persistent-threat-apt/

- **Havex or Dragonfly (mid-2010s)**: Targeting industrial control systems, Dragonfly posed a significant threat to critical infrastructure.[78] Over 2,000 sites were targeted in this cyber espionage campaign.[79]

- **Ransomware and Spyware Hybrids**: Some modern malware combines ransomware and spyware functionalities, encrypting data while also stealing information. This dual threat increases the potential damage to victims.[80] Recent Ransomware Attacks (2025): In April 2025, a zero-day vulnerability in the Windows Common Log File System (CLFS), tracked as CVE-2025-29824, was exploited by the RansomEXX ransomware gang (Storm-2460) to target IT and real estate sectors in the U.S., financial firms in Venezuela, a software company in Spain, and retail in Saudi Arabia. The attackers used PipeMagic malware to escalate privileges and deploy ransomware, highlighting the ongoing threat of spyware evolving into ransomware hybrids.[81]

Types of Spyware

16- Spyware manifests in various forms, each designed to gather information and compromise privacy in multiple ways. The following are common types:

- **Adware**: Software that automatically displays or downloads advertising material when a user is online. It can slow down the device and inundate the screen with pop-up ads.[82]
- **Keyloggers**: Surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard. This can capture sensitive information such as passwords and credit card numbers.[83]
- **Infostealers**: Programs that scan the device for specific data, such as login credentials, and transmit it to the attacker. These can steal personal information and financial data.[84]
- **Browser Hijackers**: Software that modifies browser settings to redirect to malicious websites or display unwanted advertisements. This can lead to privacy breaches and exposure to harmful content.[85]

---

[78] Nelson, N. (18 January 2016). The impact of Dragonfly malware on industrial control systems. Global Information Assurance Certification (GIAC). https://www.giac.org/paper/gicsp/724/impact-dragonfly-malware-industrial-control-systems/148912
[79] Moes, T. (January 2024a). Spyware examples: The 5 worst attacks of all time. SoftwareLab. Retrieved from https://softwarelab.org/blog/spyware-examples/
[80] Almohaini, R., Almomani, I., & AlKhayer, A. (19 November 2021). Hybrid-based analysis impact on ransomware detection for Android systems. Applied Sciences, 11(22), 10976. https://www.mdpi.com/2076-3417/11/22/10976
[81] The Record. (8 April 2025). Microsoft zero-day used in ransomware attack on real estate sector. The Record. https://therecord.media/microsoft-zero-day-used-ransomware-attack-real-estate
[82] Malwarebytes. (2024). *Adware - What is Adware and How to Remove Adware*. https://www.malwarebytes.com/adware
[83] Malwarebytes. (2024). *Keylogger | What is a Keylogger? How to protect yourself*. https://www.malwarebytes.com/keylogger
[84] Maguire, E. (13 November 2024). Infostealers: What they are, how they work, and how to protect yourself. Proton. https://proton.me/blog/infostealers
[85] Nemchick, E. (20 February 2024). What are browser hijackers? Removal + prevention tips. Norton. https://us.norton.com/blog/malware/what-are-browser-hijackers

- **Rootkits**: A collection of software tools that enable unauthorized access to a computer or other software. Rootkits can hide deep within the system, making detection and removal challenging.[86]
- **Trojans**: Malicious programs that disguise themselves as legitimate software to install other types of spyware on the device and create backdoors for attackers. Trojans can facilitate further infections and unauthorized access.[87]
- **Pre-installed System Spyware (Samsung Galaxy Series in the MENA region):** Certain Samsung Galaxy devices distributed across the MENA region contain a form of unremovable pre-installed system software that behaves like spyware. Because it is embedded at the firmware level, users cannot disable or remove it, allowing continuous data collection and remote access capabilities. Its integration into the device's core system makes it difficult to detect or control, posing significant privacy and security risks for users.[88] While documented in the MENA region, similar components may exist in other markets, underscoring the need for caution regards this brand's devices.[89]

Signs of a Key-logger

17- Detecting a key-logger can be challenging, but several indicators may suggest its presence on a device:

- **Unfamiliar Software**: Applications or programs are running on the device that were not installed by the user.[90]
- **Slower Performance**: The device exhibits slower performance than usual, frequently crashes, or freezes.
- **Lagging Mouse Movements**: Mouse movements are lagging, and keystrokes are delayed.
- **Strange Background Noises**: Unusual background noises are heard during phone calls.
- **Disappearing Cursor**: The cursor disappears randomly while the mouse is in use.
- **Unexpected Ads**: Advertisements related to recent searches or browsing history appear, even if those items have not been searched for recently.
- **Overheating**: The device overheats frequently, even when not running many programs.

---

[86] Fortinet. (n.d.). What is a rootkit? Fortinet. https://www.fortinet.com/resources/cyberglossary/rootkit
[87] McGowan, E. (08 May 2024). What is a Trojan? Norton. https://us.norton.com/blog/malware/what-is-a-trojan
[88] Cybersecurity News. (17 November 2025). *Spyware on Samsung devices*. Cybersecurity News. https://cybersecuritynews.com/spyware-on-samsung-devices/
[89] Doffman, Z. (30 November 2025). *Israel's IDF bans Android to stop hackers—iPhones mandatory*. Forbes. https://www.forbes.com/sites/zakdoffman/2025/11/30/israels-idf-bans-android-to-stop-hackers-iphones-mandatory/
[90] Corentin, C. (18 October 2024). I think my PC is infected: How to identify, remove, and prevent malware. ToolsLib. https://blog.toolslib.net/2024/10/18/i-think-my-pc-is-infected-how-to-identify-remove-and-prevent-malware/

- **Nonsensical Texts**: Texts with random characters or messages that do not make sense are received.

Government-Requested Data Access

18- In some cases, governments request full data access from technology companies like Apple or Microsoft for surveillance purposes. These requests are often made to monitor specific individuals or groups and can include access to messages, emails, location data, and other personal information. Unlike traditional spyware, which is installed without the user's knowledge, government-requested data access is implemented with the cooperation of the technology company.

19- **Apple's Legal Challenge**: Apple has taken legal action against the UK government, appealing to the Investigatory Powers Tribunal. This tribunal has the authority to investigate claims against the Security Service. The legal challenge is in response to the UK government's demand for a "back door" to encrypted data, which Apple argues would compromise user privacy and security.[91]

20- **End-to-End Encryption**: Apple emphasizes the importance of end-to-end encryption, which means only the sender and receiver can read the messages, in protecting user data from unauthorized access. The company argues that creating a back door would weaken this encryption and make devices more vulnerable to cyber-attacks.[92]

21- **Government Surveillance**: The UK government's request is part of broader efforts to enhance surveillance capabilities for national security purposes. However, this raises significant privacy concerns and debates about the balance between security and individual rights.[93]

22- **Implications for Technology Companies**: The case highlights the ongoing tension between technology companies and governments over data access and privacy. It underscores the challenges that companies face in protecting user data while complying with legal requirements.[94]

23- Legislative and Governance Proposals: Legislative and governance proposals are essential for regulating the use of spyware technologies. It is crucial to balance security and privacy, especially for sensitive categories such as political dissidents, activists, and journalists. States must ensure that the use of spyware is subject to strict oversight and accountability, keeping in mind its

[91] BBC News. (04 March 2025). The invisible impact of climate change. BBC. https://www.bbc.com/news/articles/c8rkpv50x01o
[92] Apple Support. (16 September 2024). How to turn on Advanced Data Protection for iCloud. Apple. https://support.apple.com/en-us/108756
[93] BBC News. (04 March 2025). The invisible impact of climate change. BBC. https://www.bbc.com/news/articles/c8rkpv50x01o
[94] Embroker Team. (11 March 2025). Common AI data privacy risks faced by tech companies. Embroker. https://www.embroker.com/blog/ai-data-privacy-risks-for-tech-companies/

obligations under international law, in particular, international human rights law and international humanitarian law.[95]

24- Multiple international regulations, established to preserve privacy rights alongside human rights protections, govern the application of spyware. Compliance with legal frameworks as well as ethical standards requires careful negotiation from organizations and States.[96]

25- The implementation of spyware technology leads to multiple complex ethical problems that become most pronounced when monitoring activities through this method. Security requirements need to operate in harmony with organizational commitments towards preserving personal rights together with privacy integrity.[97]

26- This type of data access is often employed in situations where national security is at stake or where there is a need to monitor criminal activities.[98] While this practice raises significant privacy concerns, it is a reality in the modern digital landscape. Technology companies are sometimes legally obligated to comply with these requests, which can lead to debates about privacy, security, and the balance between individual rights and national security.[99]

Cybersecurity Companies: Benefits and Dangers

27- Cybersecurity companies play a crucial role in protecting individuals and organizations from various cyber threats. These companies offer a range of services, including malware detection, data encryption, and network security. The benefits of employing cybersecurity companies include enhanced protection against cyber-attacks, expert knowledge in handling security breaches, and the implementation of advanced security measures.[100]

28- However, there are also potential dangers associated with relying on third-party cybersecurity solutions. Adding third-party software to web communications or granting access to them can create vulnerabilities that hackers may exploit. This duality presents a significant challenge: while

[95] Center for Democracy and Technology. (03 September 2024). Civil society joint statement on the use of surveillance spyware in the EU and beyond. Center for Democracy and Technology. https://cdt.org/insights/civil-society-joint-statement-on-the-use-of-surveillance-spyware-in-the-eu-and-beyond/

[96] Privacy International. (20 September 2024). Your new guide to surveillance human rights standards is here. Privacy International. https://privacyinternational.org/long-read/5407/your-new-guide-surveillance-human-rights-standards-here

[97] Office of the High Commissioner for Human Rights. (16 September 2022). Spyware and surveillance: Threats to privacy and human rights growing, UN report warns. OHCHR. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

[98] U.S. Department of Justice. (3 March 2025). Data security. U.S. Department of Justice. https://www.justice.gov/nsd/data-security

[99] Heimlich, N. (18 October 2024). Key legal considerations for businesses in the technology industry. Nick Heimlich Law. https://nickheimlichlaw.com/key-legal-considerations-for-businesses-in-the-technology-industry/

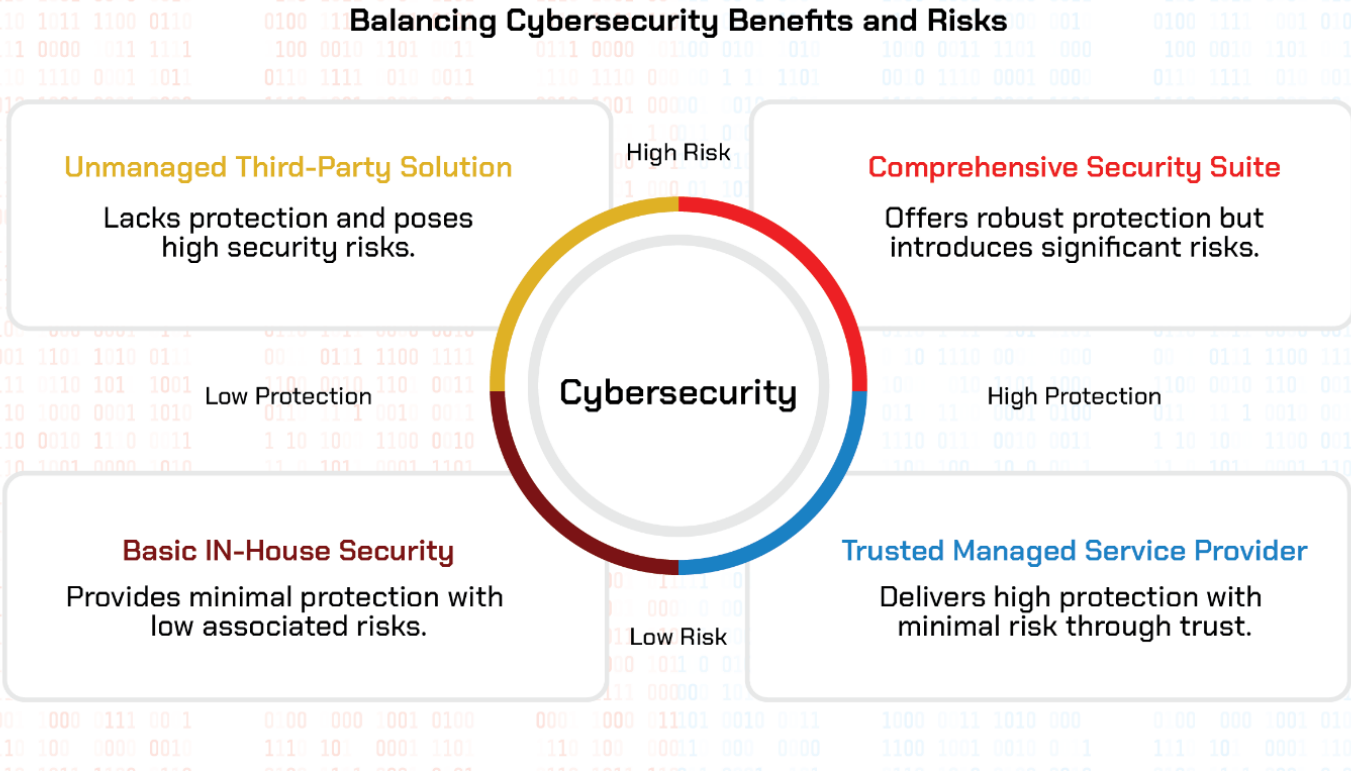
[100] DeCloss, D. (10 March 2025). Why proactive cybersecurity gives companies an edge. Forbes. https://www.forbes.com/councils/forbestechcouncil/2025/03/10/why-proactive-cybersecurity-gives-companies-an-edge/

third-party cybersecurity solutions can provide robust protection, they can also introduce new risks if not effectively managed.[101]

29- Public-Private Partnerships: Public-private partnerships are vital for making cyberspace safer and investing in better global IT capacity for defensive purposes. Collaboration between institutions, intelligence services, police forces, companies, academia, and civil society organizations is essential.[102]

30- It is essential to carefully evaluate and select reputable cybersecurity companies[103] and to continuously monitor and update security measures to mitigate these risks.[104] Balancing the benefits and dangers of third-party cybersecurity solutions is critical to maintaining a secure digital environment.[105]

Figure 3: Balancing Cybersecurity Benefits and Risks[106]



[101] Rosencrance, L. (21 June 2024). 5 major risks third-party services may bring along with them. CSO Online. https://www.csoonline.com/article/574543/5-major-risks-third-party-services-may-bring-along-with-them.html
[102] Cybersecurity and Infrastructure Security Agency. (2024). Partnerships and collaboration. CISA. https://www.cisa.gov/topics/partnerships-and-collaboration
[103] Eden Data. (26 April 2024). The complete guide to choosing a cybersecurity company. Eden Data. https://www.edendata.com/post/how-to-choose-a-cyber-sec-company
[104] Ward, T. (15 March 2025). The importance of security monitoring and logging. Spyrus. https://spyrus.com/the-importance-of-security-monitoring-and-logging/
[105] Expert Panel®. (31 July 2024). Top ways to assess and address third-party cybersecurity risk. Forbes Technology Council. https://www.forbes.com/councils/forbestechcouncil/2024/07/31/top-ways-to-assess-and-address-third-party-cybersecurity-risk/
[106] Figure 3: Graph and sources compiled by the GCS research team. Refer to points: 27 – 28 – 30.

Risks of Social Media and Advertisement Proposals

31- Social media apps often include features that allow users to receive advertisement proposals. While these features can be convenient and personalized, they also pose significant security risks. One of the primary concerns is the access these apps have to your phone's microphone. By granting permission to access the microphone, users may inadvertently allow the app to listen to and record conversations.

32- Malicious actors can exploit this access to gather sensitive information, track user behavior, and even conduct targeted phishing attacks. The potential for abuse is heightened by the fact that many users are unaware of the extent of the permissions they have granted to these apps.

33- To mitigate these risks, it is essential to review and manage app permissions regularly. Users should be cautious about granting microphone access and should only do so for apps that are trusted and necessary. Additionally, disabling microphone access when it is not needed can help protect privacy and reduce the risk of unauthorized surveillance.

34- Impact on Journalists: The use of advanced spyware technologies to surveil journalists and media actors poses significant threats to freedom of the press and digital security. In 2023, new cases involving journalists being spied on were documented, while accountability for previous use of surveillance technology against media continues to prove evasive. This ongoing threat underscores the need for determined action from states to protect journalists and counter threats to media freedom.[107]

35- This issue has been a significant point of contention between major tech companies, particularly Meta (formerly Facebook) and Apple. Apple has taken a strong stance on user privacy, implementing features like App Tracking Transparency (ATT) to give users more control over their data. This has led to conflicts with Meta, which relies heavily on data collection for its advertising business model. Apple's efforts to protect user privacy have been praised by privacy advocates but have also resulted in financial impacts for companies like Meta.[108]

Risks Associated with Online Games and Social Media

36- Online games together with social media platforms function today as primary engagement channels for communication between users. Despite offering entertainment, they present important safety

[107] Council of Europe. (5 March 2024). Safety of Journalists platform 2024 report: Serious concern about the use of spyware against journalists, abusive lawsuits and journalists in exile. Council of Europe. https://www.coe.int/en/web/portal/-/safety-of-journalists-platform-2024-report-serious-concern-about-the-use-of-spyware-against-journalists-abusive-lawsuits-and-journalists-in-exile

[108] Terpstra, P. (3 January 2025). Apple vs. Meta: The privacy debate intensifies. TUAW. https://www.tuaw.com/2025/01/03/apple-vs-meta-the-privacy-debate-intensifies/

threats to users.[109] Certain games, alongside social media applications, let their users interact with unknown individuals, and this functionality gets misused by predators who seek personal information and perform phishing scams (tricking users into giving away personal information).

37- Some apps and games manage to request access permissions that exceed the necessary requirements for their functionality, including microphone and camera usage. The permission requests can enable unauthorized third parties to perform surveillance while breaching privacy security. Users must check app permissions frequently alongside taking necessary precautions to protect their private information on these social media websites.[110]

38- Parents require knowledge about possible threats that their children encounter through online games and social media platforms. Keeping track of children's online activities combined with adequate education about safety practices helps defend them from potential hazards.[111]

Risks of Using Old Mobile Devices

39- Numerous users inaccurately believe older mobile devices provide better security than newer versions. The security advantages of outdated devices keep some diplomatic staff and parliamentary members using them. The reality demonstrates that these devices become more perilous, especially when the battery component is taken out.[112]

40- Old mobile devices carry security risks because these devices neglect to receive important security patches (*updates that fix security issues*), which creates vulnerabilities for multiple types of malignant software and tracking programs. These devices either lack the capability to run modern encryption technology, or they fail to implement it while maintaining exposure of sensitive data to possible security breaches.[113] The battery removal from the device creates security vulnerabilities since useful protections might be deactivated, and the device becomes easier to tinker with.[114]

41- Space and planetary customer security becomes seriously endangered when people operate with outdated technological equipment. The current generation of devices includes sophisticated security elements that get ongoing updates that defend against new security threats.[115] It is best to

[109] Innocent Lives Foundation. (11 March 2023). How predators have infiltrated social media. Innocent Lives Foundation. https://www.innocentlivesfoundation.org/how-predators-have-infiltrated-social-media/
[110] Cybersecurity and Infrastructure Security Agency. (17 January 2025). Manage application permissions for privacy and security. CISA. https://www.cisa.gov/resources-tools/training/manage-application-permissions-privacy-and-security
[111] Cybersecurity and Infrastructure Security Agency. (29 November 2021). Cybersecurity awareness program: Parent and educator resources. CISA. https://www.cisa.gov/resources-tools/resources/cybersecurity-awareness-program-parent-and-educator-resources
[112] Spadafora, A. (17 November 2022). When does an old smartphone become unsafe to use? Tom's Guide. https://www.tomsguide.com/us/old-phones-unsafe,news-24846.html
[113] Cybersecurity and Infrastructure Security Agency. (21 October 2021). Protecting data on old devices you don't use anymore. CISA. https://www.cisa.gov/resources-tools/training/protecting-data-old-devices-you-dont-use-anymore
[114] Gunther, C. (14 January 2024). Your Android device is too old to receive updates, now what? How-To Geek. https://www.howtogeek.com/your-android-device-is-too-old-to-receive-updates-now-what/
[115] Apple Inc. (16 April 2025). Apple security releases. Apple Support. https://support.apple.com/en-us/100100

choose devices with current software versions while securing them effectively to achieve maximum protection levels.[116]

Hidden Cameras in Devices with Lenses

42- Any device with a lens, whether it is a camera, projector, or other optical device, may potentially house a hidden spy camera. These hidden cameras can be incredibly discreet and difficult to detect, even if the device appears to be disconnected from electricity. This is because many modern spy cameras are equipped with small, high-capacity batteries that can power the device for extended periods.[117]

43- The main power source in these devices operates using lithium-ion batteries, which deliver extended battery duration. The operating time of advanced spy cameras extends from several months to a year on a single charge based on usage patterns and battery power capacity.[118] These batteries contain energy-saving features that enable the camera to stay dormant while waiting for movement detection, thus saving additional power reserves.[119]

44- The combination of high-capacity batteries with efficient power management enables specific mini spy cameras to remain operational for a hundred-day duration with a single battery charge.[120] These surveillance tools can be integrated into ordinary items such as pens and clocks, so they become almost unnoticeable.[121] Awareness about these threats coupled with standard privacy protection measures such as lens inspections and specialized tools for detecting hidden cameras is essential for maintaining privacy.[122]

Security Cameras and Power Cuts

45- Security cameras are often relied upon to provide a sense of safety and surveillance. However, there are risks associated with power cuts that can render these cameras ineffective. In some cases, individuals attempting to spy may cause a power cut to disable security cameras temporarily.[123]

---

[116] Romero, A. (25 March 2025). These devices are getting Samsung's March 2025 security update. 9to5Google. https://9to5google.com/2025/03/25/samsung-march-2025-security-update-these-devices/
[117] Ellison, J. (24 November 2024). Is there a device that can find hidden cameras? BlinksAndButtons. https://blinksandbuttons.net/is-there-a-device-that-can-find-hidden-cameras/
[118] Ribeiro, J. (18 September 2022). Top 4 hidden spy cameras with the longest battery life. ProductPeek. https://www.productpeek.com/mini-spy-cameras-with-longest-battery-life/
[119] Social Moms. (5 March 2025). Best mini spy camera with longest battery life. Social Moms. https://www.socialmoms.com/featured/best-mini-spy-camera-with-longest-battery-life/
[120] Ra, D. (20 April 2025). 6 best hidden spy cameras with longest battery life. BestCartReviews. https://bestcartreviews.com/home-improvement/spy-cameras/
[121] Adomaite, L., & Kačerauskas, M. (5 November 2020). 23 times people found hidden spy cams in various shapes and forms. Bored Panda. https://www.boredpanda.com/hidden-cameras-disguised-everyday-objects/
[122] Mitchell, A. (1 March 2025). 10 best devices to detect hidden cameras and microphones. Dock Universe. https://dockuniverse.com/best-device-to-detect-hidden-cameras-and-microphones/
[123] Coleir, E. (13 November 2023). Alternative power solutions for maintaining CCTV camera operations during power outages. Sky Five Properties. https://www.skyfiveproperties.com/blog/alternative-power-solutions-maintaining-cctv-camera-operations-power-outages

This tactic can be particularly concerning for those living in apartments or for diplomatic personnel.[124]

46- To mitigate this risk, it is advisable to have at least one security camera connected to a power bank or an alternative power source. This ensures that surveillance continues even during a power outage, providing continuous protection. Additionally, placing cameras in strategic locations, such as corners with a wide field of view, can enhance security coverage.[125]

47- For continuous internet connectivity, the camera should have a built-in Wi-Fi or 5G connection.[126] Alternatively, a small portable Wi-Fi device, such as a mobile hotspot, can be used. These devices can also be connected to a power bank to ensure they remain operational during power outages. Examples of suitable power banks include the Mini UPS Battery Backup and the Mini UPS Battery Backup 15000mAh, which are designed to provide reliable power to routers and other devices.

48- It is also important to consider the advancements in eavesdropping devices. Modern eavesdropping tools have become more sophisticated and smaller in size, making them harder to detect.[127] For example, eavesdropping devices can be implanted in everyday items like nails used by women. Therefore, it is crucial to remain vigilant and regularly check for any suspicious devices.[128]

49- Case Study: Ring Surveillance Issues: The Federal Trade Commission (FTC) charged Ring with compromising its customers' privacy by allowing employees and contractors to access consumers' private videos and failing to implement basic privacy and security protections, enabling hackers to take control of consumers' accounts, cameras, and videos. This case underscores the importance of robust security measures and privacy protections for all smart devices, including those with hidden cameras.[129]

New Surveillance Technologies

50- The continuous evolution of surveillance technology now produces devices such as Ray-Ban smart glasses that integrate internet-connected mobile cameras. Smart glasses from Ray-Ban enable users to capture hidden video and photo content before transferring them to cloud storage for instant

---

[124] TheHomeReviews. (15 February 2025). CCTV cameras not working after power cut: Step-by-step solution. TheHomeReviews. https://thehomereviews.com/cctv-cameras-not-working-after-power-cut/

[125] Serious Home Security. (7 February 2023). A complete list of ways to power a security camera. Serious Home Security. https://serioushomesecurity.com/ways-to-power-a-security-camera/

[126] Eufy. (16 April 2025). What you need to know about 5G security cameras. Eufy. https://www.eufy.com/blogs/security-camera/5g-security-camera

[127] Eufy. (2024). What you need to know about 5G security cameras. https://www.eufy.com/blogs/security-camera/5g-security-camera

[128] Stillinger Investigations, Inc. (2025). The silent invasion: Uncover the hidden listening devices in your home or office in 5 easy steps. Stillinger Investigations. https://www.investigatesc.com/the-silent-invasion-uncover-the-hidden-listening-devices-in-your-home-or-office-in-5-easy-steps/

[129] Federal Trade Commission. (31 May 2023). FTC says Ring employees illegally surveilled customers, failed to stop hackers from taking control of users' cameras. FTC. https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users

mobile application sharing. The modern devices that offer advanced features and convenience capabilities have severe implications for privacy and security.[130] Surveillance through unauthorized technological devices causes breaches of privacy as well as invisible monitoring activities. People need to understand privacy threats because they must establish protective measures like disabling device cameras and keeping constant track of their app authorizations.[131]

51- Surveillance has now reached a new dimension of micro-level intrusion with the recent introduction of China and its mosquito-sized[132] spy drone. The innovation of this ultra-miniaturization of aerial devices, which comes with secret sensors, demonstrates the rate at which the surveillance industry is evolving. The fact that it has emerged shows the importance of implementing legal and ethical considerations to avoid its misuse or safeguard national security and the privacy of individuals.

Emerging and Advanced Surveillance Vectors

52- An additional area of concern relates to the potential misuse of implantable medical devices as vectors for covert surveillance in high-risk environments. Research on implantable medical devices (IMDs) demonstrates that wireless therapeutic implants including pacemakers, neurostimulators, and similar systems, may be vulnerable to unauthorized access or external manipulation when targeted by adversaries.[133] Comparable vulnerabilities have been documented in hearing-related technologies, such as cochlear implants and connected hearing devices, where wireless programming interfaces and data-exchange protocols expose potential pathways for interception or monitoring.[134]

53- Although artificial eardrum implants are intended solely for therapeutic use, the theoretical risk exists that, in rare circumstances, hostile actors could exploit such devices by embedding covert communication or monitoring components similar to the documented misuse of modified paging devices in intelligence activities. In contexts involving governmental, diplomatic, or institutional responsibilities, unexplained auditory impairments requiring externally sourced implants may

---

[130] Growcoot, M. (14 July 2022). Meta admits smart glasses put privacy at risk, offers no solutions. PetaPixel. https://petapixel.com/2022/07/14/meta-admits-smart-glasses-put-privacy-at-risk-offers-no-solutions/

[131] Cap_able. (3 October 2024). The privacy risks of smart glasses: AI and the loss of personal space. Cap_able. https://www.capable.design/blogs/notizie/the-privacy-risks-of-smart-glasses-ai-and-the-loss-of-personal-space

[132] Min, R. (27 June 2025). China unveils tiny spy drone that looks like a mosquito. What other small spy drones exist? *Euronews*. Retrieved from: https://www.euronews.com/next/2025/06/27/china-unveils-tiny-spy-drone-that-looks-like-a-mosquito-what-other-small-spy-drones-exist?utm_source=chatgpt.com

[133] Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., & Maisel, W. H. (2008, November). *Security and privacy for implantable medical devices*. *Communications of the ACM, 51*(11), 56–63. https://www.secure-medicine.org/hubfs/public/publications/PervasiveIMDSecurity.pdf

[134] Cybellum. (2023, 15 March). *Cyber safe and sound: How hearing aids became medical device cybersecurity targets*. Cybellum Blog. https://cybellum.com/blog/cyber-safe-and-sound-how-hearing-aids-became-medical-device-cybersecurity-targets/

warrant heightened vigilance, as proximity-based access through an implanted device could inadvertently extend surveillance exposure to other member of the household, particularly when a family member is the implant recipient.

Repeating Security Measures and Unnoticed Vulnerabilities

54- Security systems in select situations introduce replicated scenes that create vulnerabilities that attackers can exploit without detection. A predictable security protocol Signal becomes a vulnerable point because such patterns enable attackers to spot opportunities. Security personnel who maintain regular patrol routes allow attackers to predict their movements, thereby enabling them to find unprotected areas.[135] Security risk reduction requires changing security routines through random check implementation.[136] Advanced analytics systems linked with surveillance cameras together with motion sensors help security staff identify events that human observation would otherwise miss.[137] Security protocols should be updated often, and security checks must be performed in detail to detect and fix possible weaknesses immediately.[138]

Tracking Devices and Surveillance

55- The market now provides affordable tracking devices which enables simple monitoring of both people and their belongings. Spies can use basic tracking devices that stick onto personal belongings without being noticeable so they can see items' live positions. These affordable tracking devices have created numerous privacy issues because they are widely obtainable to the public.

56- For example, a spy with experience can remove the cover of a tracking device and implant the device more easily and quickly. This makes it challenging for the target to detect the tracking device. The use of such technology has simplified the process of surveillance, making it more accessible to individuals with malicious intent.[139]

57- Authorities concerned with tracking or eavesdropping on a person no longer need to send special devices to spies. Instead, they can use commercially available tracking devices to monitor

[135] Legato Security. (7 November 2024). Uncovering vulnerabilities that may have gone unnoticed. Retrieved from https://www.legatosecurity.com/blog/uncovering-vulnerabilities-that-may-have-gone-unnoticed
[136] Admin. (21 October 2024). Best practices for comprehensive and effective facility security checks. Retrieved from https://citizens-guard.com/best-practices-for-comprehensive-and-effective-facility-security-checks/
[137] Admin3. (10 March 2025). How does modern CCTV surveillance technology enhance security? Retrieved from https://www.cctv-services.com/how-does-modern-cctv-surveillance-technology-enhance-security/
[138] Fox, R. (7 December 2024). The importance of regular security audits. Retrieved from https://www.datasecurityintegrations.com/types/importance-regular-security-audits/
[139] Justina. (8 October 2024). How to tell if you're being tracked: A guide to devices, signs, and safety. Retrieved from https://investigationsamerica.com/how-to-tell-if-youre-being-tracked-a-guide-to-devices-signs-and-safety/

movements and record daily conversations. It is important to be aware of the potential for misuse of these devices and to take steps to protect personal privacy.[140]

58- Misuse of Tracking Apps: The majority of tracking apps that target couples and children exist freely in popular application markets such as Google Play and the Apple App Store. Though made to improve personal security and communication functions, these apps allow surveillance misuse by cyber-attackers. The tracking applications provide spyware with an easier method to monitor and track their targets.[141]

59- Examples of Tracking Apps

- For Children: An example of a tracking app for children is Life360.[142] This app allows parents to track their children's location, receive alerts about their movements, and ensure their safety.[143]
- For Couples: An example of a tracking app for couples is Find My Friends. This app enables partners to share their location with each other, facilitating easier coordination and communication.

60- Potential Misuse: Malicious actors can exploit these tracking apps to monitor individuals without their consent. By gaining access to the app or the associated account, they can track the person's location, movements, and activities in real-time. This misuse underscores the importance of securing tracking apps and being vigilant about privacy settings and permissions.[144]

61- Smart Rings and Surveillance: Smart rings, such as the Samsung Galaxy Ring[145] and the Oura Ring,[146] are becoming increasingly popular because of their compact design and advanced health-tracking capabilities. These rings can monitor various health metrics, including heart rate, sleep patterns, and physical activity. However, their ability to track the precise movements of the wearer raises significant privacy concerns. The data collected by these rings can be used to monitor an individual's daily activities and movements, potentially leading to unauthorized surveillance. As these devices become more widespread, it is crucial to consider the implications for personal privacy and to implement appropriate safeguards to prevent misuse.

---

[140] Sadler, S. (25 January 2022). Misuse of technology – tracking devices. Retrieved from https://www.prismrisk.gov/about-prism/blog/misuse-of-technology-tracking-devices/

[141] Vigderman, A., & Turner, G. (21 February 2024). Tracking or stalking? The dark side of tracking apps. Retrieved from https://www.security.org/blog/tracking-or-stalking-the-dark-side-of-tracking-apps/

[142] *Life360 | International location sharing app*. (2025). Life360 | Family Tracking App | Location Sharing & Family Safety. https://intl.life360.com/

[143] Mustapha, A. (19 January 2025). Spyware: How it affects your phone, and how to protect yourself. Retrieved from https://www.gizchina.com/2025/01/19/spyware-how-it-affects-your-phone-and-how-to-protect-yourself/

[144] Federal Trade Commission. (2024). Stalkerware: What to know. Retrieved from https://consumer.ftc.gov/articles/stalkerware-what-know

[145] Samsung. (2025). Galaxy Ring. Retrieved from https://www.samsung.com/us/rings/galaxy-ring/

[146] Oura Health Oy. (2025). Oura Ring. Retrieved from https://ouraring.com/

62- Wallets with Tracking Devices: Wallets embedded with tracking devices are growingly popular because of their ease in finding lost items. Giftable without the recipient's awareness of the embedded tracking device, these wallets stay linked to the giver's device. This hidden tracking feature lets the giver track the recipient's whereabouts and movements without permission, so it raises major privacy issues. The Ekster Parliament Wallet, which has a Chipolo tracking card, is one such wallet.[147]

Email Security Practices

63- Understanding CC and BCC:[148]

- **CC (Carbon Copy)**: When CC is used, all recipients can see each other's email addresses. This can be useful for transparency but may pose privacy concerns if the recipients do not know each other.
- **BCC (Blind Carbon Copy)**: BCC hides the email addresses from other recipients, providing an added layer of privacy. This is particularly useful for large email distributions where recipients should not see each other's addresses.

64- **Best Practices for Email Security:**[149]

- **Verify Recipients**: Always double-check the recipients before sending an email, especially when dealing with sensitive information. Ensure that the email is only sent to authorized individuals.
- **Encrypt Sensitive Emails**: Use email encryption tools to protect sensitive information. Encryption ensures that only the intended recipient can read the email content.
- **Be Cautious with Attachments and Links**: Avoid opening attachments or clicking on links from unknown or suspicious sources. These could have malware or phishing attempts.
- **Regularly Update Email Software**: Ensure that the email client and any associated software are regularly updated to protect against vulnerabilities.
- **Monitor for Unusual Activity**: Regularly check the email account for any unusual activity, such as unexpected login attempts or unfamiliar sent emails. Report any suspicious behavior immediately.

[147] The Wallet Shoppe. (8 September 2023). Who makes the best wallet tracker in 2025? [4 great options]. https://thewalletshoppe.com/best-wallet-tracker/
[148] Indeed Editorial Team. (26 March 2025). BCC vs. CC: What's the difference? Retrieved from https://www.indeed.com/career-advice/career-development/bcc-vs-cc
[149] DeMers, J. (2025). 21 email security best practices every professional must know. Retrieved from https://emailanalytics.com/21-email-security-best-practices-every-professional-must-know/

- **Enhance Knowledge and Awareness**: Remain updated on the latest email security threats and inform others within the organization about the best practices for maintaining email security.

65- **Specific Recommendations:**

- **Use BCC for Large Distributions**: When sending emails to a large group, use BCC to protect the privacy of recipients.[150]
- **Avoid Sharing Sensitive Information via Email**: Whenever possible, avoid sharing sensitive information through email. Use secure file-sharing services or encrypted communication channels instead.[151]
- **Periodically Update Email Password**: Regularly update email passwords to mitigate the risk of unauthorized access.[152]
- **Be Wary of Public Wi-Fi**: Avoid accessing email accounts over public Wi-Fi networks, as they can be insecure. Use a VPN if it is necessary to access email in public places.[153]
- **Hide Option for Passwords**: When changing passwords, use the hide option to prevent others from seeing what you are typing. Additionally, avoid mentioning passwords aloud to ensure they remain confidential.[154]

66- By implementing these email security practices, the risk of unauthorized access can be significantly reduced, and sensitive information can be protected from potential threats.

Antivirus Programs for Detecting Keyloggers

67- Several antivirus programs are highly effective at detecting and removing key-loggers. Here are some of the best options:[155]

- **Norton 360**: Known for its comprehensive protection, Norton 360 uses artificial intelligence and machine learning to detect and block advanced malware, including key-loggers.
- **Bitdefender Total Security**: This antivirus software offers exceptional real-time malware and key-logger detection, ensuring comprehensive protection for devices.
- **TotalAV Total Security**: With easy-to-use features and excellent device optimization tools, TotalAV provides robust protection against key-loggers.

---

[150] Writtenhouse, S. (13 November 2022). What do CC and BCC mean in emails? Retrieved from https://www.howtogeek.com/846295/what-do-cc-and-bcc-mean-in-emails/
[151] DeMers, J. (2025). 21 email security best practices every professional must know. Retrieved from https://emailanalytics.com/21-email-security-best-practices-every-professional-must-know/
[152] Ibidem
[153] Ibidem
[154] Ibidem
[155] Moes, T. (January 2024a). Spyware examples: The 5 worst attacks of all time. SoftwareLab. Retrieved from https://softwarelab.org/blog/spyware-examples/

- **McAfee Total Protection**: Reliable malware protection with secure web browsing tools, McAfee is another great option for key-logger detection.
- **Microsoft Defender Antivirus**: Built into Windows 10 and 11, Microsoft Defender offers strong protection against key-loggers and other types of malwares.

Mobile Spyware

68- **How Mobile Spyware Works**: Mobile spyware operates by hiding in the background of a mobile device, often without creating a shortcut icon, making it difficult for users to detect its presence. Once installed, it can perform various malicious activities,[156] such as:

- Stealing Information: Mobile spyware can access and steal information like incoming and outgoing SMS messages, call logs, contact lists, emails, browser history, and photos.[157]
- Tracking Location: Some mobile spywares can track the device's location, providing real-time updates to the attacker.[158] Additionally, numerous websites offer services for tracking locations, which can further facilitate unauthorized monitoring.[159]
- Recording Conversations: Advanced spyware can record phone calls and ambient sounds, capturing private conversations.[160]

69- **Obsolescence of Traditional Surveillance Devices**: In the era of smartphones, traditional devices such as covert microphones used for spying on conversations have become largely obsolete. Modern spyware can be easily deployed to smartphones, allowing for comprehensive surveillance of all conversations, not just phone calls. This shift underscores the increased efficiency and effectiveness of smartphone spyware in monitoring and recording communications.[161] For instance, sophisticated spyware like Pegasus can infiltrate both iOS and Android devices, enabling attackers to access messages, emails, and even ambient sounds. This technological advancement has rendered older methods of surveillance, such as hidden microphones, unnecessary and less effective compared to the capabilities of smartphone spyware.[162]

---

[156] McAfee. (19 July 2023). Mobile spyware: How hackers can turn your phone into a stalking machine. Retrieved from https://www.mcafee.com/blogs/mobile-security/mobile-spyware/
[157] McAfee. (24 May 2023). Mobile spyware—How you can keep stalkers off your phone. Retrieved from https://www.mcafee.com/blogs/mobile-security/mobile-spyware-how-you-can-keep-stalkers-off-your-phone/
[158] RSA Conference. (12 December 2019). Tracking every move: From location-based apps to stalkerware and advanced attackers. Retrieved from https://www.rsaconference.com/library/blog/tracking-every-move-from-location-based-apps-to-stalkerware-and-advanced-attacker
[159] Example: *LocationTool*. (2025). https://location-tool.com/en
[160] Buxton, O. (9 September 2024). Is my phone listening to me? Retrieved from https://us.norton.com/blog/how-to/is-my-phone-listening-to-me
[161] Hauk, C. (20 February 2024). Is someone spying on your cell phone? How to tell & stop them. Retrieved from https://pixelprivacy.com/resources/spying-on-your-cell-phone/
[162] McAfee. (2025). *What is Pegasus Spyware?* McAfee. https://www.mcafee.com/learn/what-is-pegasus-spyware/

Notable Mobile Spyware Examples

70- **Pegasus**: Discovered in 2016, Pegasus is one of the most sophisticated mobile spyware programs. It can infect both iOS and Android devices, often without user interaction, and exfiltrate data such as messages, emails, and location information.[163]

71- Pegasus spyware from the NSO Group seeks journalists and activists, among other political figures, all over the globe. Research indicated that more than 50,000 telephone numbers were selected as potential surveillance targets. Recent cases show how extensive the improper use of commercial spyware damaged individual privacy alongside human rights.[164]

72- The widespread use of Pegasus spyware technology has had a significant impact on human rights. Recent leaks have shown the misuse of this technology for intrusive surveillance of individuals' digital communications and metadata. This misuse highlights the substantial risks posed by such spyware to the promotion and protection of human rights.[165]

- **DarkHotel (2014)**: This spyware targeted high-profile individuals in luxury hotels, using hotel Wi-Fi networks. Thousands of infections have been attributed to DarkHotel since 2008.[166]
- **Pegasus (mid-2010s)**: Known for infecting smartphones, Pegasus was used against journalists, activists, and others. There were attempts to hack or successful hacks into 37 mobile phones of high-profile individuals.[167]

Indicators of Mobile Spyware

73- Detecting mobile spyware can be challenging, but there are several signs to be aware of:

- **Unusual Battery Drain**: Spyware operating in the background can cause the battery to deplete more rapidly than usual.[168]
- **Increased Data Usage**: Spyware may utilize data to transmit information to the attacker, resulting in higher data consumption.[169]

---

[163] Nemchick, E. (6 October 2023). What is Pegasus spyware + how to remove it? Retrieved from https://us.norton.com/blog/emerging-threats/pegasus-spyware
[164] Bertašavičius, V. (9 December 2024). What is Pegasus spyware, and how to avoid it? Retrieved from https://cybernews.com/malware/what-is-pegasus-spyware/
[165] Ní Aoláin, F. (April 2023). Position paper on global regulation of counter-terrorism spyware technology trade. Retrieved from https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf
[166] Kaspersky. (2025). DarkHotel malware virus threat definition. Retrieved from https://www.kaspersky.com/resource-center/threats/darkhotel-malware-virus-threat-definition
[167] Moes, T. (January 2024a). Spyware examples: The 5 worst attacks of all time. SoftwareLab. Retrieved from https://softwarelab.org/blog/spyware-examples/
[168] ForestVPN. (13 December 2024). How can I tell if my phone is being monitored? Retrieved from https://forestvpn.com/blog/mobile-security/how-can-i-tell-if-my-phone-is-being-monitored/
[169] McGowan, E. (25 June 2024). How to tell if your cell phone is tracked, tapped, or monitored by spy software. Retrieved from https://us.norton.com/blog/privacy/how-to-tell-if-your-cell-phone-is-tracked-tapped-or-monitored-by-spy-software

- **Slow Performance**: The device may become sluggish or unresponsive due to the activities of the spyware.[170]
- **Strange Behavior**: Unexpected pop-ups, applications opening autonomously, or settings changing without user input can indicate the presence of spyware whether the device is iPhone[171] or Android.[172]

Protecting Against Mobile Spyware

74- To safeguard mobile devices from spyware, consider the following measures:

- **Install Reputable Security Software**: Utilize trusted antivirus and anti-spyware applications to scan and protect the device.
- **Keep Software Updated**: Regularly update the operating system and applications to patch security vulnerabilities.[173]
- **Be Cautious with Downloads**: Only download apps from official app stores and avoid clicking on suspicious links.[174]
- **Review App Permissions**: Check the permissions requested by apps and deny any that seem unnecessary or invasive.[175]

75- By understanding how mobile spyware works and taking proactive steps to protect devices, the risk of falling victim to these malicious programs can be reduced.

Latest Mobile Spyware Trends

76- Mobile spyware continues to evolve, with latest trends emerging as attackers adapt to changing technologies and user behaviors. Here are some of the latest trends in mobile spyware:

- **Increase in Financially Motivated Threats**: There has been a significant rise in financially motivated mobile threats, including a 111% increase in spyware and a 29% growth in banking malware. Attackers are increasingly targeting financial data and transactions.[176]

---

[170] Trevino, A. (9 February 2024). How to tell if spyware is on your phone and how to remove it. Retrieved from https://www.keepersecurity.com/blog/2024/02/09/how-to-tell-if-spyware-is-on-your-phone-and-how-to-remove-it/
[171] Winder, D. (23 December 2024). Apple warns users of iPhone spyware attacks—What you need to know. Forbes. Retrieved from https://www.forbes.com/sites/daveywinder/2024/12/23/apple-warns-users-of-iphone-spyware-attacks-what-you-need-to-know/
[172] Protectstar. (18 January 2023). How to detect and remove spyware from an Android phone. Protectstar. Retrieved from https://www.protectstar.com/en/blog/how-to-detect-and-remove-spyware-from-an-android-phone
[173] Securecubicle. (15 March 2025). How to keep your software updated on multiple devices. Securecubicle. Retrieved from https://www.securecubicle.com/how-to-keep-your-software-updated-on-multiple-devices/
[174] Williams, B. (29 November 2024). Take back control: How to stop unwanted downloads on your phone. GadgetsRanked. Retrieved from https://gadgetsranked.com/how-do-i-stop-things-from-downloading-on-my-phone/
[175] Walsh, R. (1 December 2020). How to check app permissions on Android and iOS. ProPrivacy. Retrieved from https://proprivacy.com/guides/check-app-permissions
[176] Google Threat Intelligence Group. (12 February 2025). Cybercrime: A multifaceted national security threat. Google Cloud Blog. Retrieved from https://cloud.google.com/blog/topics/threat-intelligence/cybercrime-multifaceted-national-security-threat

- **Phishing and Malicious Web Content**: Mobile phishing attacks have exploded in popularity. Attackers use convincing personas to trick users into sharing credentials, which are then used to infiltrate corporate infrastructure. This trend highlights the importance of securing mobile devices against phishing attempts.[177]
- **Advanced Persistent Threats (APTs)**: Nation-state actors continue to develop sophisticated surveillance-ware. For example, the Houthi-developed mobile spyware, based on the Dendroid RAT, targets military personnel and uses themes like religion and military to lure victims.[178]
- **iOS-Targeted Root Enablers**: There has been an increase in the number of iOS-targeted root enablers, which are tools that allow attackers to gain root access to iOS devices. This trend indicates that iOS devices are becoming more attractive targets for sophisticated spyware.[179]
- **Malicious Apps on Official Marketplaces**: Despite efforts to secure app stores, malicious apps continue to appear on platforms like Google Play. These apps often disguise themselves as legitimate tools, such as file managers, to trick users into downloading them.[180]
- **Fake Investment Apps**: Attackers are using fake investment apps to steal personal data. These apps rely on social engineering to coax users into providing information like phone numbers and full names, which are then used for phone fraud.[181]
- **Legacy and End-of-Life OS Vulnerabilities**: Devices running outdated operating systems are particularly vulnerable to spyware attacks. Legacy systems often lack the latest security patches, making them easy targets for attackers.[182]
- **IoT and Mobile Convergence**: The convergence of IoT and mobile devices has led to an increase in attacks targeting both. IoT devices often have weaker security, providing an entry point for attackers to access connected mobile devices.[183]

Best Practices for Mobile Security

77- To ensure a mobile device remains secure, it is important to follow best practices that protect against various threats. Here are some key recommendations:

---

[177] Lookout. (17 June 2024). The rising threat of mobile phishing and how to avoid it. Lookout. Retrieved from https://www.lookout.com/blog/mobile-phishing
[178] Cybersecurity and Infrastructure Security Agency. (n.d.). Nation-state cyber actors. CISA. Retrieved from https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors
[179] Lookout. (Q2 2024). Mobile threat landscape report: Q2 2024. Retrieved from https://www.lookout.com/threat-intelligence/report/q2-2024-mobile-landscape-threat-report
[180] Misiūnas, A. (7 March 2025). How do malicious apps end up on official app stores? Cybernews. Retrieved from https://cybernews.com/security/how-do-malicious-apps-end-up-on-official-app-stores/
[181] Federal Trade Commission. (n.d.). Investment scams. Consumer Advice. Retrieved from https://consumer.ftc.gov/articles/investment-scams
[182] ITU Online. (26 October 2024). End-of-life (EOL) software: Analyzing vulnerabilities and attacks. ITU Online. Retrieved from https://www.ituonline.com/comptia-securityx/comptia-securityx-4/end-of-life-eol-software-analyzing-vulnerabilities-and-attacks/
[183] Silber, M. (6 January 2025). Five predictions shaping the future of mobility and IoT in 2025. Forbes. Retrieved from https://www.forbes.com/councils/forbestechcouncil/2025/01/06/five-predictions-shaping-the-future-of-mobility-and-iot-in-2025/

- **Use Strong Passwords and Biometrics**: Always use strong, unique passwords for the device and applications. Consider enabling biometric authentication, such as fingerprint or facial recognition, for added security.
- **Keep Software Updated**: Regularly update the operating system and applications to ensure the latest security patches and features are in place. Real-World Example of Mobile Security Updates: On March 31, Apple released a new update, iOS 18.4 and iPadOS 18.4, accompanied by a document detailing the updates and the security vulnerabilities addressed in the previous version.[184] This update includes multiple security enhancements aimed at improving the protection of user data and device security.
- **Install Reputable Security Software**: Utilize trusted antivirus and anti-spyware applications to scan and protect the device from malware.
- **Be Cautious with Downloads**: Only download applications from official app stores like Google Play or the Apple App Store. Avoid downloading applications from unknown sources.
- **Review App Permissions**: Check the permissions requested by applications and deny any that seem unnecessary or invasive.
- **Avoid Public Wi-Fi**: Public Wi-Fi networks can be insecure. Use a virtual private network (VPN) if it is necessary to connect to public Wi-Fi.
- **Disable Unused Features**: Turn off Bluetooth, NFC, and location services when not in use to reduce the risk of unauthorized access.
- **Encrypt Data**: Enable encryption on the device to protect sensitive information in case the device is lost or stolen.
- **Backup Data**: Regularly back up data to a secure location, such as a cloud service or an external drive, to prevent data loss.
- **Be Wary of Phishing Attacks**: Avoid clicking on suspicious links or downloading attachments from unknown sources. Phishing attacks can trick individuals into revealing personal information.
- **Monitor Accounts**: Regularly check accounts for any unusual activity and report any suspicious behavior immediately.

[184] Apple. (31 March 2025). About the security content of iOS 18.4 and iPadOS 18.4. Apple Support. Retrieved from https://support.apple.com/en-us/122371

Smartwatch Spyware

78- Smartwatches have become increasingly popular because of its convenience and advanced features. However, like smartphones, they are also vulnerable to spyware. Spyware on smartwatches can perform various malicious activities, compromising user privacy and security.[185]

Capabilities of Smartwatch Spyware

79- Smartwatch spyware can exploit the device's features to gather sensitive information and monitor user activities. Some of the key capabilities include:

- **Tracking Location**: Spyware can use the smartwatch's GPS to track the user's location in real-time, providing detailed movement patterns to the attacker.
- **Accessing Health Data**: Smartwatches often collect health-related data, such as heart rate, sleep patterns, and activity levels. Spyware can access and transmit this information, potentially revealing sensitive health details.
- **Recording Conversations**: Advanced spyware can utilize the smartwatch's microphone to record conversations, capturing private discussions and ambient sounds.
- **Intercepting Notifications**: Spyware can intercept notifications from connected devices, such as text messages, emails, and app alerts, providing attackers with access to personal communications.
- **Monitoring App Usage**: Spyware can track the usage of apps on the smartwatch, including fitness trackers, messaging apps, and payment services, gathering information on user behavior and preferences.

Common Infection Methods

80- Smartwatch spyware can infiltrate devices through several methods:

- **Malicious Apps**: Spyware is often disguised as legitimate apps, which users unknowingly download and install.
- **Phishing Attacks**: Attackers may use phishing emails or messages to trick users into clicking on malicious links that install spyware.
- **Exploiting Vulnerabilities**: Some spyware exploits security vulnerabilities in the smartwatch's operating system or apps to gain access to the device.

Protecting Against Smartwatch Spyware

81- To safeguard smartwatches from spyware, consider the following measures:

[185] Nielsen, E. (30 November 2024). The security risks of smartwatches. Spotter Up. Retrieved from https://spotterup.com/the-security-risks-of-smartwatches/

- **Install Reputable Security Software**: Utilize trusted antivirus and anti-spyware applications to scan and protect the device.
- **Keep Software Updated**: Regularly update the operating system and applications to patch security vulnerabilities.
- **Be Cautious with Downloads**: Only download apps from official app stores and avoid clicking on suspicious links.
- **Review App Permissions**: Check the permissions requested by apps and deny any that seem unnecessary or invasive.

82- By understanding the capabilities of smartwatch spyware and taking proactive steps to protect devices, the risk of falling victim to these malicious programs can be reduced.

Future Trends in Spyware

83- The advancement of technology will lead to spyware developing more complicated features by implementing artificial intelligence and machine learning capabilities. Securing IoT devices will become more difficult because future spyware will learn to bypass security measures at an accelerated pace.[186]

84- Spyware developers are likely to escalate attacks on Internet of Things (IoT) devices because of their increasing proliferation and consistently weak security architecture.[187] Researcher teams such as those at MIT's CSAIL have already developed adversarial intelligent agents designed to mimic threat actor behaviors for testing network defenses. While these tools are meant for defensive simulations, if adopted by spyware vendors, they could serve as force-multipliers in surveillance, evasion, and infection campaigns.[188] Controlled experiments also demonstrate that platforms like OpenAI's Operator can autonomously gather personal data from professional social networks and execute credential-based intrusions with minimal human input.[189] There are currently no established mechanisms to govern the use of autonomous AI-powered spyware systems under existing legal instruments concerning information privacy. Even though the risks are severe, key frameworks such as the Budapest Convention on Cybercrime,[190] the General Data Protection

[186] Landry, M. (October 2024). The future of spy technology: What to expect in 2025. Marie Landry. Retrieved from https://www.marielandryceo.com/2024/10/the-future-of-spy-technology-what-to.html
[187] Jones, D. (4 March 2025). More than 86K IoT devices compromised by fast-growing Eleven11 botnet. Cybersecurity Dive. Retrieved from https://www.cybersecuritydive.com/news/86000-iot-compromised-eleven11-botnet/741507/
[188] Shipps, A. (January 29, 2025).3 Questions: Modeling adversarial intelligence to exploit AI's security vulnerabilities. MIT Computer Science & Artificial Intelligence Laboratory (CSAIL). https://www.csail.mit.edu/news/3-questions-modeling-adversarial-intelligence-exploit-ais-security-vulnerabilities
[189] TechRadar Pro. (30 July 2025). Agentic AI: The rising threat that demands a human-centric cybersecurity response. TechRadar. https://www.techradar.com/pro/agentic-ai-the-rising-threat-that-demands-a-human-centric-cybersecurity-response
[190] This source has been previously cited; see Reference No. 37 for full citation details.

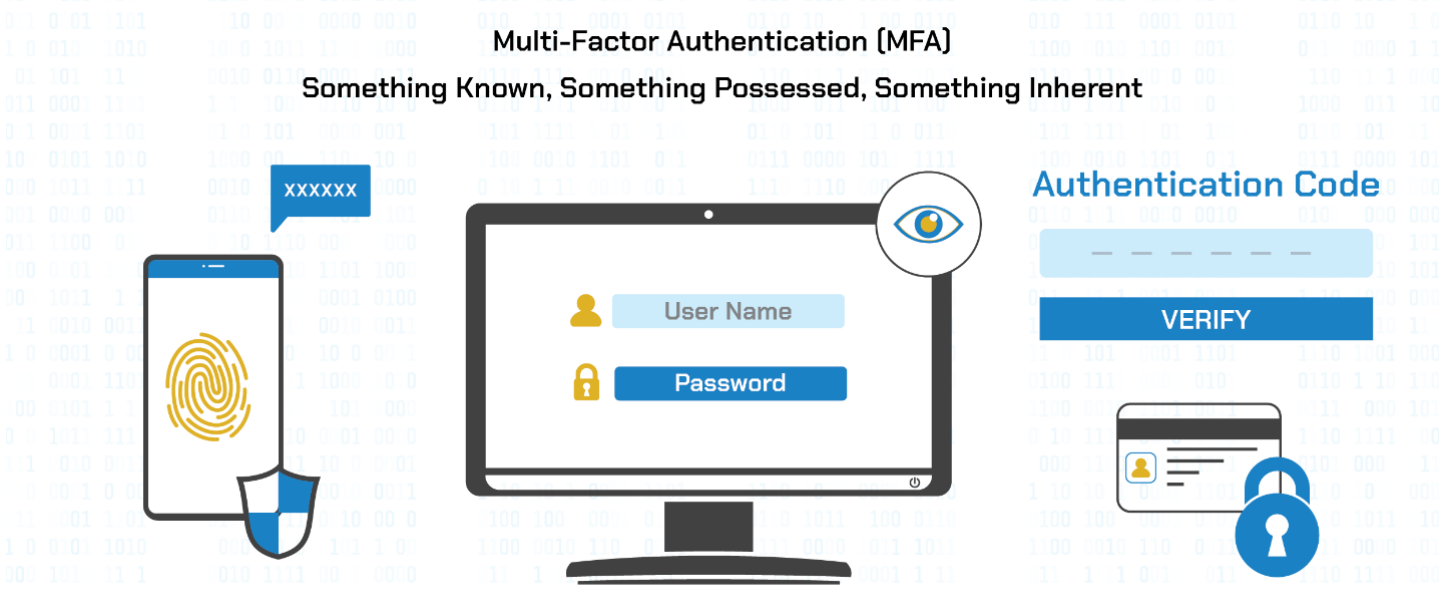
Regulation[191] lack specific provisions to address these technologies. This creates a dangerous normative vacuum that weakens the effectiveness of international cybersecurity and privacy safeguards.

85- When combined with AI's growing role in public surveillance systems, these capabilities could radically diminish privacy and outpace traditional cybersecurity safeguards. Policymakers must urgently address how agentic AI enables self-learning, self-directed spyware operations, or risk enabling a future where surveillance becomes invisible, pervasive, and legally ungoverned.[192]

Multi-Factor Authentication (MFA)

86- Multi-Factor Authentication (MFA) functions as a security process which demands two or more verification factors when users want to access resources including applications or online accounts or VPNs. The security improvement from this method depends on protecting against unauthorized entry even when one authentication element gets compromised.[193]

Figure 4: Multi-Factor Authentication (MFA)[194]



[191] European Parliament & Council of the European Union. (27 April 2016). Regulation (EU) 2016/679 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

[192] West, D. M. (15 April 2025). How AI can enable public surveillance. Brookings Institution. https://www.brookings.edu/articles/how-ai-can-enable-public-surveillance/

[193] Microsoft. (n.d.). What is multifactor authentication. Microsoft Support. Retrieved from https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661

[194] Figure 4: Graph and sources compiled by the GCS research team. Refer to footnote 172, among others.

How MFA Works

87- Multi-Factor Authentication (MFA) typically involves a combination of the following factors:

- **Something Known**: This is usually a password or PIN, which is information that only the user should know.
- **Something Possessed**: This could be a physical device like a smartphone, security token, or smart card. For example, a one-time passcode (OTP) sent to the phone.
- **Something Inherent**: The verification method based on something inherent uses biometric identification features comprising fingerprints and facial recognition together with iris scans.

Example of MFA in Action

88- Using email logging serves as an example to understand MFA security.

- To initiate the process, users must first input their account username along with their password.
- Users require their smartphone to receive a temporary code that serves to authenticate their login.
- Users who possess the password must still provide a second factor before accessing the account because this combination provides substantial protection.

Benefits of MFA

89- Multi-Factor Authentication (MFA) offers several advantages that enhance security and protect sensitive information:

- Multiple verification methods in MFA create a setting that attackers can't get into without permission because it has better security features.
- Multiple security elements defend critical data because compromised authentication factors cannot expose the remainder of sensitive information.
- Regulations, together with standards, enforce MFA implementation as a necessary step to safeguard critical data.

Common MFA Methods

90- Common MFA Methods Login completion requires the entry of a code that reaches a mobile device through SMS or arrives by email. Mobile authenticators from Google Authenticator and Microsoft Authenticator function as applications for time-based one-time passcode generation.

91- Biometric Verification: Using fingerprints, facial recognition, or iris scans. Hardware tokens function as physical devices that either generate OTPs or create authentication through USB

interface connections. MFA implementations result in substantial personal information protection by improving account security.

Dangers of Being Hacked Across Multiple Devices

92- The connected world of today increases hacking risks which affect more than individual devices. A malicious actor who gains entry to smartphone and computer systems creates extreme security risks for the targeted devices.[195] Multiple dangers along with associated risks emerge when this situation occurs:

Comprehensive Data Theft

93- Hackers can steal a vast amount of personal and sensitive information when they have access to multiple devices. This includes:

- **Personal Identifiable Information (PII)**: Names, addresses, social security numbers, and other personal details.
- **Financial Information**: Bank account details, credit card numbers, and transaction histories.
- **Login Credentials**: Usernames and passwords for various online accounts, including email, social media, and financial services.

Heightened Risk of Identity Theft

94- Unscrupulous actors who possess complete personal information can perform identity theft operations with no major difficulty. The perpetrators utilize stolen information to access new accounts and perform unapproved transactions and loan applications which create both financial losses and damage to reputation.

Compromised Communications

95- Hackers can intercept and monitor communications, including emails, text messages, and phone calls. This can lead to:

- **Loss of Privacy**: Sensitive conversations and personal messages can be exposed.
- **Phishing Attacks**: Hackers can use contacts to send phishing emails or messages, tricking them into revealing their own information.

[195] Gadient, A. (2025). *Council Post: Lock all the doors: The cybersecurity risks of overlooked devices in computer networks*. Forbes. https://www.forbes.com/councils/forbestechcouncil/2025/02/21/lock-all-the-doors-the-cybersecurity-risks-of-overlooked-devices-in-computer-networks/

Unauthorized Access to Accounts

96- With login credentials, hackers can gain unauthorized access to various online accounts, leading to:

- **Financial Loss**: Unauthorized transactions and purchases.
- **Data Manipulation**: Deletion or alteration of important files and data.
- **Social Media Hijacking**: Unauthorized individuals may post inappropriate content or disseminate malicious links from accounts.

Device Control and Surveillance

97- Hackers can take control of devices, enabling them to:

- **Monitor Activities**: Track online activities, keystrokes, and browsing history.
- **Access Cameras and Microphones**: Spy through the device's camera and microphone, invading privacy.

Spread of Malware

98- Once a hacker has access to one device, it can be used as a gateway to infect other connected devices with malware, including:

- **Ransomware**: Encrypting files and demanding a ransom for their release.
- **Spyware**: Continuously monitoring activities and stealing information.
- **Adware**: Displaying unwanted ads and redirecting the browser to malicious websites.

Long-Term Consequences

99- The long-term consequences of being hacked can be severe, including:

- **Financial Hardship**: Recovering from financial losses and unauthorized transactions.
- **Emotional Distress**: The stress and anxiety of dealing with identity theft and privacy invasion.
- **Reputational Damage**: Harm to personal and professional reputation due to compromised accounts.

Feasibility of Regulatory Measures such as KYV (Know Your Vendor)

100- Proposals like Know Your Vendor (KYV), that seek to establish better visibility of the supply chain and trace of any spyware roots, are some promising regulatory efforts. Nonetheless, what is proposed usually is merely aspirational with no thorough viability recommendations. This approach cannot be practically implemented without many obstacles such as obstacles of legal system jurisdiction, obfuscation of vendors, government secrecy, and even technological complexity. These structures can only become discussed solutions unless there is a defined

evolution of costs, enforcement systems and the unforeseen costs like blacklisting vendors as this creates deep underground markets. Such policies need to go hand in hand with multilateral agreements, vendor accountability procedures, and capacity enhancements to regulatory as well as enforcement bodies.[196]

Comprehensive Device Security Recommendations

101- Ensuring the security of personal and organizational devices is crucial in today's digital landscape. Here are some comprehensive recommendations to enhance device security:

- **Awareness and Vigilance**:
  - Maintain constant vigilance and avoid trusting anyone blindly, especially for older generations and children.
  - Always keep devices with you, even in the restroom.
- **Account and Data Management**:
  - Disconnect devices from accounts and clouds before moving to another country.
  - Use unique passwords for personal or work accounts.
  - Format and remove devices from all accounts before selling or giving them away.
- **Hardware Security**:
  - Ensure power banks are not replaced with similar-looking ones containing spyware.
  - Use personal chargers and USBs; avoid leaving devices charging in public places.
- **Password and Access Control**:
  - Do not share passwords with anyone, including children.
  - Monitor anyone using the device and avoid giving the phone to others for taking photos.
  - Change passwords immediately if typed in public places.
- **Legal and Ethical Conduct**:
  - Refrain from engaging in illegal activities to ensure safety and security.
- **Vehicle Security**:
  - Do not lend the car to anyone unless it is equipped with a GPS tracker or camera.
- **Software Updates and Location Services**:
  - Update devices immediately or at least on the same day as the release of new software updates.
  - Keep location services enabled only for essential apps.

[196] Security Basecamp. (April 2022). *Vendor Cybersecurity Due Diligence Process: Best Practice Considerations*. Retrieved from https://www.securitybasecamp.com/wp-content/uploads/2023/11/SBC-Whitepaper-Vendor-Cybersecurity-Due-Diligence-Process-Best-Practice-Considerations-04.01.22.pdf

- **Technology Budget**:
  - Allocate a budget for technology, as it is an essential aspect of modern life.
- **Reading Glasses**:
  - Avoid using reading glasses with blue light protection, as they may reflect what is being read or written if the device camera is hacked.
- **Neighbor Awareness**:
  - Be cautious of neighbors as they may install spyware near shared walls or doors.
- **Device Shutdown and Error Reporting**:
  - Always shut down the device to prevent spyware from accessing it easily.
  - Report errors to the developer section.
- **Link and Group Safety**:
  - Avoid clicking on links from social media or other sources.
  - Do not join public news, sports, or other groups in chat apps.
- **Advertisement and Online Shopping**:
  - Use official websites for online purchases.
- **Use Reputable Brands**:
  - Always buy devices from reputable brands and official websites.
- **Avoid Public Wi-Fi**:
  - Use mobile data or a virtual private network (VPN) to secure the internet connection.
- **Backup Data**:
  - Regularly back up data to a secure location.
- **Use Strong Passwords and Biometrics**:
  - Use strong, unique passwords and enable biometric authentication.
- **Review App Permissions**:
  - Examine the permissions requested by applications.
- **Disable Unused Features**:
  - Turn off Bluetooth, NFC, and location services when not in use.
- **Encrypt Data**:
  - Enable encryption on devices.
- **Monitor Accounts**:
  - Regularly review accounts for unusual activity.
- **Zero Trust Principle**:

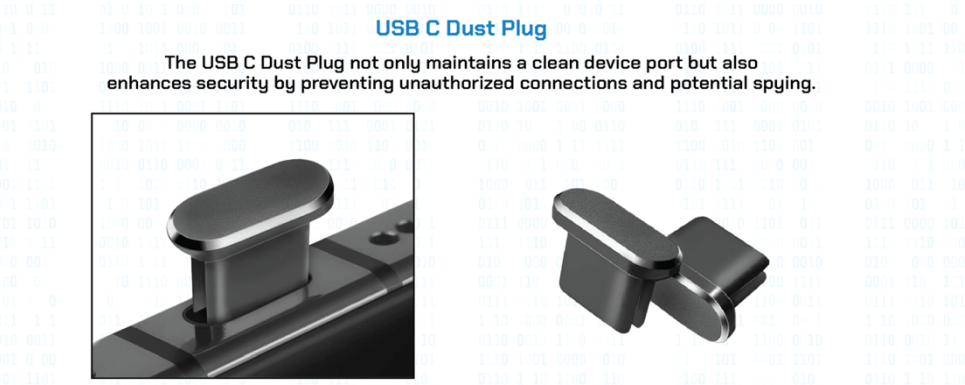
    - Adhere to the principle of "zero trust." Devices should not be trusted with anyone, and strict security practices should be maintained.
- **Use Multi-Factor Authentication (MFA)**:
    - Enable MFA for accounts.
- **Secure the Home Network**:
    - Ensure the home Wi-Fi network is secure.
- **Use Anti-Spyware and Antivirus Software**:
    - Install reputable anti-spyware and antivirus software.
- **Regularly Check for Tracking Devices**:
    - Be vigilant about checking belongings for tracking devices.
- **Avoid Open-Box or Second-Hand Devices**:
    - Do not accept or purchase open-box or second-hand devices.
- **Use Power Banks for Security Cameras**:
    - The installation of security cameras should include connections to auxiliary power systems.
- **Be Cautious with Public Interactions**:
    - Maintain hidden delicate information from public view during your time in open public areas.
- **Stay Informed**:
    - Stay aware with the latest security trends.
- **Hide Option for Passwords**:
    - Use the hidden view during the password change process.
- **Secure Contact Sharing**:
    - Secure contact-sharing solutions between iPhone users choose NameDrop while Android users should use NFC features.

- **Webcam Cover Slide**:
  - Apply a Webcam Cover Slide to protect webcam cameras on computers and tablets.

Figure 5: Webcam Cover Slide[197]

- **USB C Dust Plug**:
  - The USB C Dust Plug is a compact tool designed to protect USB C connectors on electronic devices from dust and unauthorized access. It closes the port, requiring user approval, and prevents malware and spyware from entering devices.

Figure 6: USB C Dust Plug[198]



102- Following these security guidelines will improve device safety and shield personal data along with organizational information from possible risks.

[197] Figure 5: Accessible for online purchasing. Available through searches for "Webcam Cover Slide" or at mobile retail outlets.
[198] Figure 6: Accessible for online purchasing. Available through searches for "USB C dust plug" or at mobile retail outlets.

Conclusion

103- Cybersecurity problems have changed a lot since spyware started out as adware and browser hijackers and now it's used in sophisticated tools for advanced persistent threats and mobile device infections. The report delivers detailed information about spyware development, its different types, and their impacts; it comes from the Center for Global Studies (CGS) under the Parliamentary Assembly of the Mediterranean (PAM) special program.

104- The Parliamentary Assembly of the Mediterranean (PAM), through its Center for Global Studies (CGS) and in cooperation with the Counter-Terrorism Committee Executive Directorate (CTED), actively contributes to fostering a resilient and interconnected digital society by maintaining vigilant and up-to-date cybersecurity measures to counter evolving spyware threats, aligning with the objectives of the Global Digital Compact and the Summit.

105- The protection of personal and organizational data requires a basic understanding of all spyware variants along with their infection approaches together with proper protective steps. The misuse of spyware systems violates human rights and privacy standards through illegal procedures which requires both strict regulatory control and moral governance.

106- Modern smartphone capabilities, jointly AI technology, have advanced spyware in ways that enable better, efficient, and invisible monitoring of user activities. The security protocols discussed in this report need unification to enable people and organizations to protect digital systems and personal space from potential threats.

107- Modern technology requires people to maintain permanent awareness about cybersecurity practices to protect themselves actively ahead of time. Effective spyware protection requires users to update software regularly while implementing robust security measures and restricting application permissions then practicing safe downloading behaviors. This report provides Parliamentarians, legislators, and individuals with practical tools and critical information to help them manage modern cyber security risks and establish a secure digital platform.

108- With the new entrance of the Chinese ‘Mosquito’ spyware into the cyber domain, strict adherence to legal frameworks is essential to avoid consequences that may compromise both individual and national security.