COMPLAINT

against Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland

[hereinafter: Respondent]

regarding an infringement of Article 35(1) in conjunction with Article 34(1) and (2) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act)

Submitted by Gesellschaft für Freiheitsrechte e.V. in cooperation with the project “Ein Team gegen digitale Gewalt”

Translation of a German original

Preliminary Remarks

Gesellschaft für Freiheitsrechte e.V. (Society for Civil Rights, GFF) uses legal means to defend fundamental rights and freedoms. One thematic focus area are fundamental rights in the digital age. In order to enforce online rights more efficiently, GFF has created the Centre for User Rights, which inter alia enforces user rights under the Digital Services Act (Regulation (EU) 2022/2065, DSA). The project “Ein Team gegen digitale Gewalt” (“One Team Against Digital Violence”) has been training counseling centers and women's shelters across Germany in the technical security of private means of communication since 2023. Institut für Technik und Journalismus e.V. (Institute for Technology and Journalism), the project's sponsor, is thus responding to a long-standing demand for further training in the support system.

The subject of the complaint is the advertising of stalking apps via the Respondent’s services. These adverts are displayed to users of the Google search engine through the online advertising programme “Google Ads”, offered as part of the Google search engine. By displaying the adverts, the Respondent is in breach of its obligations as a *very large online search engine* (VLOSE) under the DSA. According to this, it must take reasonable, proportionate and effective measures to mitigate systemic risks stemming from the design, functioning or use of a service (Art. 35(1) in conjunction with Art. 34 DSA).

Stalking apps allow individuals to secretly monitor and control another person’s mobile phone without their consent. Depending on their functionality, stalking apps allow private communications to be read, phone calls to be recorded and the camera and microphone to be accessed remotely. There is evidence that these apps are used to perpetrate and facilitate gender-based violence against girls and women, particularly in the context of (former) partnerships characterised by abuse. Even though the use of such apps is generally illegal, the number of people affected has been increasing for some time. Even if exact figures are not available, they are likely to be high. This is indicated by figures from data leaks.

In the course of our research, we came across numerous adverts from a variety of different providers of stalking apps. They can be easily found both in the Respondent’s Ads Transparency Centre and by using the Respondent’s search engine.

By displaying adverts for stalking apps in a prominent position, the Respondent significantly increases the chance that these apps are found and thus benefits directly through the fees charged. It does not just passively publish the adverts created by the app providers, but actively contributes to increasing the effectiveness and reach of the adverts

by providing AI-supported products and integrating them into the process of creating and displaying ads. This creates a systemic risk in relation to gender-based violence within the meaning of Art. 34(1)(d) DSA and also has actual or foreseeable negative effects on the exercise of fundamental rights within the meaning of Art. 34(1)(b) DSA. The Respondent does not fulfil its duty to mitigate this risk. While the Respondent's advertising guidelines prohibit the advertising of stalking apps, our research strongly suggests that these guidelines are not effectively enforced.

A. Facts of the case

I. Functionality of stalking apps

1 The complaint concerns the advertising of so-called stalking apps. The trade association *Coalition against Stalkerware* defines stalkerware – which also includes stalking apps – as "software, made available directly to individuals, that enables a remote user to monitor the activities on another user's device without that user's consent and without explicit, persistent notification to that user in a manner that may facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence."[1]

2 Stalking apps typically include the following functions:

- Read text messages and messages sent via messenger services and social media services;
- Record phone calls;
- Export contact lists;
- Monitor calendar entries;
- Take photos;
- Create screenshots;
- Locate mobile phone;

---

1 *Coalition against Stalkerware*, Informationen für Medien, https://stopstalkerware.org/de/informationen-fur-medien/ (accessed 17 October 2024).

- Switch on the microphone remotely to listen to calls[2]
- Keylogging (recording of all keystrokes, including passwords).[3]

3 When installing stalking apps on the target device, usually a mobile phone, the customers of the providers usually deliberately bypass the consent of the person concerned. As stalking apps are not usually displayed in the list of installed applications, those affected can hardly recognise them.[4] But even if they are listed, they are hidden among other applications by "harmless" names such as "Sync Service".[5] This is a deliberately designed deceptive component that is considered from the outset during development.

4 Stalking apps are often self-designated as so-called child protection apps. However, child protection apps can be properly distinguished from stalking apps by their limited range of functionalities. According to a study, parents primarily monitor their children's location as well as their route to school and/or screen

---

2 *Kaspersky*, Stalkerware im Jahr 2023, Kaspersky Report, February 2024, S. 8, https://media.kasperskydaily.com/wp-content/uploads/sites/96/2024/03/08131849/The-State-of-Stalkerware-in-2023-DE.pdf?kaspr=stalkerware2023 (accessed 17 October 2024) (hereinafter: Kaspersky Report 2023); *Huwiler/Oesch*, Ein Mann überwacht das Handy seiner Freundin mit einer iranischen Spyware. Dann knackt eine Schweizer Hackerin das System. Einblicke in einen lukrativen Markt, NZZ, 03.02.2024, https://www.nzz.ch/gesellschaft/wenn-der-schatz-auf-handy-mitliest-wie-eine-schweizerin-von-ihrem-partner-mit-iranischer-spyware-ausspioniert-wurde-ld.1775351 (accessed 17 October 2024), (hereinafter: NZZ Report Stalking-Apps 2024); *Coalition against Stalkerware*, What is stalkerware?, https://stopstalkerware.org/ (accessed 17 October 2024).

3 Avira, Stalkerware verbreitet sich immer mehr. Schützen Sie sich davor, https://www.avira.com/de/blog/stalkerware-verbreitet-sich-immer-mehr-schuetzen-sie-sich-davor?srsltid=AfmBOoqQHj97qLP94Q8B83aX_RlJL3HOuoqogKDOnGyQSTZFr_VR4k6k (accessed 17 October 2024). See, e.g., MacTechNews, Spyware auf tausenden Geräten – auch Macs betroffen, https://www.mactechnews.de/news/article/Spyware-auf-tausenden-Geraeten-auch-Macs-betroffen-185337.html (accessed 17 October 2024).

4 Kaspersky Report 2023, p. 8.

5 See, for example, PC Welt, So erkennen Sie Stalkerware auf dem Smartphone, https://www.pcwelt.de/article/1187394/so-erkennen-sie-stalkerware-auf-dem-smartphone.html (accessed 17 October 2024).

time.[6] 95 percent of parents surveyed stated that their children were aware of the monitoring.[7] For 41 percent location monitoring is reciprocal, meaning that children can also track their parents' location.[8] Apps used by parents therefore have significantly fewer functions and are therefore less invasive. In addition, genuine parental control apps can also be differentiated by the fact that they are usually installed with the knowledge of the child concerned and may be based on reciprocity. An app whose presence on the target device is concealed by appearing under a disguised name in the list of apps clearly contradicts this. Hence, while this does not preclude that child protection apps can amount a significant interference with the rights of children and young people, the current complaint is solely directed at stalking apps and excludes child protection apps from its scope. However, such as provided, such a distinction must primarily be drawn based on functionality as providers that advertise the *secret* monitoring of other people's entire online activities are de facto not aimed at parents.

II. Gender-specific dimension

5 The use of stalking apps has a gender-specific dimension. This is mainly due to the fact that the majority of victims of (cyber)stalking are **women and girls**, while the majority of perpetrators are men (**1.**).

6 The majority of (cyber)stalking cases also take place **in relationship contexts**: Either within an existing relationship or committed by former partners. Stalking apps facilitate the control of partners for the purpose of maintaining an abusive relationship and enable further physical or psychological threats and acts of

---

6 *Mavoa et al.*, "It's About Safety Not Snooping": Parental Attitudes to Child Tracking Technologies and Geolocation Data, 2023, Surveillance & Society, Vol. 21issue 1, p. 45 (49), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/15719/10611 (accessed 17 October 2024); *Mols et al.*, Family Surveillance: Understanding Parental Monitoring, Reciprocal Practices, and Digital Resilience, 2023, Surveillance & Society, Vol. 21 issue 4, p. 469 (475 et seq.), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/15645/11067 (accessed 17 October 2024).

7 *Mavoa et al.*, "It's About Safety Not Snooping": Parental Attitudes to Child Tracking Technologies and Geolocation Data, 2023, Surveillance & Society, Vol. 21, issue 1, p. 45 (50), https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/15719/10611 (accessed 17 October 2024).

8 Ibid.

violence. They thus represent a significant tool for perpetrating psychological and physical violence against women (**2.**).

1. Gender gap in (cyber)stalking

7 The use of stalking apps can be categorised as cyberstalking, a phenomenon that is also relevant under criminal law. The EU Directive on combating violence against women and domestic violence defines cyberstalking as a modern form of violence that is often directed against family members or people living in the same household as the perpetrator but is also perpetrated by former partners or acquaintances. The perpetrator usually misuses technology to intensify coercive and controlling behaviour, manipulation, and surveillance, thereby increasing the victim's fear and gradually isolating them from friends, family members, and their professional environment.[9]

8 The figures collected for the area of (cyber)stalking clearly show a gender-specific dimension. The victims of stalking are predominantly female, while the perpetrators are predominantly male. The crime statistics provided by the German police show a total of 23,156 cases of criminal stalking (Section 238 of the German Criminal Code (StGB)) in 2023. Of the total of 18,724 suspects, 15,206 were men.[10] In Germany, 778 people were convicted of stalking (Section 238 StGB) in 2021, 689 of whom were male.[11] The figures are consistent with a study commissioned by Weisser Ring Stiftung, an organisation focusing on the support of victims of crime. According to this study, the lifetime prevalence (based on the study participants) of being stalked at least once in their lifetime is 14.4 percent for women, compared to just 5.1 percent for men.[12] Women were affected by stalking in 83.3 percent of cases.[13] In 93.6 percent of cases, the perpetrator was

---

9 Recital 21 of Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence.

10 Polizeiliche Kriminalstatistik Bund 2023, Table 01, line 207, column P to R, (Exhibit 1).

11 Statistisches Bundesamt, Strafverfolgung 2021, 29 November 2022, Fachserie 10, Reihe 3, p. 34, https://www.destatis.de/DE/Themen/Staat/Justiz-Rechtspflege/Publikationen/Downloads-Strafverfolgung-Strafvollzug/strafverfolgung-2100300217004.pdf?__blob=publicationFile (accessed 17 October 2024).

12 *Dreßing/Gass/Kühner* (Central Institute of Mental Health, Mannheim), Ergebnisse der Stalking-Studie 2018, Abschlussbericht, August 2019, p. 5, https://weisser-ring-stiftung.de/system/files/domains/weisser_ring_stiftung/downloads/praevalenzvonstalkingergebnisse2018.pdf (accessed 17 October 2024).

13 Ibid, p. 6.

known to the victims, with 45 percent of the affected females having been stalked by their former partner.[14]

9 In 2022, the European Institute for Gender Equality published a study on cyber violence against women and girls in the European Union, which analyses the current state of research on cyberstalking.[15] Around 80 percent of stalking victims are women, while 86 percent of perpetrators are men.[16] A full 5 percent of women in the EU have experienced cyberstalking since the age of 15.[17] Cyberstalking tends to occur most frequently in the context of former relationships.[18]

10 This gender gap is reflected in the use of stalking apps. Survey results from the cyber security company *Norton* show that significantly more men use stalking apps than women. People were surveyed in ten countries. In Germany, as in France, men were twice as likely as women to use invasive apps such as stalkerware to spy on partners.[19] In the USA, men are three times more likely to

---

14 Ibid, pp. 9, 12.

15 European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (accessed 17 October 2024).

16 European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, p. 41, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (accessed 17 October 2024) with reference to *Logan*, Examining stalking experiences and outcomes for men and women stalked by (ex)partners and non-partners, Journal of Family Violence, 2020, Vol. 35, No 3, pp. 729-739.

17 European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, p. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (accessed 17 October 2024) with reference to European Union Agency for Fundamental Rights (FAR), Violence against Women: An EU-wide survey - Main results report, 2014, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf (accessed 17 October 2024).

18 European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, p. 41, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (accessed 17 October 2024) with reference to *Dreßing et al.*: Cyberstalking in a large sample of social network users: prevalence, characteristics, and impact upon victims, Cyberpsychology, Behaviour, and Social Networking, 2014, Vol. 17, No 2, pp. 61-67.

19 Norton Cyber Safety Insights Report, Special Release - Online Creeping, Resources, Germany, (Gender breakout), France (Gender breakout), 2021, https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report-special-release-online-creeping/ (accessed 17 October 2024).

use stalking apps than women.[20] Leaked data from the provider Flexispy shows that at least 80 percent of customers are men.[21]

2. Stalking apps as an instrument of physical and psychological violence against women

11 Stalking apps are a significant instrument for perpetrating physical and psychological violence against women. Cyberstalking and in particular the use of stalking apps are usually embedded in relationship contexts characterised by harassment, abuse, and other forms of physical and psychological violence. Women are disproportionately affected by violence from (former) relationship partners (**2.1**). Cyberstalking and other forms of violence are closely linked (**2.2**). Against this backdrop, the use of stalking apps favours violence against women (**2.3**). The problem is becoming more serious as the number of users increases (**2.4)**.

2.1 Violence in (former) partnerships predominantly affects women

12 Violence in relationships is a structural problem. In the vast majority of cases, the violence is directed against women. According to the Federal Criminal Police Office's Federal Situation Report on Domestic Violence in Germany in 2023, 70.5 percent of victims were female and 75.6 percent of suspects were male.[22] In the sub-category of intimate partner violence, 79.2 percent of victims were female and 77.6 percent of suspects were male. The most prominent crimes in this category are intentional bodily harm (59.1 percent), and threats, stalking, and

---

[20] Norton Cyber Safety Insights Report, Special Release - Online Creeping, Resources, US, Gender breakout, 2021, https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report-special-release-online-creeping/ (accessed 17 October 2024).

[21] *Locker/Hoppenstedt*, Mehr als tausend Deutsche nutzen Spionage-App: "100 Prozent Erfolg - übermorgen ist meine Scheidung", Vice, 4 May 2017, https://www.vice.com/de/article/ezjdbj/mehr-als-tausend-deutsche-nutzen-spionage-app-100-prozent-erfolg-uebermorgen-ist-meine-scheidung (accessed 17 October 2024).

[22] Bundeskriminalamt, Bundeslagebild Häusliche Gewalt, 2023, V. 1.0, p. 4, (Exhibit 2).

coercion with a total of 24.6 percent.[23] This gender-specific breakdown is in line with the results of US studies.[24]

2.2 Cyberstalking and other forms of violence are closely linked

13 The studies analysed by the European Institute for Gender Equality show that cyberstalking and physical stalking cannot be separated, but often merge and form a continuum. Physical stalking is a risk factor for cyberstalking and, conversely, stalking that begins online can lead to physical acts or other forms of cyber violence.[25] In over half of cyberstalking cases (54 percent), the first encounter with the stalker is said to have taken place offline, according to a British study.[26] In many cases, cyberstalking is a fundamental factor in violence in couple relationships.[27] Data from a 2014 survey shows that 7 out of 10 women who have

---

[23] Ibid, p. 5.

[24] Cf. US Department of Justice (Statistics Division), Special Report: Intimate Partner Violence, 1993 - 2010, November 2012, revised 29 September 2012, p. 1, https://bjs.ojp.gov/content/pub/pdf/ipv9310.pdf (accessed 17 October 2024); Office for Victims of Crime, Intimate Partner Violence, no publication date, p. 1, (Exhibit 3); *Black, M.C. et al*, The National Intimate Partner and Sexual Violence Survey (NISVS): 2010 Summary Report. Atlanta, GA: National Center for Injury Prevention and Control, Centers for Disease Control and Prevention, 2011, pp. 2, 9, https://www.nsvrc.org/sites/default/files/2021-04/NISVS_Report2010-a.pdf (accessed 17 October 2024).

[25] European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, p. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (accessed 17 October 2024) with reference to *Reyns/Fisher*, The Relationship between offline and online stalking victimisation: a gender-specific analysis, Violence and Victims, 2018, Vol. 33, No 4, pp. 769-786.

[26] European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, p. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (accessed 17 October 2024) with reference to *Maple/Short/Brown,* Cyber Stalking in the United Kingdom: An analysis of the ECHO pilot survey, 2011, p. 14, https://uobrep.openrepository.com/bitstream/handle/10547/270578/ECHO_Pilot_Final.pdf?sequence=1&isAllowed=y (accessed 17 October 2024).

[27] European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, p. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (accessed 17 October 2024) with reference to *Al-Alosi*, Cyber-violence: digital abuse in the context of domestic violence, University Of New South Wales Law Journal, Vol. 40, No 4, pp. 1573-1603.

experienced cyberstalking have also experienced at least one form of physical and/or sexualised violence from an intimate partner.[28]

14 In a survey conducted by cyber security company *Kaspersky*[29], 23 percent of 21,000 respondents from 21 countries said they had experienced some form of cyberstalking by someone they had recently been with. More than a third (39 percent) reported experiences of violence or abuse by a current or former partner. 10 percent of respondents said their location had been tracked, a further 10 percent had experienced unauthorised access to their social media accounts or emails, and 7 percent had had stalking software installed on their device without their knowledge.

2.3 Stalking apps as an essential part of violence against women

15 Stalking apps play a crucial role in this context. The use of stalking apps enables the monitoring of relationship partners, their harassment, abuse and stalking in other forms and/or violence.[30]

16 Stalking apps have been a recognised phenomenon in the context of violence against women worldwide for several years. According to the Bundesverband Frauen gegen Gewalt e.V. (Federal Association Women Against Violence), almost all of the 176 women's advice centres and women's helplines in Germany were already confronted with the problem of stalking apps in 2016.[31] Experts from

---

[28] European Institute for Gender Equality, Combating Cyber Violence against Women and Girls, 2022, p. 40, https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf (accessed 17 October 2024) with reference to European Union Agency for Fundamental Rights (FAR), Violence against Women: An EU-wide survey - Main results report, 2014, available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf (accessed 17 October 2024).

[29] Kaspersky Report 2023, p. 9.

[30] *Coalition against Stalkerware*, Information für Technologieunternehmmen, https://stopstalkerware.org/de/informationen-fur-technologieunternehmen/ (accessed 17 October 2024).

[31] *Locker/Hoppenstedt*, Mehr als tausend Deutsche nutzen Spionage-App: "100 Prozent Erfolg - übermorgen ist meine Scheidung", Vice, 04.05.2017, https://www.vice.com/de/article/ezjdbj/mehr-als-tausend-deutsche-nutzen-spionage-app-100-prozent-erfolg-uebermorgen-ist-meine-scheidung (accessed 17 October 2024).

advice centres report that such covert apps have become a massive threat to the safety of their clients in recent years.[32]

17 Figures from other countries support this finding. According to the US-based *National Network to End Domestic Violence*, 71 percent of domestic violence perpetrators monitor their victims' computer activity and 54 percent monitor their mobile phones using stalking apps.[33] A 2013 survey by Australia's *Domestic Violence Resources Centre Victoria* found that 82 percent of abuse victims also reported abuse using smartphones, while 74 percent of practitioners surveyed reported that stalking via apps was common among their clientele.[34]

18 In Canada, a 2012 survey of anti-violence workers found that 98 percent of perpetrators used technology to intimidate or threaten their victims, 72 percent of perpetrators had hacked the email and social media accounts of the women and girls involved, another 61 percent had hacked computers to monitor online activity and extract information, and another 31 percent had installed computer monitoring software.[35]

19 Cyberstalking, and therefore also the use of stalking apps, is thus not an isolated problem that only has an impact in the "virtual" world. Rather, the associated surveillance can also lead to physical violence. The mere fact that perpetrators know the exact location of the victim and can see from text messages, for example, whether women are alone in a certain place, enables and facilitates

---

[32] *Köver*, Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung, 2021, p. 227 (228), https://www.transcript-verlag.de/shopMedia/openaccess/pdf/oa9783839452813.pdf (accessed 17 October 2024).

[33] *Citizen Lab*, The Predator in your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry, Research Report No. 119, June 2019 (hereinafter: Citizen Lab Stalkerware Study 2019), p.1, https://citizenlab.ca/docs/stalkerware-holistic.pdf (accessed 17 October 2024) with reference to *Citron*, Spying Inc., 2015, Washington and Lee Law Review, Vol. 72, No 3, pp. 1243-1282.

[34] *Citizen Lab* Stalkerware Study 2019, p.1 with reference to *Woodlock*, Technology-facilitated Stalking: Findings and Recommendations from the SmartSafe Project, SmartSafe, 2014.

[35] *Citizen Lab* Stalkerware Study 2019, p.1 with reference to *Safety Net Canada,* Assessing Technology in the Context of Violence Against Women & Children: Examining Benefits & Risks, British Columbia Society of Transition Houses, 2013, pp. 6, 71.

physical assaults. There are also real effects on the psyche of those affected, such as anxiety or depression.[36]

2.4 Rising numbers of people affected by stalking apps

20 Data suggests that the number of users of stalking apps is increasing and accordingly, so is the risk of being monitored with a stalking app.

21 Exact figures on downloads from the major app stores, for example, are not available. The providers of stalking apps generally do not or cannot choose this distribution channel (compared to less invasive parental controls) (see **A.III.**)**.** In addition, the use of the apps often goes unnoticed due to their purpose. Even if the person concerned notices the use, they do not always file a criminal complaint. Nevertheless, the number of people affected by the secret use of stalking apps and the number of perpetrators is likely to be high. This is indicated by data hacks and leaks from stalking app providers. For example, over 2 million data records from the provider *mSpy* were publicly accessible. The data records included iCloud usernames and passwords of those affected, text messages, location data and caller data.[37] In total, 195 different stalking apps were discovered by a cybersecurity company in 2023.[38]

22 The risk of being monitored through the use of stalking apps has likely risen sharply in recent years, both worldwide and in Germany. This is suggested by figures published by cybersecurity companies. According to these figures, a total of 31,031 individual users worldwide were affected by stalking apps in 2023. This corresponds to an increase of 5.86 percent compared to 2022. Most cases within Europe were registered in Germany.[39] The trend of rising user numbers has

---

36 *Short/Linford/Wheatcroft/Maple*, The Impact of Cyberstalking: The Lived Experience - A Thematic Analysis, 2014, Studies in Health Technology and Informatics, Vol. 199, pp. 133-137; *Logan*, Examining Stalking Experiences and Outcomes for Men and Women Stalked by (Ex)partners and Non-partners, 2019, Journal of Family Violence, Vol. 35, pp. 729-739.

37 *Krebs*, Krebs on Security: For 2nd Time in 3 Years, Mobile Spyware Maker mSpy Leaks Millions of Sensitive Records, 4 September 2018, https://krebsonsecurity.com/2018/09/for-2nd-time-in-3-years-mobile-spyware-maker-mspy-leaks-millions-of-sensitive-records/ (accessed 17 October 2024); Techcrunch: Mobile spyware maker leaks 2 million records, 5 September 2018, https://techcrunch.com/2018/09/05/mobile-spyware-maker-leaks-2-million-records/ (accessed 17 October 2024).

38 Kaspersky Report 2023, p. 8.

39 Kaspersky Report 2023, p. 3, 6.

existed for some time: according to cybersecurity companies, the number has already increased dramatically in the period from January 2020 to December 2022 by 239 percent worldwide and by 575 percent in Germany in particular.[40]

III. Prohibition of advertising stalking apps by the Respondent

23 In August 2020, the Respondent updated its "Enabling Dishonest Behavior policy".[41] Since then, the Respondent's advertising guidelines expressly prohibit the advertising of "[p]roducts or services that enable a user to track or monitor another person or their activities without their authorization". In particular, the ban includes "[s]pyware and technology used for intimate partner surveillance including but not limited to spyware/malware that enable a user to monitor texts, phone calls, or browsing history".[42]

24 Stalking apps hidden on the smartphone also violate the guidelines of the Google Play Store, the distribution platform for application software.[43] Apple, the Respondent's main competitor in terms of operating app stores, also does not allow such apps – with the exception of monitoring apps aimed at parents – in its App Store.[44]

---

40 *Avast*, Stalkerware wächst deutschlandweit um 575 Prozent in den letzten drei Jahren, 14 March 2023, https://press.avast.com/de-de/stalkerware-wachst-deutschlandweit-um-575-prozent-in-den-letzten-drei-jahren (accessed 17 October 2024) (hereinafter: Avast 2023); *Avast*, Stalkerware Grows 239% Worldwide Over the Past Three Years, 14 March 2023, https://investor.gendigital.com/news/news-details/2023/Stalkerware-Grows-239-Worldwide-Over-the-Past-Three-Years/default.aspx (accessed 17 October 2024).

41 *Google*, Aktualisierung der Richtlinie zur Ermöglichung von unlauterem Verhalten, August 2020, https://support.google.com/adspolicy/answer/9726908?hl=de&sjid=4462208304556098119-EU (accessed 17 October 2024).

42 Google Ads Werberichtlinien: Ermöglichung unlauteren Verhaltens, 2024, https://support.google.com/adspolicy/answer/6016086?hl=de&sjid=5524670563677541947-EU, (accessed 17 October 2024).

43 See Google Play-Richtlinie zu Malware, https://support.google.com/googleplay/android-developer/answer/9888380?#stalkerware (accessed 31 October 2024).

44 *Apple*, App-Prüfungsrichtlinien: 5.1.1 Datenerfassung und -speicherung, lit. viii., April 2024, p. 33, https://developer.apple.com/support/downloads/terms/app-review-guidelines/App-Review-Guidelines-20240913-German.pdf (accessed 17 October 2024).

IV. The advertising of stalking apps via the Respondent's advertising programme

25 Despite the prohibition in the Respondent's advertising guidelines, adverts from the providers of stalking apps and their products can be found without effort via the Respondent's search engine by entering relevant search terms. The Respondent even supports advertising providers of stalking apps in booking and designing adverts as part of its general offers to advertisers (see **1.**). Advertising via adverts booked with the Respondent is decisive for the findability of apps and stalking apps in particular (see **2.**). In fact, providers of stalking apps book adverts with the Respondent to a considerable extent. The Respondent is aware of this (see **3.**).

1. Application procedure via the Respondent's advertising programme

26 Advertising via the Respondent's advertising programme works as follows: Using a Google Ads account, advertisers specify, among other things, the text and description of the advert, the target group and the search terms ("keywords") for which the advert is to be delivered. Typical search terms that lead to relevant hits include „Partner Handy überwachen" (monitor partner mobile phone) or „freundin handy überwachen" (monitor girlfriend mobile phone). If users of the search engine enter search terms in the search bar that match the keywords specified by advertisers, the search results display the adverts separately labelled before and between the organic search results. Advertisers can use the Respondent's automated AI programmes for both ad creation and ad delivery. Among other things, these programmes suggest suitable ad texts and titles as well as search terms and automatically create personalised ads tailored to the respective search query when the search terms are entered. In this way, the Respondent itself significantly increases the effectiveness and reach of the adverts through its own additional offer.

27 In detail:

1.1 The definition of search terms

28 In order to advertise products such as stalking apps via Google Ads, the respective providers must specify certain search terms in a Google Ads account created for this purpose, in addition to the text of the advert, the geographical scope of the campaign, the target group and the budget, for which the advert is

to be delivered. Advertisers can not only define their own search terms but can also have corresponding search terms suggested by an AI-supported programme of the Respondent, the so-called “Keyword Planner”. Based on either the content of the website specified by the advertiser or the search terms already entered manually by the advertiser, the programme automatically generates new suitable search terms for which the advertisements are to be displayed to users of the Respondent’s search engine. The advertiser can then add the search terms generated in this way to its advertising campaign.[45]

29 Irrespective of the separate use of the *Keyword Planner* tool, the Respondent already uses the information provided by the advertiser on the target group of the advertising campaign as a basis for recommending further search terms in the regular ad creation process in order to increase the ad’s reach.[46]

1.2 The definition of advert texts

30 After defining the search terms, advertisers create the advert. However, the Respondent also offers it support during this step. If the advertiser activates the “Responsive Search Ads” function, an AI-based programme automatically suggests ad headlines and ad description texts that potentially match the content available at the URL after the advertiser’s URL has been entered. The programme uses content that, in the AI’s experience, is particularly popular with search engine users. Advertisers can select this content to create the advert. As a rule, several different ad headlines and description text lines are specified by advertisers.[47]

1.3 Selection of the most effective text and title combination in the course of the respective search using "Responsive Search Ads"

31 Adverts booked in this way are not static nor fixed at the end of the creation process. Instead, they are generated anew for each person when they enter a

---

[45] *Google*, Google Ads Hilfe: Keyword-Planer, 2024, https://support.google.com/google-ads/answer/7337243?hl=de&sjid=16595194781768165231-EU#zippy=%2Ca-ideen-f%C3%BCr-neue-keywords-abrufen (accessed 17 October 2024).

[46] *Google*, Ihre erste Google Ads-Kampagne einrichten, no publication date, https://ads.google.com/intl/de_de/home/how-it-works/, (accessed 17 October 2024).

[47] *Google,* Google Ads: Responsive Search Ads. A Guide to Writing Ads that Perform, no publication date, p. 6, https://services.google.com/fh/files/misc/responsive_search_ads_a_guide_to_writing_ads_that_perform_2023.pdf (accessed 17 October 2024).

search term. Specifically, the Respondent combines the headlines and descriptions selected by the advertisers into a customised ad during the search process. With the AI-based "Responsive Search Ads" function, the Respondent's programme automatically selects the ad headline and description that comes closest to the interest of each user based on an analysis of their previous behaviour. Only this customised search ad is displayed to users. In this way, the Respondent increases the likelihood that its users will click on an advert. For instance, if a user searches for "running shoes", the Respondent's AI programme should now display the headline that matches the previous search behaviour from the headline options provided by the advertisers (e.g., "marathon shoes" instead of "shoes for sprinting" if the user previously searched for "best places to run a marathon").[48]

2. Relevance of the application for the discoverability of stalking apps

32 Advertising via the Respondent's search engine is a crucial part of making users discover and access stalking apps. This follows from the interplay of several factors:

- Since stalking apps are banned from both Apple's App Store and the Respondent's Google Play Store and thus the central distribution channels for smartphone apps (see above under **A.III.**), online advertising and search ads have a significant impact on app installations (**2.1**)**.**

- The Respondent's market dominance on the market for search engines (and search ads) increases the proliferation of these apps: By using the Respondent's advertising programme, stalking apps are made accessible to a very large group of people who would otherwise not have found these apps or would have found them only with difficulty (**2.2**).

- Stalking apps would not be discoverable to the same extent via organic search results without the display of adverts by the Respondent (**2.3**).

---

[48] See *Google*, Google Ads: Unlock the Power of Search. Inside Google AI-powered ads, no publication date, p. 8 and 24 https://services.google.com/fh/files/misc/unlock_the_power_of_search_2022.pdf (accessed 17 October 2024).

2.1 Effect of online advertising and search ads on app installations

33 According to a study, 40 percent of users find new apps via search engines. This puts search engines in second place, directly behind the use of app stores (46 percent).[49] A survey by the Respondent points in the same direction: it comes to the conclusion that 31 percent of users become aware of new apps via online adverts while surfing the internet and 21 percent via search engines.[50]

34 Online advertising plays a crucial role for companies. In 2023, online advertising in Germany accounted for 49.7 percent of the total net revenue of all advertising media (including print, television, etc.).[51] It has a much more positive impact on company turnover and company value than offline advertising.[52] There are also differences between the various forms of online advertising. For example, the *paid search advertising* of interest here, i.e., paid adverts that are displayed for certain search terms alongside the organic results of a search engine (search ads), leads to far higher increases in sales compared to *online display advertising*. The latter refers to advertising using banner ads, text, media content, or promotional videos (display ads).[53] This is reflected in the economic development of the advertising market as a whole: net advertising revenue from search ads rose by 11.8 percent in 2023, while display ads grew by just 6.4 percent.[54] According to a report, the Respondent is said to have earned around USD 46 million with “Google search & other” in the first quarter of 2024.[55] It can be assumed that a large part of this comes from advertising revenue.

---

49 *Marketing Charts*, Here’s How US Adults Discover Apps, and Why They Keep Using Them, 13 June 2024, https://www.marketingcharts.com/digital/mobile-phone-229739 (accessed 17 October 2024).

50 *Google*, How people discover, use, and stay engaged with apps, October 2016, p. 5, https://www.thinkwithgoogle.com/_qs/documents/331/how-users-discover-use-apps-google-research.pdf (accessed 17 October 2024).

51 *ZAW*, Werbemarkt nach Medien, no publication date, https://zaw.de/branchendaten/werbemarkt-nach-medien/ (accessed 17 October 2024).

52 *Bayer, E. et al*: The impact of online display advertising and paid search advertising relative to offline advertising on firm performance and firm value, In: International Journal of Research in Marketing, December 2020, Issue 37, No. 4, p. 789 (pp. 790, 801) (Exhibit 4).

53 Ibid, p. 801.

54 See *ZAW*, Werbemarkt nach Medien, no publication date, https://zaw.de/branchendaten/werbemarkt-nach-medien/ (accessed 17 October 2024), (11.8 percent compared to 6.4 percent growth for “display ads” incl. video streaming).

55 Alphabet Investor Relations, Alphabet Announces First Quarter 2024 Results, p. 2, https://abc.xyz/assets/91/b3/3f9213d14ce3ae27e1038e01a0e0/2024q1-alphabet-earnings-release-pdf.pdf (accessed 17 October 2024).

2.2 Increased access opportunities due to the market power of the Respondent

35 In this context, the Respondent has enormous market power. In the period from 1 January 2024 to 30 July 2024, the Respondent's online search engine had an average of 377,400,000 users per month based on users logged in with their Google account. Based on distinguishable sessions of non-logged-in users, it had an average monthly number of 448,000,000 users.[56]

36 The Respondent's online search engine has a global market share of 79.62 percent in terms of search engine usage on desktops and a global market share of 94.08 percent on mobile devices.[57] Only recently, a US court ruled in an antitrust dispute that the Respondent maintained a monopoly position with its search engine.[58]

2.3 No equivalent exposure without the display of the adverts by the Respondent

37 Without the Respondent's adverts, stalking apps would not be found among organic search results for relevant search terms to the same extent as they currently are. Organic search results for relevant search terms predominantly refer to trustworthy sources that inform users about the dangers of stalking apps.

38 This is because there is not yet one established app that is sufficiently well-known even without advertising. In addition, some of the providers regularly change their names – from "SpyHide" to "oospy", for example.[59] In addition, the names of the stalking apps themselves are often generic and without any major unique selling

---

[56] *Google*, Information about Monthly Active Recipients under the Digital Services Act (EU), 16 August 2024, p. 2, https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-24_2024-1-1_2024-6-30_en_v1.pdf (accessed 17 October 2024).

[57] *Statista Research Department*: Marktanteile der Suchmaschinen weltweit nach mobiler und stationärer Nutzung im September 2024, 2 October 2024 https://de.statista.com/statistik/daten/studie/222849/umfrage/marktanteile-der-suchmaschinen-weltweit/ (accessed 17 October 2024).

[58] The New York Times, 5 August 2024, https://www.nytimes.com/interactive/2024/08/05/technology/google-antitrust-ruling.html (accessed 17 October 2024).

[59] NZZ Report Stalking Apps 2024; see *Köver*, Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung, 2021, p. 227 (234 et seq.), https://www.transcript-verlag.de/shopMedia/openaccess/pdf/oa9783839452813.pdf (accessed 17 October 2024).

points (like “uMobix” and “mektabyt”). This makes it difficult to find the providers’ websites. As a result, stalking apps are often not found by searching for a specific app name. Instead, users search with more general or contextualised terms, such as “monitor mobile phone girlfriend”. When these and corresponding search terms are entered, ads are prioritised and displayed before organic search results. As a result, stalking apps are found immediately, while the providers’ websites only appear in lower-ranking search results, if at all.

3. Advertisements for stalking apps displayed by the Respondent’s search engine

39 The research on which the complaint is based has revealed that the Respondent displays a large number of adverts for stalking apps via its search engine. It has been actively aware of the placement of adverts by operators of stalking apps for many years. Nevertheless, evidence suggests that the Respondent continues to allow these apps to be advertised contrary to its own guidelines.[60]

40 Two methodological starting points were chosen for the search. First, the Respondent’s search engine was used to search with contextualised terms. Second, the Respondent’s advertising archive was used to trace which adverts the Respondent displayed in a specific time window.

41 By setting up the advertising archive[61], the *Ads Transparency Centre*, the Respondent is fulfilling its corresponding obligation under the DSA. Art. 39 DSA obliges VLOSE to set up an advertising archive. Art. 39(2) 2 DSA specifies the minimum information that must be included. This includes the total number of users reached. In the entries of the Respondent’s advertising archive, the respective target groups of the advertisement and the extent of visibility can be traced for each advert displayed. It documents how often an advert was displayed on the Respondent’s platforms, broken down by delivery location of the advert. However, a search in the advertising archive presupposes that the name of the advertiser is known. Since there are a large number of stalking app providers, a conclusive search of the advertising archive is hardly possible. Consequently, the

---

[60] See also *Williams,* in: MIT Technology Review, Google is failing to enforce its own ban on ads for stalkerware, 12 May 2022, https://www.technologyreview.com/2022/05/12/1052125/google-failing-stalkerware-apps-ads-ban/ (accessed 17 October 2024).

[61] *Google*, Ads Transparency Centre, https://adstransparency.google.com/?region=DE (accessed 17 October 2024).

following results are by no means conclusive. However, this extract alone evidences that a significant amount of adverts is displayed.

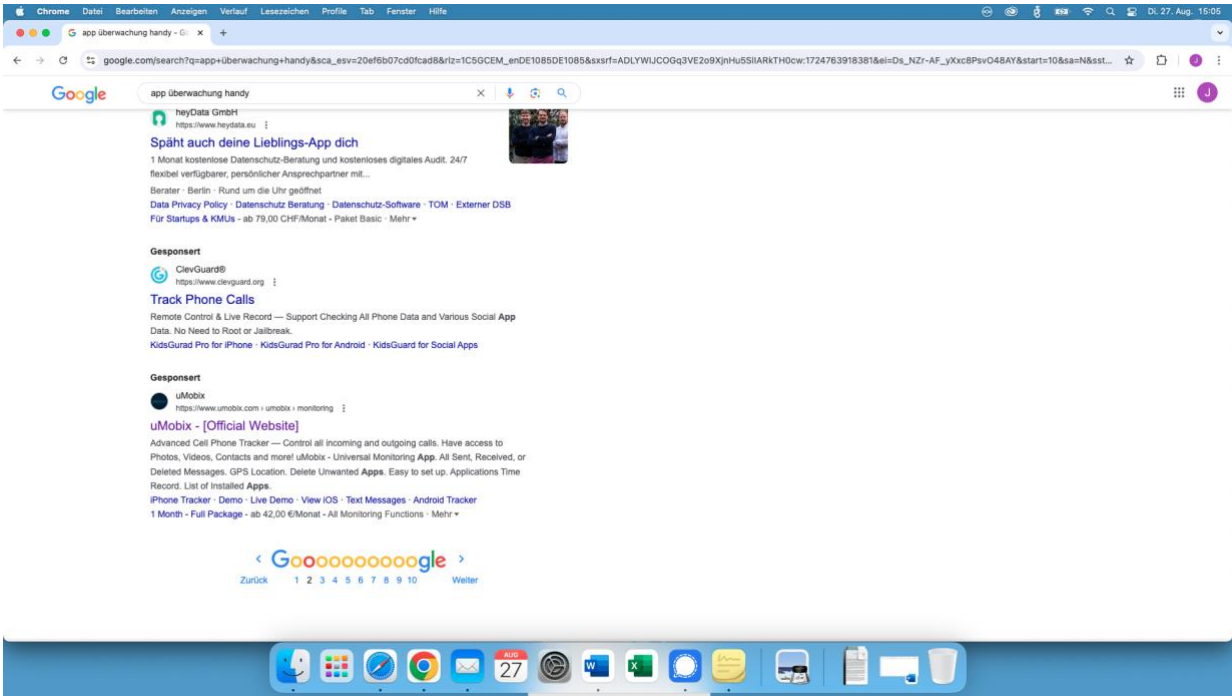
42 In addition, our search results revealed adverts that are missing from the advertising archive. According to the Respondent[62], this may be due to the fact that it takes up to 72 hours for information about the advert to become available. Other reasons for the absence of the advert in the advertising archive could be that the advert has already been removed due to a policy violation, has not been displayed in the last 365 days or is only one of many variants of the advert. However, none of these explanations explained our finding of an advert from the stalking app provider “mekatbyt.com”. Even three days later, the advert could not be found in the advertising archive after another search. It is questionable whether this is due to technical limitations of the advert, but this is rather unlikely given the nature of the advert (see **Exhibit 23.1**).

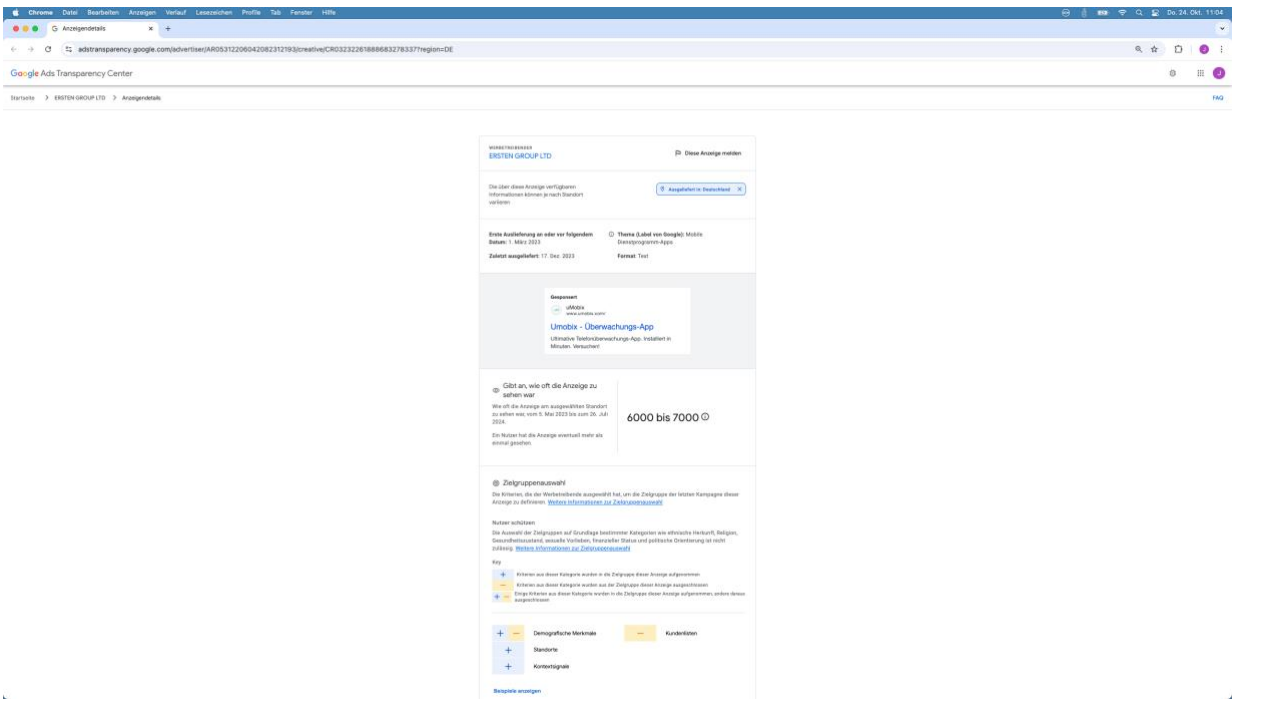
43 In our research, we found ads by the following providers of stalking apps: uMobix, mSpy, Spynger, ClevGuard, SpyX, Haqerra, spyera, Spytech SpyAgent, GuardW, SpyBubble, Msafely, TiSpy, Spylix, Cicispy, FamiSpy, Spy366 PRO, phonemonitor, geistertrupp, zyslen, and mektabyt.

1) uMobix [63]

[62] *Google,* Ads Transparency Centre FAQ, https://adstransparency.google.com/faq (accessed 17 October 2024).

[63] https://umobix.com (accessed 14 October 2024).


app überwachung handy
heyData GmbH
https://www.heydata.eu
Späht auch deine Lieblings-App dich
1 Monat kostenlose Datenschutz-Beratung und kostenloses digitales Audit. 24/7 flexibel verfügbarer, persönlicher Ansprechpartner mit...
Berater · Berlin · Rund um die Uhr geöffnet
Data Privacy Policy · Datenschutz Beratung · Datenschutz-Software · TOM · Externer DSB
Für Startups & KMUs - ab 79,00 CHF/Monat - Paket Basic · Mehr
Gesponsert
ClevGuard®
https://www.clevguard.org
Track Phone Calls
Remote Control & Live Record — Support Checking All Phone Data and Various Social App Data. No Need to Root or Jailbreak.
KidsGurad Pro for iPhone · KidsGurad Pro for Android · KidsGuard for Social Apps
Gesponsert
uMobix
https://www.umobix.com › umobix › monitoring
uMobix - [Official Website]
Advanced Cell Phone Tracker — Control all incoming and outgoing calls. Have access to Photos, Videos, Contacts and more! uMobix - Universal Monitoring App. All Sent, Received, or Deleted Messages. GPS Location. Delete Unwanted Apps. Easy to set up. Applications Time Record. List of Installed Apps.
iPhone Tracker · Demo · Live Demo · View iOS · Text Messages · Android Tracker
1 Month - Full Package - ab 42,00 €/Monat - All Monitoring Functions · Mehr
Gooooooooooogle
Zurück 1 2 3 4 5 6 7 8 9 10 Weiter


Google Ads Transparency Center
ERSTEN GROUP LTD
Diese Anzeige melden
Ausgeliefert in Deutschland
Erste Auslieferung an oder vor folgendem Datum: 1. März 2023
Zuletzt ausgeliefert: 17. Dez. 2023
Thema (Label von Google): Mobile Überwachungsprogramm-Apps
Format: Text
Gesponsert
uMobix
Umobix - Überwachungs-App
Ultimative Telefonüberwachungs-App. Installiert in Minuten. Versuchen!
Gibt an, wie oft die Anzeige zu sehen war
6000 bis 7000
Zielgruppenauswahl
Demografische Merkmale
Kundenlisten
Standorte
Kontextsignale
Beispiele anzeigen

- **Search term** „App Überwachung Handy“ (App surveillance mobile phone), 27 August 2024

- **Advertising archive**: records similar adverts from the same provider that have been displayed 6,000 to 7,000 times in Germany

- **Functionalities of the app**: hidden monitoring of

    - Social media applications

    - Incoming and outgoing calls and messages

    - Contact list, videos, photos, and audio recordings

    - Keylogging

    - GPS localisation

    - Remote access to the device

2) mSpy[64]

- **Search term**: „WhatsApp heimlich mitlesen“ (WhatsApp secretly read along), 27 August 2024 (**Exhibit 5.1**)

- **Advertising archive**: records similar adverts from the same provider that were displayed 3,000 to 4,000 times in Germany (**Exhibit 5.2**)

- **Functionalities** of the app: hidden monitoring of

    - Common social media applications

    - Incoming and outgoing calls and messages

    - Contact list

[64] https://mspy.mobi (accessed 14 October 2024).

- Browser history
- Calendar
- Videos, photos, and audio recordings
- Keylogging
- GPS localisation of the device

3) Spynger[65]

- **Search term**: “Spynger App”, 29 August 2024 (**Exhibit 6.1**)
- **Advertising archive**: records similar adverts from the same provider that were played 25,000 to 30,000 times in Germany (**Exhibit 6.2**)
- **Functionalities** of the app: hidden monitoring of the
  - social media applications used
  - Listening to incoming and outgoing calls
  - Access to photos and videos
  - GPS localisation
  - Keylogging

4) ClevGuard[66]

- **Search term**: „Freundin Handy ausspionieren“ (spy on girlfriend mobile phone), 27 August 2024 (**Exhibit 7.1**)

---

65 https://spynger.net/de (accessed 14 October 2024).
66 https://www.clevguard.de (accessed 14 October 2024).

- **Advertising archive**: records similar adverts from the same provider that were displayed 40,000 to 45,000 times in Germany (**Exhibits 7.2, 7.3, 7.4**)
- **Functionalities** of the app: hidden monitoring of
  - Common social media applications
  - Incoming and outgoing calls and messages
  - Contact list
  - Browser history
  - Calendar
  - Videos, photos, and audio recordings
  - GPS localisation of the device

5) SpyX[67]

- **Search term**: „Freundin Handy ausspionieren“ (spy on girlfriend mobile phone), 27 August 2024 (**Exhibit 8.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed 250,000 to 300,000 times in Germany (**Exhibits 8.2**)
- **Functionalities** of the app: hidden monitoring of
  - Common social media applications
  - Incoming and outgoing calls and messages
  - Contact list

[67] https://spyx.com/de (accessed 14 October 2024).

- Browser history
- Calendar
- Videos, photos, and audio recordings
- Keylogging
- GPS localisation of the device

6) Haqerra[68]

- **Search term**: “Handy Spion kostenlos” (mobile phone spy for free), 27 August 2024 (**Exhibit 9.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed 25,000 to 30,000 times in Germany (**Exhibits 9.2**)
- **Functionalities** of the app: hidden monitoring of
  - Common social media applications
  - Incoming and outgoing calls and messages
  - Contact list
  - Browser history
  - Calendar
  - Videos, photos, and audio recordings
  - Keylogging
  - GPS localisation

[68] https://haqerra.net (accessed 14 October 2024).

7) Spyera[69]

- **Search term**: “Spyera”, 29 August 2024 (**Exhibit 10.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed 3,000 to 4,000 times in Germany (**Exhibit 10.2**)
- **Functionalities** of the app: hidden monitoring of
  - Common social media applications
  - Incoming and outgoing calls and messages
  - Contact list
  - Browser history
  - Calendar
  - Videos, photos, and audio recordings
  - Keylogging
  - GPS localisation/geofencing
  - Monitoring of the device using screenshots
  - Control via microphone and monitoring of the surrounding area

8) Spytech SpyAgent[70]

- **Search term**: „Freundin Handy Überwachen Unsichtbar“ (girlfriend mobile phone monitoring invisible), 27 August 2024 (**Exhibit 11.1**)

---

69 https://spyera.com/de/ (accessed 14 October 2024).
70 https://www.spytech-spyagent.com (accessed 14 October 2024).

- **Advertising archive**: records similar adverts from the same provider that were displayed 15,000 to 20,000 times in Germany (**Exhibits 11.2, 11.3**)
- **Functionalities** of the app: hidden monitoring
    - Common social media applications
    - Incoming and outgoing calls and messages
    - Contact list
    - E-mails
    - Browser history
    - Calendar
    - Videos, photos, and audio recordings
    - Key and mouse logging
    - Monitoring the device using screenshots

9) GuardW [71]

- **Search term**: “Handy Spion Kostenlos” (mobile phone spy for free), 27 August 2024 (**Exhibit 12.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed 3,000 to 4,000 times in Germany (**Exhibits 12.2, 12.3**)
- **Functionalities** of the app: hidden monitoring of
    - Common social media applications

[71] https://www.guardw.net/de/ (accessed 14 October 2024).

- Incoming and outgoing calls and messages
- Contact list
- Browser history
- Calendar
- Videos, photos, and audio recordings
- GPS localisation

10) SpyBubble[72]

- **Search term**: “Guard Spy App”, 29 August 2024 (**Exhibit 13.1**)
- **Advertising archive**: records similar adverts from the same provider that have been displayed between 10,000 and 15,000 times in Germany (**Exhibit 13.2**)
- **Functionalities** of the app: hidden monitoring of
  - Common social media applications
  - Incoming and outgoing calls and messages
  - Contact list
  - Browser history
  - Videos, photos, and audio recordings
  - Keylogging
  - GPS localisation

[72] https://spybubblepro.com (accessed 14 October 2024).

11) Msafely[73]

- **Search term**: „Freundin Handy Ausspionieren“ (girlfriend mobile phone spying), 27 August 2024 (**Exhibit 14.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed between 30,000 and 35,000 times in Germany (**Exhibit 14.2**)
- **Functionalities** of the app: hidden monitoring of
    - Common social media applications
    - Incoming and outgoing calls and messages
    - Contact list
    - Browser history
    - E-mails
    - Videos, photos, and audio recordings
    - Keylogging
    - GPS localisation/geofencing

12) TiSpy[74]

- **Search term**: „Freundin Handy Ausspionieren“ (girlfriend mobile phone spying), 27 August 2024 (**Exhibit 15.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed 7,000 to 8,000 times in Germany (**Exhibit 15.2**)

---

[73] https://msafely.com (accessed 14 October 2024).
[74] https://tispy.net (accessed 14 October 2024).

- **Functionalities** of the app: hidden monitoring of
    - Common social media applications
    - Incoming and outgoing calls and messages
    - Contact list
    - Browser history
    - Calendar
    - Videos, photos, and audio recordings
    - Keylogging
    - GPS localisation
    - Screen recording

13) Spylix[75]

- **Search term**: „Freundin Handy Ausspionieren“ (girlfriend mobile phone spying), 27 August 2024 (**Exhibit 16.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed 2,000 to 3000 times in Germany (**Exhibit 16.2**)
- **Functionalities** of the app: hidden monitoring of
    - Common social media applications
    - Incoming and outgoing calls and messages
    - Contact list

[75] https://www.spylix.com (accessed 14 October 2024).

- Browser history
- Videos, photos, and audio recordings
- Keylogging
- GPS localisation

14) CiciSpy[76]

- **Search term**: „Handy klonen“ (clone mobile phone), 27 August 2024 (**Exhibit 17.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed 4,000 to 5,000 times in Germany (**Exhibits 17.2, 17.3, 17.4**)
- **Functionalities** of the app: hidden monitoring of
  - Common social media applications
  - Incoming and outgoing calls and messages
  - Contact list
  - Browser history
  - Calendar
  - Videos, photos, and audio recordings
  - Keylogging
  - GPS localisation

[76] https://www.cicispy.com (accessed 14 October 2024).

15) FamiSpy[77]

- **Search term**: „Freundin Handy Ausspionieren“ (girlfriend mobile phone spying), 29 August 2024 (**Exhibit 18.1**)
- **Advertising archive**: similar ads from the same provider that were displayed up to 1,000 times in Germany (**Exhibit 18.2**)
- **Functionalities** of the app: hidden monitoring of
  - Common social media applications
  - Incoming and outgoing calls and messages
  - Contact list
  - E-mails
  - Browser history
  - Videos, photos, and audio recordings
  - Keylogging
  - Monitoring the device using screenshots

16) Spy366PRO[78]

- **Search term**: „Freundin Handy Ausspionieren“ (girlfriend mobile phone spying), 29 August 2024 (**Exhibit 19.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed between 20,000 and 25,000 times in Germany (**Exhibit 19.2**)

---

77 https://famispy.com/de/ (accessed 14 October 2024).
78 https://spy366.pro (accessed 14 October 2024).

- **Functionalities** of the app: hidden monitoring of
    - Common social media applications
    - Incoming and outgoing calls and messages
    - Contact list
    - E-mails
    - Browser history
    - Videos, photos, and audio recordings
    - Keylogging
    - Monitoring the device using screenshots

17) PhoneMonitor[79]

- **Search term**: „Überwachung Partnerin Handy“ (surveillance partner mobile phone), 29 August 2024 (**Exhibit 20.1**)
- **Advertising archive**: records similar adverts from the same provider that have been displayed up to 1,000 times in Germany (**Exhibits 20.2, 20.3**)
- **Functionalities** of the app: hidden monitoring of
    - Social media applications
    - Web activities
    - Incoming and outgoing telephone calls and messages
    - Remote access to the smartphone

[79] https://phonemonitor.com (accessed 14 October 2024).

- GPS localisation

18) Geistertrupp[80]

- **Search term**: “Spy App”, 29 August 2024 (**Exhibit 21.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed 4,000 to 5,000 times in Germany (**Exhibit 21.2**)
- **Functionalities** of the app: “hacking” into
  - Various social media applications
  - Listening to calls
  - GPS localisation
  - Message recovery

19) Zyslen[81]

- **Search term**: „Freundin Handy Ausspionieren“ (girlfriend mobile phone spying), 29 August 2024 (**Exhibit 22.1**)
- **Advertising archive**: records similar adverts from the same provider that were displayed 150,000 to 175,000 times in Germany (**Exhibit 22.2**)
- **Functionalities** of the app: depending on the package booked, the monitoring of
  - WhatsApp messages
  - All applications on the smartphone

---

[80] https://www.geistertrupp.com (accessed 14 October 2024).
[81] https://zyslen.com (accessed 14 October 2024).

- General communication
- GPS localisation
- Browsing history
- Remote access

20) mektabyt [82]

- **Search term**: “Überwachung Partnerin Sofort” (surveillance partner now), 29 August 2024 (**Exhibit 23.1**)
- **Advertising archive**: not recorded in the advertising archive, no advert was listed in the advertising archive even 72 hours after the first search (**Exhibit 23.2**)
- **Functionalities** of the app:
  - Interception of telephone calls
  - Viewing of photos and videos
  - Monitoring messages and call list

[82] https://www.mektabyt.com (accessed 14 October 2024).

B. Legal assessment: Violation of Art. 35(1) in conjunction with Art. 34 DSA

44 The evidence we collected suggests that the Respondent is in breach of its duty to mitigate risks pursuant to Art. 35(1) in conjunction with Art. 34 DSA.

45 Pursuant to Art. 35(1) DSA, providers of very large online platforms and very large online search engines shall put in place reasonable, proportionate, and effective risk mitigation measures, tailored to the specific systemic risks identified pursuant to Art. 34. Particular consideration must be given to the impact of such measures on fundamental rights. In accordance with Art. 35(1) DSA, this may include adapting their advertising systems and adopting targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide.

46 As a VLOSE, the Respondent is the addressee of the risk mitigation obligation (**I.**). Although systemic risks within the meaning of Art. 34(1) DSA stem from the advertising of stalking apps (**II.**), it has not taken sufficient risk mitigation measures (**III.**).

I. Respondent as provider of a very large online search engine

47 The Respondent is the addressee of the risk mitigation obligation pursuant to Art. 35(1) DSA.

48 The standard is aimed at providers of very large online platforms and very large online search engines. The Respondent operates the Google search engine which the European Commission has designated as a VLOSE within the meaning of Art. 33 DSA pursuant to Art. 33(4) DSA.[83]

[83] *European Commission*, Commission Decision of 25 April 2023, https://digital-strategy.ec.europa.eu/de/library/designation-decisions-first-set-very-large-online-platforms-vlops-and-very-large-online-search (accessed 17 October 2024).

II. Systemic risks stem from the advertising of stalking apps

49 The advertising of stalking apps via Google Ads creates systemic risks within the meaning of Art. 34(1)(b) and (d) DSA.

50 The negative effects of the advertising of stalking apps in relation to gender-based violence and the exercise of fundamental rights constitute systemic risks (**1.**). These result from the operation of the advertising programme linked to the Respondent's search engine (**2.**).

1. Systemic risks

51 The conditions for a systemic risk (**1.1**) are met (**1.2**)**.**

1.1 Definition and assessment of systemic risks

52 The DSA does not define the term "systemic risk". Its meaning must therefore be determined by interpretation (**1.1.1**). Whether a risk is systemic can be determined – in the absence of case law – using an assessment standard developed by the Commission (**1.1.2**). The assessment is based on the risk categories contained in Art. 34(1)(a) to (d) DSA, which include in particular all actual or foreseeable negative effects in relation to gender-based violence (d) as well as any actual or foreseeable negative effects for the exercise of fundamental rights (lit. b) (**1.1.3**).

1.1.1 Interpretation of the concept of systemic risk

53 Systemic risks are hazards that – in contrast to individual legal violations and hazards that are limited to individual affected parties – have an overarching quality that affects public interests. They are systemic because the structure and functioning of VLOSEs contribute to the fact that individual hazards regularly develop a wide range or that a risk arises from a large number of legal violations, which takes on a systemic significance beyond the sum of the individual cases.[84]

---

[84] *Beyerbach,* in: Müller-Terpitz/Köhler: Digital Services Act, 2024, Art. 34 para. 14.

54 In this respect, systemic risks can be understood as structural risks of platform or search engine operation.[85]

1.1.2 Evaluation standard

55 When assessing the risk, the probability and the severity must be taken into consideration (Art. 34(1) DSA). Providers could, for example, consider whether the possible negative effects could affect a large number of people, are irreversible, or how difficult it is to remedy the possible effects and restore the previous situation (Recital 79 DSA).

56 In August 2023, the European Commission published a document entitled “Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns”, specifying its understanding of the requirements of Art. 34 DSA for risk assessment. The assessment standard it sets out relates specifically to disinformation campaigns and is aimed at researchers. Nevertheless, some of the criteria have a more general character. According to this, for a risk to be considered “systemic” within the meaning of Art. 34 DSA, a proportionality assessment must be carried out depending on quantitative and qualitative factors.[86]

57 The risk assessment therefore consists of two steps: a qualitative risk assessment followed by a quantitative risk assessment.[87] The qualitative risk assessment is based on the risk categories listed in Art. 34(1) DSA.[88] The subsequent quantitative assessment aims to determine and evaluate the reach, i.e., the extent to which the content has been disseminated.[89] The higher the level of risk inherent in the content in context, the smaller the audience required to reach a systemic level. And by contrast, the lower the level of risk inherent in the content in context, the larger the audience required to reach a systemic level.[90]

---

85 *Beyerbach,* in: Müller-Terpitz/Köhler: Digital Services Act, 2024, Art. 34 para. 15.
86 *European Commission*, Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns, August 2023, 1st edition, p. 15, https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1 (accessed 17 October 2024).
87 Ibid, p. 15 ff.
88 Ibid, p. 15.
89 Cf. ibid., p. 17.
90 Ibid. S. 15.

58 The qualitative and quantitative evaluation criteria are also reflected in the United Nations Guiding Principles on Business and Human Rights as scale and scope.[91] These are considered recognised standards for assessing negative impacts of businesses on human rights and are complemented by a third criterion, the remediability of the impact. This criterion is also embedded in Recital 79 of the DSA.

1.1.3 Risk categories

59 Art. 34(1) DSA contains four categories of systemic risks which, according to the assessment in the German legal literature, are to be understood as non-exhaustive examples.[92]

60 According to the wording, these categories must always be taken into account. Pursuant to Art. 34(1) DSA, this includes the dissemination of illegal content, any actual or foreseeable negative effects for the exercise of fundamental rights, any actual or foreseeable negative effects on civic discourse and electoral processes, and public security, as well as any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences on a person's physical and mental well-being.

61 Two risk categories are particularly significant here:

a) Category 4: "effects in relation to gender-based violence"

62 The fourth category includes, all actual or foreseeable negative effects in relation to gender-based violence (Art. 34(1)(d) DSA). The European legislator thus recognises the importance of the structural problem of violence against women (see **A.II.2.1** above).

---

[91] *United Nations*, Guiding Principles on Business and Human Rights, 2011, p. 16, https://www.undp.org/asia-pacific/bizhumanrights/publications/guiding-principles-business-and-human-rights (accessed 31 October 2024).

[92] *Beyerbach,* in: Müller-Terpitz/Köhler: Digital Services Act, 2024, Art. 34 para. 18; *Kaesling,* in: Hofmann/Raue: Digital Services Act, 1st ed. 2023, Art. 34 para. 57.

63 With regard to the risk of gender-based violence, Art. 34(1)(d) DSA requires actual or foreseeable negative effects. This means that the negative effects do not have to have materialised; a certain likelihood that these effects will occur is sufficient.[93]

64 In contrast to the category of negative consequences to the person's physical and mental well-being (see Art. 34(1)(d) DSA), no threshold of "serious negative consequences" applies with regard to the negative effects in relation to gender-based violence.[94] The fact that forms of gender-specific violence, as a particular structural form of violence, can in principle already be covered by the first two risk categories, and yet has been listed by the legislator as an additional risk category, shows that the risks relating to gender-specific violence are of particular importance.

65 Recital 10 of Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence can be used to define the term "gender-based violence". Accordingly, violence against women is a form of gender-based violence inflicted primarily on women and girls by men. It is rooted in socially constructed roles, behaviour, activities and attributes that a given society considers appropriate for women and men.

b) Category 2: "any actual or foreseeable negative effects for the exercise of fundamental rights"

66 Another category of risk is any actual or foreseeable negative effects for the exercise of fundamental rights (Art. 34(1)(b) DSA). The DSA is intended to ensure an online environment in which the fundamental rights enshrined in the Charter are effectively protected (Recital 9). Art. 34(1)(b) DSA lists individual fundamental rights by way of example, but not exhaustively ("in particular"). These include Art. 7 of the Charter (respect for private and family life) and Art. 8 of the Charter (protection of personal data). This risk category covers the fundamental rights dimension of all structural risks encountered on platforms.[95] It expresses the

---

93 *Beyerbach,* in: Müller-Terpitz/Köhler: Digital Services Act, 2024, Art. 34 para. 16.
94 *Kaesling,* in: Hofmann/Raue: Digital Services Act, 1st ed. 2023, Art. 34 para. 109.
95 *Kaesling,* in: Hofmann/Raue: Digital Services Act, 1st ed. 2023, Art. 34 para. 75.

indirect (horizontal) effect of fundamental rights, i.e., the influence that private actors can have on the exercise of such rights.[96]

1.2 Evaluation of Advertising stalking apps

67 Advertising stalking apps has actual and foreseeable negative effects in relation to gender-based violence pursuant to Art. 34(1)(d) DSA and for the exercise of the fundamental rights enshrined in Arts. 7 and 8 of the Charter in connection with Art. 34(1)(b) DSA.

68 The threshold of a systemic risk has been reached. This is evident from the qualitative (**1.2.1**) and quantitative (**1.2.2**) assessment as well as the assessment of the remediability of the impacts (**1.2.3**).

1.2.1 Qualitative evaluation

69 Advertising stalking apps results in a particularly high qualitative risk. Stalking apps have serious consequences in individual cases and violate highly personal rights.

70 Stalking apps have a gender-specific dimension. They are a technical tool for cyberstalking and part of violence against women (see **A.II.**). They therefore have actual, or at least foreseeable, effects in relation to gender-specific violence. Based on its wording, Art. 34(1)(d) DSA does not require the effects to reach a threshold. Even if such a threshold were to be required, we assume that this threshold would have been met due to the severe effects on persons affected by cyberstalking and stalking apps in particular. These effects are often connected with other forms of psychological and physical violence (see **A.II.2.**).

71 In addition, there are actual or at least foreseeable negative effects for the exercise of the fundamental rights to respect for private and family life and the protection of personal data enshrined in Arts. 7 and 8 in connection with Art. 34(1)(b) DSA. Stalking apps allow full access to devices and the personal data they contain (see **A.I.**). Some of the data is highly personal, such as communication content, photos, data in period tracking apps, etc.

---

[96] *Kaesling,* in: Hofmann/Raue: Digital Services Act, 1st ed. 2023, Art. 34 para. 76.

1.2.2 Quantitative evaluation

72 The more serious the risk of the advertised product can affect the individual person, the lower the actual reach, i.e., the number of adverts displayed, must be in order to reach the systemic risk threshold.

73 Hence, as the negative effects are severe for the individual person, the facilitation of ads for stalking apps can be considered a systemic risk even if only a limited number of people were affected. However, Google Transparency Centre shows that stalking app ads also have a considerable reach (**A.IV.3.**). Thus, their quantitative dimension is high as well. This is exacerbated by the Respondent's considerable market power (**A.IV.2.2**).

1.2.3 Remediability of the impacts

74 Considering that pursuant to the United Nations Guiding Principles on Business and Human Rights and Recital 79 of the DSA, the risk assessment includes considering whether an impact is irreversible and how difficult it is to remedy the potential impacts and restore the situation prevailing prior to the potential impact,[97] the findings become more severe. The psychological and physical effects on individuals affected by stalking apps cannot be undone and often burden them for life.

2. Risk from the respondent's advertising programme

75 The systemic risks described above arise from the operation of the Respondent's advertising programme which linked to the search engine (**2.1**). The above-mentioned risks stem from the provision and operation of this programme (**2.2**).

---

[97] See also *Ebert et al*, The Business & Human Rights Dimension oft he Digital Services Act, 31.08.2023, https://freiheitsrechte.org/uploads/publications/Digital/Grundrechte-im-Digitalen/The-Business-Human-Rights-Dimension-of-the-Digital-Services-Act.pdf (accessed 31 October 2024).

2.1 The respondent's advertising programme as a system linked to the VLOSE

76 In accordance with Art. 34(1) DSA, potential risks may arise not only from the operation of the service itself, but also from systems connected to a service, including algorithmic systems.

77 The Respondent's advertising programme constitutes a system linked to the operation of the Respondent's search engine, and thus as a system linked to a VLOSE – with a partly platform-like character – within the meaning of Art. 34(1) DSA.

78 The advertising programme itself has not yet been classified as a very large online platform (VLOP). However, it is embedded in the Respondent's search engine service and represents a system connected to the Google search engine that has platform-like elements.

79 The classification of the Respondent's advertising programme as an online platform pursuant to Art. 3(i) DSA is supported by the fact that the programme enables advertisers to store and publicly disseminate information (here in the form of advertisements) to a specific group of people. This includes all users of the search engine who use specified search terms. However, for objective and technical reasons, the advertising programme cannot be used without the search engine service, as adverts are published as part of the search results. The advertising function (Google Ads) and the search function (search engine) interact closely, particularly due to the respondent's AI tools (see **A.IV.1.** above).

80 The fact that systemic risks can also arise from advertising systems is set out in Art. 34(2)(d) DSA. According to this, providers should also consider the influences of the systems for selecting and displaying advertising. Art. 35(1)(e) DSA also explicitly targets advertising systems with regard to the risk mitigation measures to be taken.

2.2 Link between risks and advertising programme

81 The systemic risks are directly related to the functioning of the advertising programme.

82 Art. 34(1) DSA presupposes that the risks arise from the design or functioning of the service and its related systems, including algorithmic systems, or the use of their services.

83 In view of the effect of online advertising via search ads (see **A.IV.1.**) and the limited distribution channel outside the common app stores (see **A.III.**), it is only the advertising via the Respondent's search engine that achieves the visibility and subsequent use of stalking apps. The reach that this type of advertisement has due to the market power of the Respondent is considerable (see **A.IV.2.2**).

84 Moreover, the Respondent does not merely passively publish adverts created by providers. Instead, it even actively contributes to increasing the effectiveness and reach of such adverts by providing and using AI programmes (see **A.IV.1.** above). It is precisely the use of such algorithmic systems that the EU legislator expressly had in mind when establishing systemic risks, as the wording of Art. 34(1) DSA underlines. Without the display of adverts by the Respondent, stalking apps would not be discoverable to the same extent (see **A.IV.2.**). By displaying adverts, the Respondent therefore increases the risk of the use of such apps and thus also of the gender-based violence associated with this use and the detrimental effects on the exercise of fundamental rights.

III. Inadequate risk mitigation by the Respondent

85 The Respondent has not taken sufficient measures to mitigate the risks described.

86 According to Art. 35(1) DSA, providers of VLOSEs are obliged to take reasonable, proportionate, and effective risk mitigation measures that are tailored to the specific systemic risks identified pursuant to Art. 34 DSA. According to Art. 35(1)(e) DSA, this includes in particular the adaptation of their advertising systems and the adoption of targeted measures aimed at limiting or adjusting the presentation of advertisements in association with the service they provide. Recital 88 DSA provides that corrective measures may include, in particular, the cessation of advertising revenue for certain information.

87 The problem posed by stalking apps, as well as the advertisement of these apps by the Respondent has been the subject of public debate for several years (see **A.IV.3.** above). The Respondent has apparently recognised the risks associated with the advertising in principle by banning stalking apps from its Play-Store and prohibiting the advertising of these apps on its platforms (see **A.III.** above).

88 Nevertheless, the result of our research, i.e., that advertisement for stalking apps is still easily found on the Respondent's search engine, makes it very doubtful that the Respondent has in fact taken sufficient measures to adequately reduce the risk. Instead of enforcing its own advertising guidelines, the Respondent even generates revenue from the advertising business with the providers of the stalking apps (see **A.IV.2.1** above).

89 According to the Respondent's advertising guidelines, it is inadmissible to advertise stalking apps via Google Ads. However, this is not sufficient as a risk mitigation measure as the Respondent does not sufficiently enforce these guidelines, at least not consistently, as evidenced by the advertisements that continue to be displayed and are presumably decisively shaped by the AI-supported tools provided by the Respondent (see **A.IV.1.** above). Hence, one it can be assumed that this is issue exists not only in sporadic individual cases but rather that the ban itself is not sufficiently implemented in practice. Likewise, the European Commission itself has voiced its assessment that the mere existence of a regulatory framework is not sufficient to eliminate a systemic risk. Instead, the effectiveness of a risk mitigation measure is characterised by, among other things, how quickly and how regularly respective regulations are enforced in individual cases.[98]

90 Against this background, we come to the conclusion that the Respondent has not sufficiently fulfilled its mitigation obligation.

IV. Art. 65(2) DSA

91 Finally, as the present case concerns an infringement of the provisions of Chapter III Section 5, we suggest that a request be sent to the Commission to examine the matter in accordance with Art. 65(2) DSA, as there is reason to believe that the Respondent, as a provider of a VLOSE, is in breach of Art. 35(1) in conjunction with Art. 34 DSA.

---

98 *European Commission*, Digital Services Act: Application of the Risk Management Framework to Russian disinformation campaigns, August 2023, 1st edition, p. 21, https://op.europa.eu/en/publication-detail/-/publication/c1d645d0-42f5-11ee-a8b8-01aa75ed71a1 (accessed 17 October 2024).

List of Exhibits

Polizeiliche Kriminalstatistik Bund 2023, Table 01, line 207, columns P to R (Exhibit 1)

Bundeskriminalamt, Bundeslagebild Häusliche Gewalt, 2023, V. 1.0 (Exhibit 2)

Office for Victims of Crime, Intimate Partner Violence, no publication date, p. 1, (Exhibit 3)

Bayer, E. et al: The impact of online display advertising and paid search advertising relative to offline advertising on firm performance and firm value, In: International Journal of Research in Marketing, December 2020, Issue 37 Issue 4, p. 789 (p. 790, 801) (Exhibit 4)

mSpy (Exhibit 5.1, 5.2)

Spynger (Exhibit 6.1, 6.2)

ClevGuard (Exhibit 7.1, 7.2, 7.3, 7.4)

SpyX (Exhibit 8.1, 8.2)

Haqerra (Exhibit 9.1, 9.2)

spyera (Exhibit 10.1, 10.2)

Spytech SpyAgent (Exhibit 11.1, 11.2, 11.3)

GuardW (Exhibit 12.1, 12.2, 12.3)

SpyBubble (Exhibit 13.1, 13.2)

Msafely (Exhibit 14.1, 14.2)

TiSpy (Exhibit 15.1, 15.2)

Spylix (Exhibit 16.1, 16.2)

Cicispy (Exhibit 17.1, 17.2, 17.3, 17.4)

FamiSpy (Exhibit 18.1, 18.2)

Spy366 PRO (Exhibit 19.1, 19.2)

phonemonitor (Exhibit 20.1, 20.2, 20.3)

geistertrupp (Exhibit 21.1, 21.2)

zyslen (Exhibit 22.1, 22.2)

mektabyt (Exhibit 23.1, 23.2)