European Court of Human Rights

Salman BUTT v. the United Kingdom Application no. 32946/20

WRITTEN SUBMISSIONS OF PRIVACY INTERNATIONAL

Introduction and summary of intervention

1. This intervention is submitted by Privacy International (PI), pursuant to leave granted by the President of the Section in accordance with Rule 44(3) of the Rules of the Court. PI is a human rights organization that works globally at the intersection of modern technologies and human rights and is dedicated to promoting the right to privacy.

2. The present case concerns the gathering and processing, by the Extremism Analysis Unit ("EAU") of the UK Home Office, of publicly available data concerning the applicant's allegedly extremist views and the EAU's assessment based on those data that the applicant was an extremist. The applicant's personal data seems to have been obtained by the EAU from several sources, including his profile on social media platforms, such as Facebook and Twitter. This case presents the Court with a unique opportunity to reaffirm the applicability of Article 8 of the Convention and the protections afforded by it with regard to individuals' private social and political life as well as their democratic identity in the digital era.

3. This submission aims to assist the Court in its consideration of the compatibility of the aforementioned conduct by the UK Home Office with Article 8 of the Convention. It is structured in three parts. First, it will explain the serious risks social media monitoring poses to individuals' privacy and other fundamental rights, and modern democracies as a whole. Second, it will assert that, in accordance with the Court's case-law, the mere processing of an individual's social media personal data by public authorities, should be regarded as a serious interference with their right to respect for private life. This should be irrespective of the systematic nature of the processing or whether personal data have been manifestly made public by the individual, especially in cases where the personal data processed can reveal political opinions. Third, it will highlight the need for robust safeguards governing the processing of individuals' social media personal data. This should, at the very minimum, include provisions for the effective exercise of individuals' data protection rights, as well as transparency and accountability mechanisms, including independent oversight. The severity of the interference means it should only be permitted where strictly necessary and subject to appropriately robust safeguards.

Social media monitoring raises serious risks for individuals' fundamental rights as well as for modern democracies

4. Social media platforms have come to play a vital role for the development of individuals' private social and political life, as well as their online identity. They constitute the digital life setting of today's civic spaces where people formulate and discuss ideas, raise dissenting views, consider possible reforms, expose bias and corruption, and organise to advocate for political, economic, social, environmental, and cultural change.[1]

5. At the same time, the wealth of information hosted on social media platforms, which can range from names and photos to political and religious views, physical and mental health of users and their families or friends, has attracted the interest of public authorities and law enforcement. The latter are increasingly - overtly or covertly - monitoring social media accounts for various purposes, including preventing or detecting crime or threats to national security. This monitoring can take various forms and usually involves the manual or automatic review of content posted in public or private groups or pages; review of results of searches and queries of users; review of activities or types of content users post; or "scraping" – extracting data,

[1] PI, Protecting Civic Spaces: Defending Democracy and Dissent, May 2019 p. 1 https://privacyinternational.org/sites/default/files/2019-07/Protectin%20civic%20spaces%20PI%20May%202019.pdf

including the content of a web page – and replicating content in ways that are directly accessible to the person gathering social media intelligence. Notably, social media intelligence may include tools to collect, retain, and analyse a vast range of social media data and interpret that data into trends and analyses.[2]

6. In the UK, Guidance produced by the Association of Chief Police Officers of England, Wales, and Northern Ireland on the policing of anti-fracking protests in 2011 suggests that, "[s]ocial media is a vital part of any … intelligence picture".[3] Protests at a widespread cull of badgers in 2013 were closely monitored through social media analysis.[4] A 2013 report suggested that a staff of 17 officers in the National Domestic Extremism Unit was scanning the public's tweets, YouTube videos, Facebook profiles, and anything else UK citizens post in the public online sphere.[5] The UK Chief Surveillance Commissioner's Annual Report 2014-15 stated that:

> Perhaps more than ever, public authorities now make use of the wide availability of details about individuals […] that are provided on social networking sites and a myriad of other means of open communication between people using the Internet and their mobile communication devices. I repeat my view that just because this material is out in the open, does not render it fair game.[6]

7. In 2019, PI investigated the use of "overt" social media intelligence by the Local Authorities in Great Britain. Following an exercise involving a total of 251 Freedom of Information Act (FOIA) requests, PI found that 62.5% of Local Authorities that responded were using "overt" social media monitoring, while 31% were using "covert" social media monitoring.[7] The key distinction between "overt" and "covert" social media intelligence is that "overt" surveillance relies only on publicly available information, whereas "covert" surveillance involves attempts to add the targeted user as a validated contact, to use fake profiles, to obtain further information than what is publicly available.[8] Our research also revealed that Local Authorities could monitor social media accounts, such as Facebook, as part of their intelligence gathering and investigation tactics regarding subjects as diverse as council tax payments, children's services, benefits, and monitoring protests and demonstrations. In some cases, local authorities will go so far as to use such information to make accusations of fraud and withhold urgently needed support from families who are living in extreme poverty.[9]

8. PI's research also indicated that there is no quality check on the effectiveness of this form of intrusive surveillance on decision making, while it constitutes a serious interference with privacy as analysed below. Social media monitoring is used by the local authorities without individuals' knowledge or awareness, in a wide variety of their functions, predominantly intelligence gathering and investigations.[10]

9. It is important to emphasise that the risks surrounding the use of social media monitoring by public authorities and law enforcement do not only pertain to the right to privacy but may often

---

[2] PI, Social Media Intelligence, October 2017 https://privacyinternational.org/explainer/55/social-media-intelligence
[3] Association of Chief Police Officers, Policing linked to Onshore Oil and Gas Operations, 2011 https://netpol.org/wp-content/uploads/2015/08/Onshore-Oil-and-Gas-Operations-2015.pdf
[4] Brian Wheeler, Whitehall chiefs scan Twitter to head off badger protests, BBC News, 20 June 2013 https://www.bbc.co.uk/news/uk-politics-22984367
[5] Paul Wright, Meet Prism's Little Brother: Socmint, Wired, 26 June 2013 https://www.wired.co.uk/article/socmint
[6] Office of Surveillance Commissioners, Annual Report, 2015 https://www.ipco.org.uk/docs/OSC%20Annual%20Report%202014-15.pdf
[7] PI, Is your Local Authority looking at your Facebook likes?, May 2020 p. 15 https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020.pdf
[8] PI, Social Media Intelligence, October 2017 https://privacyinternational.org/explainer/55/social-media-intelligence
[9] See below para 29.
[10] PI, Is your Local Authority looking at your Facebook likes?, May 2020, p. 24 https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020.pdf
[10] PI, Social Media Intelligence, October 2017 https://privacyinternational.org/explainer/55/social-media-intelligence

negatively impact the exercise of other fundamental rights, especially freedoms of expression and peaceful assembly, threatening as such the very existence of modern democracies.

10. Further, the European Data Protection Supervisor (EDPS) has rightly underscored:

> Social media users monitoring is a personal data processing activity that creates high risk for individuals' rights and freedoms. Repurposing of data is likely to affect a person's information self-determination, further reduce the control of data subjects' over their data... Indeed, the diminution of intimate space available to people, as a result of unavoidable surveillance by companies and governments, has a chilling effect on people's ability and willingness to express themselves and form relationships freely, including in the civic sphere so essential to the health of democracy.[11]

11. The United Nations Human Rights Council has urged caution with regard to social media surveillance. General Comment No. 37 on Article 21 of the International Covenant on Civil and Political Rights (Right of peaceful assembly), adopted by the UN Human Rights Committee, established that:

> The mere fact that assemblies take place in public does not mean that participants' privacy is not capable of being infringed… The same applies to the monitoring of social media to glean information about participation in peaceful assemblies. Independent scrutiny and oversight must be exercised over the collection of personal information and data of those engaged in peaceful assemblies.[12]

The monitoring of social media accounts by authorities constitutes a serious interference with the right to respect for private life (Article 8§1 ECHR)

12. In determining whether there has been an interference with individuals' "private life", the Court has on several occasions investigated whether individuals *"had a reasonable expectation that their privacy would be respected and protected"* (*Barbulescu v. Romania* [GC], App. No. 1496/08, §73). It has underlined that *"a reasonable expectation of privacy is a significant though not necessarily conclusive factor"* (*Halford v. UK*, App. No. 20605/92, §45), and that a series of other factors will also be taken into account such as *"the question whether there has been compilation of data on a particular individual, whether there has been processing or use of personal data or whether there has been publication of the material concerned in a manner or degree beyond that normally foreseeable"* (*Uzun v. Germany*, App. No. 35623/05, §45).

13. As the Court rightly held in *Peck v. UK* (App. No. 44647/98, §§61-62), the disclosure to the media for broadcast use of video footage of the applicant whose suicide attempt was caught on close circuit television cameras [constituted] a serious interference with the applicant's private life, notwithstanding that he was in a public place at the time. In that case, the Court's reasoning rested on the assumption that no person could reasonably expect footage depicting sensitive aspects of their private life to be later released in the media, even if their actions are *"already in the public domain"* (Ibid).

14. Similarly, in *Perry v. UK* (App. No. 63737/00), the Court held that the overt video surveillance of an individual in a police station for the purposes of using the footage in subsequent proceedings did constitute processing or use of personal data of a nature to amount to an interference with his private life. The Court noted:

> Whether or not he was aware of the security cameras running in the custody suite, there is no indication that the applicant had any expectation that footage was being taken of him within the police station for use in a video identification procedure and, potentially, as evidence prejudicial to his defence at trial. This ploy adopted by the police went beyond the normal or expected use of this type of camera... (§41)

[11] EDPS, Formal consultation on EASO's social media monitoring reports (case 2018-1083), p.3 https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf
[12] Human Rights Committee, General Comment 37 para 72 https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx

15. In certain cases, the Court has held that even the *"mere storing"* of an individual's data would be enough to engage Article 8. In its landmark judgment in *S. and Marper v. UK* (App. Nos. 30562/04 and 30566/0), the Grand Chamber noted:

> The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 [...]. The subsequent use of the stored information has no bearing on that finding. (§67)

16. *S. and Marper* concerned the processing of biometric data of individuals, such as fingerprints and DNA samples. Due to their sensitive nature, such data are regarded as "special category data", under both Council of Europe Convention 108+ (§6) and the EU General Data Protection Regulation (GDPR) (§4) which all Council of Europe member states are bound by. The exact same protections are afforded by both these texts with regard to data revealing "political opinions" such as those at issue in the present case.

17. In *Breyer v. Germany* (App. No 50001/12), the Court further expanded this reasoning to apply to all categories of personal data, regardless of their sensitivity. It reiterated:

> the mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 of the Convention. [The Court] takes furthermore note of the Federal Constitutional Court's finding that the extent of protection of the right to informational self-determination under domestic law was not restricted to information which by its very nature was sensitive and that, in view of the possibilities of processing and combining, there is no item of personal data which is in itself, that is, regardless of the context of its use, insignificant. (§81)

18. The Court has held on multiple occasions that a broad interpretation of "private life", in the context of personal data, corresponds with that of the Convention 108+, the purpose of which is "*to protect every individual [...] with regard to the processing of their personal data, thereby contributing to respect for [...] the right to privacy*" (*Amann v. Switzerland* [GC], App. No. 27798/95, §65, *Benedik v. Slovenia*, App. No. 62357/14, §102). As the Court underlined in *S. and Marper*, "*[t]he protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention*" (App. Nos. 30562/04 and 30566/0 §103).

19. Further, the European Data Protection Supervisor (EDPS) has stated:

> [Social media monitoring] involves **uses of personal data that go against or beyond individuals' reasonable expectations**. Such uses often result in personal data being used beyond their initial purpose, their initial context and in ways the individual could not reasonably anticipate.[13] (emphasis added)

20. Finally, both European and non-European regulators had similar findings with respect to a case involving the use of social media surveillance by private entities. In January 2020, an investigation by the New York Times revealed that the U.S. based company Clearview AI was collecting "*images of people's faces from across the internet, such as employment sites, news sites, educational sites, and social networks including Facebook, YouTube, Twitter, Instagram*" in an effort to assist "*law enforcement match photos of unknown people to their online images*".[14] Subsequent reports by various media revealed that the company had entered into

[13] EDPS, Formal consultation on EASO's social media monitoring reports (case 2018-1083), p.3 https://edps.europa.eu/sites/edp/files/publication/19-11-12_reply_easo_ssm_final_reply_en.pdf.
[14] Kashmir Hill, The secretive company that might end privacy as we know it, The New York Times, 18 January 2020 https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

contracts with "*more than 2,400 police agencies*",[15] including Council of Europe member states' authorities.[16]

21. Following the serious fundamental rights' alarms raised by these revelations, a plethora of data protection regulators initiated investigations into the use of the technology by law enforcement and its compliance with data protection laws. In a letter to the European Parliament, the Chair of the European Data Protection Board (EDPB) highlighted that such forms of social media monitoring "*may undermine the right to respect for private life and the protection of personal data, but also other fundamental rights and freedoms*."[17] They may also "*affect individuals' reasonable expectation of anonymity in public spaces*."[18]

22. Most recently, the Swedish and the Canadian data protection regulators found that the Swedish Police had breached data protection laws when using Clearview AI to identify individuals,[19] and that the company's "*unlawful practices represented mass surveillance of Canadians*",[20] respectively. In rejecting any arguments around the inapplicability of data protection laws to personal data published by individuals online, the latter underlined that "*individuals who posted their images online, or whose images were posted by third party(ies),* ***had no reasonable expectations that Clearview would collect, use and disclose their images for identification purposes***"[21] (emphasis added).

23. Therefore, the Intervener submits that any processing operation performed by authorities upon individuals' personal data published on social media for purposes that go beyond what individuals might expect or foresee should be regarded as a serious interference with their right to respect for private life, particularly when such processing relates to personal data revealing political opinions. To hold otherwise would be to deny the necessary protection afforded by the Convention to individuals' private life in the digital environment, a field "*where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole*" (Klass v. Germany, App. No. 5029/71, §56).

Social media monitoring needs to be subject a foreseeable legal framework which contains a series of strict safeguards in accordance with Article 8§2 ECHR

The use of "overt" social media monitoring should be in accordance with the law

24. The Intervener argues that the use of "overt" social media surveillance by the EAU must be accessible and subject to strict safeguards to be considered "*in accordance with the law*" under Article 8§2. In *Malone v. The United Kingdom* (App. No. 8691/79, §70) the Court held that the provisions need to be laid down *"with reasonable precision in accessible legal rules that sufficiently indicated the scope and manner of exercise of the discretion conferred on the relevant authorities".* Further, in *Weber and Saravia v. Germany*, (App. No. 54934/00 §93), the Court stated that *"the domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures".*

[15] Elizabeth Lopatto, Clearview AI CEO says 'over 2400 police agencies are using its facial recognition software' The Verge, 26 August 2020 https://www.theverge.com/2020/8/26/21402978/clearview-ai-ceo-interview-2400-police-agencies-facial-recognition
[16] Caroline Haskins, Ryan Mac, Logan McDonald, Clearview AI wants to sell its facial recognition software to authoritarian regimes around the world, Buzzfeed News, 5 February 2020 https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22
[17] European Data Protection Board, EDPB response to MEPs Sophie in 't Veld et al., 10th June 2020 https://edpb.europa.eu/our-work-tools/our-documents/letters/edpb-response-meps-sophie-t-veld-moritz-korner-michal-simecka_en
[18] Ibid.
[19] European Data Protection Board, Swedish DPA: Police unlawfully used facial recognition app, 12 February 2021 https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_el
[20] Office of the Privacy Commissioner of Canada, Joint investigation of the Clearview AI, Inc, 2 February 2021 https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/
[21] Ibid.

25. We submit that "overt" social media monitoring does not comply with these principles because in the UK, it is only the "covert" social media surveillance that is subject to the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA requires that when public authorities, need to use covert techniques (such as covert social media intelligence) to obtain private information about someone, they do it in a way that is necessary, proportionate, and compatible with human rights. It also provides for the need to obtain judicial approval prior to using covert techniques and requires internal approval of a RIPA Authorising Officer as well as that of a magistrate.[22]

26. However, no equivalent legislation exists for the use of "overt" social media intelligence. This is very problematic, considering that our research on the use of social media intelligence by public authorities indicates that there is a confusion surrounding what amounts to "overt" and "covert" social media monitoring. Section 26(9)(a) RIPA provides that surveillance is covert if it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place. This could apply to any social media monitoring, since individuals are often unaware that they are being monitored.

27. Further, the Surveillance Commissioner's Guidance[23] defines overt social media monitoring as looking at "open source" data, being publicly available data and data where privacy settings are available but not applied. However, to be "overt" it must also involve only a 'one-off' look at the individual's social media. If this becomes "repeated viewing" (being repetitive examination of public posts as part of an investigation), even of so-called open-source sites, then this becomes "covert" social media monitoring.[24] It is "covert" monitoring that must be subject to assessment and may be classed as Directed Surveillance as defined by Regulation of Investigatory Powers Act 2000 (RIPA). When this form of surveillance is said to involve repeated viewing of an individual's social media then authorisation is required, and it is known as RIPA authorisation.[25]

28. Yet, there is a lack of consistency as to what constitutes repeat viewing. From the Freedom of Information responses we have received and the policies some local authorities have disclosed with these responses, it appears that if a local authority spent time looking at an individual's social media, kept that page open, took screenshots of the page and stored those, this may still be considered "overt" and does not require authorisation or result in any checks and balances.[26] We are concerned that some local authorities have stated that even spending over three weeks "googling" or otherwise monitoring a person's name on various dates during that time may not fall within the Regulation of Investigatory Powers Act.[27] Our research demonstrates that even the public authorities that are using social media monitoring are not clear when relevant conditions would apply. We therefore submit that the same guarantees that apply to covert surveillance should also apply to all social media monitoring.

The need for robust safeguards

29. PI is concerned that the safeguards designed specifically to govern the use of "overtly" collected intelligence are often lacking. Our research indicates that the large majority of public authorities who use overt social media monitoring appear to have no processes or procedures in place to audit this surveillance tactic, have no idea how often overt social media monitoring is being

[22] UK Home Office, Surveillance and counter-terrorism guidance, 26 March 2013 https://www.gov.uk/guidance/surveillance-and-counter-terrorism
[23] PI, Office of Surveillance Commissioners Guidance - Covert surveillance of Social Networking Sites (SNS), 24 May 2020 https://privacyinternational.org/long-read/3537/office-surveillance-commissioners-guidance-covert-surveillance-social-networking
[24] Ibid.
[25] UK Home Office, Surveillance and counter-terrorism guidance, 26 March 2013 https://www.gov.uk/guidance/surveillance-and-counter-terrorism
[26] PI, 'Is your Local Authority looking at your Facebook likes?' May 2020, p 9 https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020.pdf
[27] Ibid.

used nor are therefore able to assess whether it is being used in a way that is legitimate, necessary, proportionate and effective.[28] Further, there is no requirement to obtain prior authorisation when conducting "overt" social media monitoring by public authorities and law enforcement agencies, unlike for "covert" social media intelligence which is governed by the Regulation of Investigatory Powers Act 2000 (RIPA).[29] This has led to a situation where law enforcement officials (and intelligence agencies) may believe that everything that a given social networking website sets as publicly available is fair game for them to access, collect, and process with very limited regulation, oversight, or safeguards.[30]

30. PI's research also highlighted that the respect given to an individual's privacy in relation to what individuals' say and do online appears to be based on the arbitrary distinction of privacy settings. This distinction is promoted by the Home Office guidance[31] and by the Investigatory Powers Commissioner[32] whose annual reports document concerns related to public authorities use of social media monitoring.[33] This is troubling, considering the context where privacy settings constantly change and can apply differently to different content and situations, individuals may share without necessarily being aware who can access their information and how it is used.[34]

31. As underlined above, social media monitoring poses significant risks for individuals' fundamental rights. Regulators and UN bodies have highlighted the need for such conduct to adhere to strict safeguards. In its case-law, the Court has emphasised that the "*domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of*" the Convention (*S. and Marper*, App. Nos. 30562/04 and 30566/0 § 103). These safeguards need to govern all processing operations performed on personal data by public authorities, including their collection, retention or storage, analysis, dissemination or disclosure, or any other form of processing. As the Court highlighted in *Marper*:

> The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored. The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse. The above considerations are especially valid as regards the protection of special categories of more sensitive data… (§103)

32. If left unregulated, the routine collection and processing of publicly available information for intelligence gathering may lead to the kind of abuses we observe in other forms of covert surveillance or other police operations. The potential abuse could involve the systematic targeting of certain ethnic and religious groups by law enforcement agencies. It is impossible to guarantee that there is no racial or religious bias in online monitoring if there is no notice, transparency, supervision and oversight of the police social media intelligence activities.

---

[28] Ibid, p. 21
[29] Ibid, p 10
[30] Ibid, p 17
[31] PI, Home Office Covert Surveillance and Property Interference, August 2018, 24 May 2020 https://privacyinternational.org/long-read/3532/home-office-covert-surveillance-and-property-interference-august-2018
[32] Privacy International, History of the UK Regulators' concerns regarding Local Authority use of social media monitoring, 24 May 2020 https://privacyinternational.org/long-read/3531/history-uk-regulators-concerns-regarding-local-authority-use-social-media-monitoring
[33] UK Home Office, Surveillance and counter-terrorism guidance, 26 March 2013 https://www.gov.uk/guidance/surveillance-and-counter-terrorism
[34] PI, Is your Local Authority looking at your Facebook likes? May 2020, p. 7 https://privacyinternational.org/sites/default/files/2020-05/Is%20Your%20Local%20Authority%20Looking%20at%20your%20Facebook%20Likes_%20May2020.pdf

33. As public authorities and law enforcement agencies are often secretive about the use of social media monitoring and sources of information, it can be extremely difficult for individuals to challenge any allegations.[35] We therefore submit that the use of "overt" social media monitoring by government authorities should, at the very minimum, include transparency and accountability safeguards, including authorisation by an independent judicial authority, independent oversight and notification.

Any interference with the right to privacy should be subject to prior authorisation by an independent judicial authority

34. We submit that overt social media monitoring should be subject to prior independent authorisation, especially since social media monitoring can be as intrusive as other forms of surveillance. The need for a prior authorisation is also evident from our research, which demonstrated the confusion on behalf of Local Authorities as to when a requirement for authorisation in social media intelligence applies.[36] In *Zakharov*, this Court approved of authorisation by a non-judicial authority "provided that that authority is sufficiently independent from the executive." (*Zakharov v. Russia*, App. No. 47143/06 §258-260). The Court repeated the principles in *Szabó*:

> in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exceptions, warranting close scrutiny ... supervision by a politically responsible member of the executive, such as the Minister for Justice, does not provide the necessary guarantees (*Szabó and Vissy v. Hungary,* App. No. 37138/14 § 77-79).

35. It added that independent, "preferably judicial," review "reinforce[s] citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained" (*Szabó and Vissy v. Hungary,* App. No. 37138/14 § 77-79). At the moment, the relevant guidelines do not contain sufficient substantive and procedural safeguards governing the access and use of retained data obtained from social media intelligence. This requirement for independent authorisation has been further confirmed by international human rights bodies.[37]

36. We submit that a system of prior judicial authorisation would minimise unnecessary or disproportionate interferences with privacy. A limited post-authorisation oversight regime that only examines a restricted breadth of information is not sufficient. This is particularly the case when there is no complaint mechanism available to challenge such interferences.

Any interference with the right to privacy should be subject to independent and effective oversight

37. State surveillance of social media should be subject to independent, effective, adequately resourced and impartial domestic oversight mechanisms capable of ensuring transparency as appropriate, and accountability.[38] As the UN High Commissioner for Human Rights noted, effective oversight should ensure that:

> Oversight bodies should be independent of the authorities carrying out the surveillance and equipped with appropriate and adequate expertise, competencies and resources. Authorization and oversight should be institutionally separated. Independent oversight bodies should proactively investigate and monitor the activities of those who conduct surveillance and have access to the products of surveillance, and carry out periodic

[35] Ibid.
[36] See paras 25-28 above
[37] UN Human Rights Committee, Concluding observations on the fifth periodic report of Belarus, UN Doc. CCPR/C/BLR/CO/5, 22 November 2018; UN OHCHR, Report on the right to privacy in the digital age, UN Doc. A/HRC/39/29, 3 August 2018; CoE ComHR, "Memorandum on surveillance and oversight mechanisms in the UK", CommDH (2016)20, 17 May 2016, para. 28 (referring to the Venice Commission's Report on Democratic Oversight (2007)).
[38] Ibid. See also UN General Assembly, Resolution on the Right to Privacy in the Digital Age, UN Doc. A/RES/73/179, 17 December 2018.

> reviews of surveillance capabilities and technological developments. The agencies carrying out surveillance should be required to provide all the information necessary for effective oversight upon request and regularly report to the oversight bodies, and they should be required to keep records of all surveillance measures taken. Oversight processes must also be transparent and subject to appropriate public scrutiny and the decisions of the oversight bodies must be subject to appeal or independent review.[39]

38. We submit that effective oversight cannot be limited to an automatic and superficial review of the reported interferences, without the ability to review all available information and authority to issue binding decisions.

Subjects of secret surveillance should always be notified (even if *post facto*)

39. There is an increasing consensus that notification requirements are necessary to enable individuals who are subjected to secret surveillance measures to challenge unlawful surveillance decisions. This Court has consistently recognised the importance of notification as both an adequate safeguard against the abuse of surveillance powers under Article 8 and as part of the right to an effective remedy under Article 13 (*Szabó and Vissy v. Hungary,* App. No. 37138/14 §86, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, App. No. 62540/00 §91). In *Weber,* the Court noted that there is "in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively" (*Weber and Saravia v. Germany*, App. No. 54934/00 §135).

40. In its landmark judgement in *Schrems*, the CJEU added that:

> [a]ccording to settled case-law, the very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law. Thus, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him or her, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection.[40]

41. International human rights bodies and experts, including the UN High Commissioner for Human Rights, have repeatedly underlined the significance of notification to ensure effective remedy of violations of the right to privacy.[41] As to when, practicably, an individual should be notified, this Court has acknowledged that "*as soon as notification can be carried out without jeopardising the purpose of the restriction after the termination of the surveillance measure, information should, however, be provided to the persons concerned*" (*Weber and Saravia v. Germany*, App. No. 54934/00 §135).

42. In light of the above, we submit that it is key that this Court concludes that notification is a necessary safeguard in cases of "overt" social media monitoring. Considering that social media monitoring allows law enforcement to gather a large amount of personal data, including personal data deemed as sensitive (such as data revealing political or religious beliefs), and to profile individuals, the need for a notification regime is amplified. Whilst notification of surveillance is not an absolute right in the sense that it should operate without restrictions, any restriction on notification should be strictly limited, i.e. it should only be delayed where it would seriously jeopardize the purpose for which the surveillance is authorised, or where there is an imminent threat to human life. Any such delay in notification, moreover, must be judicially

---

[39] UN OHCHR, Report, note 22, para. 40. See also ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, App. No. 62540/00, Judgment (28 June 2007), para. 85

[40] CJEU, *Data Protection Commissioner v. Facebook Ireland and Schrems (Schrems II)*, Case C-311/18, Judgment, 16 July 2020, para.187, see also CJEU, Joined cases *Tele2 Sverige AB v Post-och telestyrelse*n and *Secretary of State for the Home Department v Tom Watson*, Cases Nos. C–203/15 and C–698/15, Judgment, 21 December 2016, para 121.

[41] The right to privacy in the digital age, UN Doc. A/HRC/27/37, 30 June 2014, para 47; Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/23/40, 17 April 2013, para. 82; Joint Declaration on Surveillance Programmes and Their Impact on Freedom of Expression, 21 June 2013, para. 5.

authorised and subject to continuing judicial oversight. The burden must be on the government to satisfy an independent and impartial tribunal that continued non-notification is both necessary for a legitimate aim and proportionate.

Data subject rights

43. We also submit that any social media monitoring needs to be subject to strict safeguards to ensure that data subjects can exercise their rights under the data protection legislation and Article 8 ECHR. The Court has repeatedly emphasised that the "exercise of the right under Article 8 to respect for one's private and family life must be practical and effective" (*Phinikaridou v. Cyprus*, App No 23890/02 §64). It has further reiterated that individuals who are the subject of personal files held by public authorities have a vital interest in being able to access the information held on them (*Haralambie v. Romania*, App No. 21737/03). We submit that in most cases of social media monitoring individuals will not be aware of any monitoring activities carried out by authorities. Therefore, it is of fundamental importance that those who have been subject to monitoring are able to verify the lawfulness of the processing of their personal data. Whilst this could be subject to some restrictions (such as in instances of ongoing investigations), any restrictions should be limited.

The standard of review to be applied by this Court

44. With regard to the margin of appreciation enjoyed by the respondent state, the Court has acknowledged that the former "*goes hand in hand with European supervision*" (*Peck* App. No. 44647/98, §77; *Funke v. France*, App. No. 10828/84, §55). Additionally, in cases where "*the right at stake is crucial to the individual's effective enjoyment of intimate or key rights*", then the margin will "*tend to be narrower*" (*Breyer*, App. No 50001/12 §80). The existing European consensus (see Convention 108+ §6 and GDPR §4 above) on the need for strict conditions applying to the processing of personal data, especially sensitive data such as those revealing political opinions, and the severity of the interference caused by social media monitoring with individuals' right to respect for private life, call for this Court "*to exercise **careful scrutiny***" (emphasis added) of the impugned measure that concerns the processing of personal data "*by the authorities without the consent of the person concerned*" (*S. and Marper*, App. Nos. 30562/04 and 30566/0 §104).

Conclusion

45. As demonstrated above, social media monitoring constitutes a serious interference with individuals' privacy rights, as well as modern democracies. PI therefore submits that the monitoring of social media accounts by authorities constitutes a serious interference with Article 8§1 of the Convention, and that its use must be subject to robust safeguards.

5 March 2021

On behalf of the Interveners

Dr Ksenia Bakina and Ioannis Kouvakas
Legal Officers
Privacy International (PI)
London EC1M 5UY