The State of Surveillance – An Overall Account of Surveillance?

Felix Bieker(✉)

Unabhängiges Landeszentrum für Datenschutz (ULD, Office of the Data Protection Commissioner) Schleswig-Holstein, Kiel, Germany
fbieker@datenschutzzentrum.de

Abstract. The article argues that the extent of surveillance has reached a critical level for democratic societies. However, the jurisprudence of the ECtHR, ECJ and German constitutional court, which never question the extent of surveillance on the structural level, rather aims to legitimize even the most far-reaching measures and thus does not offer effective ex post protection. The introduction of legislative ex ante mechanisms also does not promise to counter the current issues surrounding surveillance measures. Instead, such a mechanism could further legitimize surveillance. The article concludes that while tools to assess the level of surveillance could be helpful when they depart from the premise that the extent of surveillance must be reduced, civil society is best suited to operate and advance these tools in the general discourse.

Keywords: Surveillance · Privacy · Data protection · Data retention · ECtHR · ECJ · Bundesverfassungsgericht · Big brother watch · Digital Rights Ireland · Surveillance calculus · Überwachungs-Gesamtrechnung

1 Introduction

As technology advances and is capable of processing ever more data, it brings new possibilities of surveillance. Whether it is location tracking via Wifi and Bluetooth or automated face or voice recognition, the new data produced by these technologies allow for further intrusions. And from this new data springs a "need" to process those data [1]. This "need" has meanwhile led to a steady stream of surveillance measures, which observers argue has already led to a surveillance society [2, 3].

This is exemplified by the myriad of new surveillance technologies introduced by various legislators: From the bulk retention of air passenger data [4], to DNA phenotyping [5], a technology falsely touted as "genetic composite sketch", the use of facial

I would like to thank all participants of the 2021 IFIP Summer School, who provided input at this tutorial. This work is funded by the German Ministry of Education and Research within the project "Privacy, Democracy and Self-Determination in the Age of Artifical Intelligence and Globalisation" (PRIDS), https://forum-privatheit.de.

Published by Springer Nature Switzerland AG 2022
M. Friedewald et al. (Eds.): Privacy and Identity 2021, IFIP AICT 644, pp. 47–53, 2022.
https://doi.org/10.1007/978-3-030-99100-5_5

recognition software [6] or the expanded monitoring of recipients of social welfare benefits [7], all of which often lead to the discrimination of already marginalized groups (generally cf. [8]).

All of these and the many other, already existing surveillance instruments impact the lives of large portions of the population. And they can create a feeling as well as a reality of being constantly monitored (also cf. [9]). In sum these surveillance pressures can have adverse effects on individuals as well as a democratic society as a whole [10].

Yet, these effects are only reluctantly being considered in the legal debate, where the focus, as is the nature of Western judiciary proceedings, lies on an individual complaint about a specific measure considered to violate specific rights. In the following, I will briefly introduce the relevant rights concerning data processing on the European and German national level and consider the jurisprudence of the European Court of Human Rights (ECtHR), the European Court of Justice (ECJ) and the German constitutional court (2). I will then consider whether and how an overall account of surveillance should and could be attained (3) and conclude with an outlook (4) for a way towards rescinding surveillance measures.

2 Rights, Courts and Surveillance

In Europe, there are several layers of rights protections, which aim, inter alia, to protect individuals from the State. On the regional level, there is the ECHR [11], which contains the right to privacy, while on the EU level, the Charter of Fundamental Rights (CFR) [12] additionally contains a right to data protection (in depth, cf. [10]). Both of these rights are concerned when personal data are processed and have been invoked against surveillance measures. On the national level, in Germany, there are especially the rights to informational self-determination as well as to the integrity and confidentiality of IT systems provided by the Basic Law [13], which also protect individuals from data processing and, inter alia, against surveillance measures.

These rights are enforced via judicial proceedings. However, courts will usually consider a specific measure and examine whether it violates any of the invoked rights. The courts will generally not move (much) beyond the scope of the claims and merely assess the case at hand, without considering the wider legal and societal implications of surveillance. Nevertheless, there have been judgments that (seem to) have referred to a broader scope of assessment.

In the recent ECtHR's Grand Chamber judgment in the case of Big Brother Watch [14], it appeared, prima facie, that the court had broadened its approach. It held that the UK's bulk data retention regime amounted to a fundamental rights violation. In its analysis, the ECtHR made reference to a 'global assessment' of the measure in question. Yet, when applying this standard, it found that there were several criteria, which, when they were all fulfilled, would provide sufficient safeguards to legitimize even one of the most far-reaching data retention schemes [14, paras. 360 et seqq.]. In that regard, the global assessment does the opposite of what it could be understood to mean: rather than consider the overall impact of surveillance or at least the wider implications of a surveillance measure, the Court effectively lowered the standard of protection [15] awarded by an earlier judgment by the chamber in the same case [16].

At the EU level, the ECJ, has repeatedly engaged with mass-surveillance instruments [17–20] and by now developed a steady jurisprudence on the requirements, which it finds to legitimize such measures (cf. most recently [21–23]). It has lately begun to acknowledge some of the risks of discrimination entailed in automated surveillance systems, especially those employing machine learning technology [19 para. 141; 21 paras. 180–182], which members of the affected marginalized groups have long pointed out [24–26]. However, the court has considered the wider effects of surveillance only fleetingly. In its seminal judgment on the data retention directive, *Digital Rights Ireland and Seitlinger*, the ECJ stated that such a mass retention was likely to create a feeling of constant surveillance [15, para. 37]. The Court has since reiterated this finding in subsequent judgments and found that certain measures would lead to 'virtually total' surveillance [20, paras. 71–72; 19, paras. 183–187]. However, the ECJ has only considered these effects with regard to the weight of an interference and, in all of these cases, found that the interferences with the right to privacy and the right to data protection were particularly serious. It has not taken the further implications of surveillance creating effects on democratic societies into consideration.

The passages from the ECJ judgments echo the case law of the German constitutional court: in a 2010 judgment concerning the German bulk data retention rules [27], the court found that the State could not completely register the populace's exercise of their constitutional freedoms. This argument was based on the court's most widely received ruling on data protection, the census judgment of 1983. There it had stated that it would not be in accordance with fundamental rights and the legal order, if modern information technology rendered the individual a mere object of automated processing [28]. It argued that individuals who are unsure whether their conduct is constantly monitored and permanently recorded, used or transferred to third parties, will try not to raise suspicion through deviant behaviour.

In its 2010 judgment, the court ruled that in the future, the legislator had to exercise greater restraint with regard to surveillance measures [27]. The State could not retain any data useful for law enforcement purposes. Rather, in a democracy under the rule of law, the retention of such data had to be an exception.

With this ruling, it may seem that the constitutional court reigned in the "needs" of surveillance. However, in the case of the bulk data retention at hand, it found the measure to still just be permissible with certain adjustments. The court only hinted that even further reaching surveillance could be struck down in an *orbiter dictum*, i.e. a non-operative part of the judgment, which has no direct legal effects. Consequently, the rules stayed in force until the ECJ found them incompatible with EU fundamental rights [17]. Furthermore, even though this issue has been raised by applicants in recent proceedings [29], the court has not engaged with its own arguments.

3 An Overall Account of Surveillance?

Nevertheless, the arguments of the constitutional court and the ECJ could be further pursued in order to broaden the scope of review for surveillance measures. There has long been a debate about the effects on and amount of surveillance in Western societies at least since these programmes were extended considerably in the wake of 9/11

[9, 30]. However, it has taken considerable time before these discussions reached the legal discourse.

In the German academic debate, the arguments of the constitutional court were used to argue that there was a limit of State surveillance which must not be exceeded, but which apparently had not yet been reached. With this so-called surveillance calculus (Überwachungs-Gesamtrechnung) [31], the court had stipulated a requirement of the legislator to maintain an overview of all State surveillance measures in effect and the gravity of the interferences entailed by these measures. Once a certain, but undefined, threshold was reached, the legislator would have to exchange one surveillance measure for another, rather than introducing additional ones.

However, such a compilation, in practice, encounters issues on several levels: On the micro level it is unclear, how the different surveillance measures of the various legislators on the EU, national and local level can be counted and, especially, weighed. Furthermore, it is unclear how the legislator would have to act, once the threshold was reached [32]. Would the oldest surveillance measure have to be repealed or would the latest never take effect?

Another difficult question is the qualification of interferences with rights. The gravity of an interference and whether it is justified is the result of a deliberative process, so different results may be reached via different argumentative avenues. Such results do not easily lend themselves to being quantified. Rather, it must be borne in mind that pseudo-mathematical calculations may seem to deliver objective results, but only serve to obscure the weighing that led to the result.

More importantly, on the macro level, such a calculus poses the question of the effects of such an evaluation by the legislator. After all, the legislator has demonstrated a great willingness to continually pass new legislation to introduce surveillance measures. If they are now asked to provide an evaluation of the existing surveillance regime, they might be tempted not to assess this question with the required rigor.

If the legislator, after carrying out such an in-depth assessment, concluded that the threshold of harmful surveillance has not been reached, such a calculus would ultimately serve to legitimize the present surveillance apparatus rather than challenge it. If the aggregate weight of all measures is to be examined, then a benchmark for an acceptable level of surveillance has to be defined in advance. Yet, it is doubtful that, if a benchmark were set at this point, the legislator itself or a court would find that the current level of surveillance is already unacceptable, as under the jurisprudence of the German constitutional court this would mean that the status quo is not in accordance with democratic principles [33].

An alternative approach to the surveillance calculus might be found in existing legislation: In Article 35(10) GDPR the legislator introduced the legislative data protection impact assessment (DPIA). With this instrument the legislator, as part of the general impact assessment of a new provision, can already perform a generalized DPIA. Under such a legislative DPIA the envisaged legislative measure would have to be vetted for adverse impacts on the rights of individuals. However, as any legal provision on a measure that still has to be realized in practice, it would only analyse the rules on an abstract level and would have to be accompanied by a specific DPIA once the rules have been

implemented [34]. The scope of this assessment could include the effects of currently existing surveillance measures and how the proposed measure would impact on these.

However, the legislative DPIA, just as any instrument that obliges the legislator to consider whether a surveillance measure is justifiable, encounters the same issues with regard to the legitimization effect, described above. In deciding to introduce a new surveillance measure, the legislator has mostly already deemed that such a measure is indeed necessary to combat a perceived threat. This may indeed be the biggest obstacle to any ex ante control instrument.

According to the separation of power that is a facet of the rule of law, it is the responsibility of the administration to implement the measure in a way that complies to fundamental rights. Where this is not the case, individuals can challenge measures before the courts. Yet, from the case law of the German constitutional court, the ECJ and the ECtHR, it does not appear that the ex post control offered by the judiciary effectively limits the amount of surveillance on a structural level. Rather they inadvertently serve to further legitimize far-reaching surveillance measures. In that regard, the courts' jurisprudence could also be characterized as going two steps forward and one step back, as they will strike down particularly far-reaching provisions of surveillance measures, but not actually question the measures themselves. This could also be observed with the judgments on data retention, where all of the courts only prescribed several safeguards, but did not question the massive data collection itself.

4 Outlook: A Way Forward

With regard to the problematic legitimizing effect of legislative ex ante and judicial ex post control of mass surveillance, there may be other, more effective means of surveying surveillance for different actors. Certainly, an overview of the current state of surveillance can have a sobering effect for the public [35], who may not be aware of the extent of existing legal bases for such measures.

Perhaps such activities are better performed by independent advocacy groups and activists, rather than lawyers and courts. At a time, when the extent of surveillance is so expansive that, outside the constitutional law discourse, other disciplines argue that we have already been living in surveillance societies for a considerable time, we must seek these other avenues as more effective routes to organize against surveillance.

However, the lessons learnt from the legal discourse can be employed to develop tools that civil society can use in order to implement a useable way to monitor surveillance measures. In order to avoid the legitimizing effect, any such examination should be carried out independently from public bodies and start from the premise that the level of surveillance is already critical. The focus should be on rescinding surveillance measures rather than expanding them. Such a tool should further ensure that the deliberative nature of such an examination is not be expressed in pseudo-mathematical formulas. Rather, it should rely on providing an easily workable metric that allows for comprehensible illustration and comparison on a scale containing three or four tiers. Such a tool could provide an additional basis for discussions, organizing and protest in order to counter the effects of surveillance on our societies.

References

1. Rule, J.B.: "Needs" for surveillance and the movement to protect privacy. In: Ball, K., Haggerty, K.D., Lyon, D. (eds.) Routledge Handbook of Surveillance Studies, pp. 64–71. Routledge, London/New York (2014)
2. Lyon, D.: Surveillance society. In: Monitoring Everyday Life. Open University Press, Buckingham/Philadelphia (2001)
3. Zuboff, S.: Big other: surveillance capitalism and the prospects of an information civilization. J. Inf. Technol. **30**, 75–89 (2015). https://doi.org/10.1057/jit.2015.5
4. Orrù, E.: The European PNR framework and the changing landscape of EU-security. VerfBlog 21 December 2021. https://verfassungsblog.de/os3-pnr/
5. Bartram, I., Plümecke, T., Zur Nieden, A.: Extended DNA analyses: surveillance technology at the intersection of racism and sexism. Internet Policy Rev. **10**(4) (2021). https://doi.org/10.14763/2021.4.1603
6. Buolamwini, J., Gebru, T.: Gender shades: intersectional accuracy disparities in commercial gender classification. In: Proceedings of Machine Learning Research, vol. 81, pp. 1–15 (2018). http://proceedings.mlr.press/v81/buolamwini18a.html
7. Carter, L.: Prescripted living: gender stereotypes and data-based surveillance in the UK welfare state. Internet Policy Rev. **10**(4) (2021). https://doi.org/10.14763/2021.4.1593
8. Theilen, J.T., Baur, A., Bieker, F., Ammicht Quinn, R., Hansen, M., González Fuster, G.: Feminist data protection: an introduction. Internet Policy Rev. **10**(4) (2021). https://doi.org/10.14763/2021.4.1609
9. Fox Cahn, A., Enzer, E.: A hollow promise: 20 years of constitutional erosion in the name of counter-terrorism. VerfBlog 13 December 2021. https://verfassungsblog.de/os3-hollow-promise/
10. Bieker, F.: The Right to Data Protection – Individual and Structural Dimensions of Data Protection in EU Law. T.M.C. Asser Press/Springer, The Hague (2022)
11. Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No. 005, 4 November 1950. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=005
12. Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012P%2FTXT
13. Grundgesetz für die Bundesrepublik Deutschland, BGBl III, 100-01. https://www.gesetze-im-internet.de/gg/BJNR000010949.html
14. ECtHR [GC]. Judgment of 25 May 2021, Big Brother Watch and Others v. the United Kingdom, App. nos. 58170/13, 62322/14 and 24960/15. ECLI:CE:ECHR:2021:0525JUD005817013. https://hudoc.echr.coe.int/eng?i=001-210077
15. Milanovic, M.: The grand normalization of mass surveillance: ECtHR grand chamber judgments in big brother watch and centrum för rättvisa. EJIL:Talk! 26 May 2021. https://www.ejiltalk.org/the-grand-normalization-of-mass-surveillance-ecthr-grand-chamber-judgments-in-big-brother-watch-and-centrum-for-rattvisa/
16. ECtHR. Judgment of 13 September 2018, Big Brother Watch and Others v. the United Kingdom, App. nos. 58170/13, 62322/14 and 24960/15. ECLI:CE:ECHR:2018:0913JUD005817013. https://hudoc.echr.coe.int/eng?i=001-186048
17. ECJ. Judgment of 8 April 2014, Case C-293/12 Digital Rights Ireland and Seitlinger and others. ECLI:EU:C:2014:238. https://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=5249759

18. ECJ. Judgment of 6 October 2015, Case C-362/14 Maximillian Schrems v Data Protection Commissioner. ECLI:EU:C:2015:650. https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6146191
19. ECJ. Opinion of 26 July 2017 Avis 1/15. ECLI:EU:C:2017:592. https://curia.europa.eu/juris/document/document.jsf?text=&docid=194498&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6146191
20. ECJ. Judgment of 21 December 2016, Joined Cases C-203/15 and C-698/15 Tele2 Sverige. ECLI:EU:C:2016:970. https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6146191
21. ECJ. Judgment of 6 October 2020, Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net. ECLI:EU:C:2020:791. https://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6146191
22. ECJ. Judgment of 6 October 2020, Case C-623/17, Privacy International. ECLI:EU:C:2020:790. https://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6146191
23. ECJ. Judgment of 2 March 2021, Case C-746/18, Prokuratuur. ECLI:EU:C:2021:152. https://curia.europa.eu/juris/document/document.jsf?text=&docid=238381&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6146191
24. Browne, S.: Dark Matters: On the Surveillance of Blackness. Duke University Press, Durham (2015). https://doi.org/10.1215/9780822375302
25. Kalluri, P.: Don't ask if artificial intelligence is good or fair, ask how it shifts power. Nature **583**, 169 (2020). https://doi.org/10.1038/d41586-020-02003-2
26. Costanza-Chock, S., Philip, N., Ahearn, C.: Design justice, A.I., and escape from the matrix of domination. J. Design Sci. (2018). https://doi.org/10.21428/96c8d426
27. Bundesverfassungsgericht. Judgment of 2 March 2010, BVerfGE 125, 260 – Vorratsdatenspeicherung. https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2010/03/rs20100302_1bvr025608.html
28. Bundesverfassungsgericht. Judgment of 15 December 1983, BVerfGE 65, 1 (43) – Volkszählung. https://openjur.de/u/268440.html
29. Bundesverfassungsgericht. Decision of 20 December 2018, - 2 BvR 2377/16 -. http://www.bverfg.de/e/rk20181220_2bvr237716.html
30. Naarttijärvi, M.: The 'Ketchup Effect': The development of public Surveillance in Sweden following 9/11. VerfBlog 15 December 2021. https://verfassungsblog.de/os3-ketchup-effect/
31. Roßnagel, A.: Die "Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 1238 (2010)
32. Hornung, G., Schnabel, C.: Verfassungsrechtlich nicht schlechthin verboten – Das Urteil des Bundesverfassungsgerichts in Sachen Vorratsdatenspeicherung, Deutsche Verwaltungsblätter, pp. 820–833 (2010)
33. Bieker, F., Bremert, B.: Rote Linien im Sand, bei Sturm: Die Überwachungs-Gesamtrechnung. FifF-Kommunikation (4), 34 (2019). https://www.fiff.de/publikationen/fiff-kommunikation/fk-jhrg-2019/fk-2019-4/fk-4-19-p34.pdf
34. Bieker, F., Bremert, B., Hagendorff, T.: Die Überwachungs-Gesamtrechnung, oder. Es kann nicht sein, was nicht sein darf. In: Roßnagel et al. (eds) Die Fortentwicklung des Datenschutzes, vol. 139, Springer, Wiesbaden (2018)
35. Adensamer, A.: Aspekte einer Überwachungs-Gesamtrechnung, FifF-Kommunikation (4), 34 (2019). https://www.fiff.de/publikationen/fiff-kommunikation/fk-jhrg-2019/fk-2019-4/fk-4-19-p25.pdf