2019

Overview of European State-Sanctioned Mass Surveillance Law

Michael Fiedorowicz

Michael Fiedorowicz
University of Chicago Law School
International Immersion Program 2019

Overview of European State-Sanctioned Mass Surveillance Law

Introduction

Privacy rights have come to the fore of European law with the passing of the General Data Protection Regulation ('GDPR').[1] While the GDPR is largely meant to address the protection of individuals' data in a business context, it is also applicable to actions taken by Member State governments; however, Article 23(1) creates a derogation from the regulation's requirements for legislation aimed at ensuring national and public security. [2] This paper provides an overview of the case law from the primary European Union ('EU') courts, the European Court of Justice ('CJEU') and the European Court of Human Rights ('ECHR'), and considers data protection rights in the context of surveillance programs aimed at crime prevention and national security. Given that the issues which may arise are likely to be similar, this overview is meant to shed light on how the courts might address the Article 23 derogation were it to arise in future cases.

The two courts have handled cases relatively similarly, and often refer to one another's case law; in doing so, they have discussed overlapping requirements for surveillance programs such as strict necessity for purposes of the relevant security interest, verifiable individualized suspicion relating to the surveillance target, and prior surveillance authorization by an independent entity. However, slight discrepancies have begun to emerge, and with the 2018 *Case*

[1] See for example: Dillet, Roman, "French data protection watchdog fines Google $57 million under the GDPR," TechChruch, 2019, https://techcrunch.com/2019/01/21/french-data-protection-watchdog-fines-google-57-million-under-the-gdpr/

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88, art. 23 [hereinafter, General Data Protection Regulation], https://gdpr-info.eu/

of Big Brother Watch and Others v. United Kingdom, it appears that the ECHR may be accepting something more like a standard wherein the court considers generally whether it is satisfied that the surveillance program contains sufficient safeguards to protect against arbitrariness and abuse. This paper also considers possible reasons for why the two courts might treat this issue differently, such as the nature of the respective underlying rights-providing documents they interpret, the Charter of Fundamental Rights of the European Union ('Charter') and the European Convention on Human Rights ('Convention'). Finally, the paper ends by analyzing implications that can be drawn for the future and ongoing cases.

GDPR Article 23(1)

Article 23(1) of the GDPR outlines conditions in which it would be permissible for a Member State to pass domestic legislation that restricts the scope of GDPR rights protections. Specifically, the derogation is operative if the legislation "is a necessary and proportionate measure in a democratic society to safeguard: (a) national security; (b) defence; (c) public security."[3]

To explore how European courts might deal with any litigation arising on the basis of this derogation, it is helpful to look to existing law dealing with mass state surveillance programs in privacy rights cases. The relevant case law deals with similar terminology and subject matter as is provided in Article 23(1), and may be particularly illustrative given the growth of mass surveillance programs run by Western European governments for security and crime-prevention purposes.[4] To be clear, it does not seem Article 23 will be applied to existing mass surveillance programs themselves insofar as Article 2(2) implies the GDPR is inoperative to instances of data

[3] Ibid
[4] Lubin, Asaf, "A New Era of Mass Surveillance is Emerging Across Europe," *Just Security*, Jan. 9, 2017, https://www.justsecurity.org/36098/era-mass-surveillance-emerging-europe/

processing relating to State-sponsored defense and security measures.[5] Indeed, the ECHR determined that the GDPR did not apply, on the basis of the Article 2(2) security exception, in the *Case of Centrum For Rattvisa v. Sweden*.[6] Under this view, Article 23(1) may be strictly viewed as applying to *legislation*.

Regardless of any ambiguity with respect to the GDPR's applicability to domestic national security laws, understanding how the courts engage with the relevant terms and issues could provide clues with respect to any sort of litigation that might arise in relation to Article 23(1). Thus, the following provides a consideration of the evolving body of case law in the CJEU and the ECHR wherein the courts work to determine the contours of the privacy rights found in Articles 7 and 8 of the Charter[7] and Article 8 of the Convention,[8] respectively. Given that the CJEU has jurisdiction to interpret European Union law, it has the final say on GDPR matters. But, as the text of the GDPR indicates, any restrictions in the rights that it outlines ought be consistent with the Convention, which is interpreted by the ECHR.[9] Furthermore, there is significant dialogue between the courts on relevant issues in their opinions; thus, exploring this interaction will be informative.

European Court of Justice Case Law

Digital Rights Ireland – April 2014

[5] General Data Protection Regulation, art. 2(2)
[6] *Case of Centrum For Rattvisa v. Sweden*, no. 35252/08, European Court of Human Rights, 19 June 2018, sec. 81, http://hudoc.echr.coe.int/eng?i=001-183863
[7] Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, p. 391–407, art. 7 [hereinafter Charter of Rights].
[8] European Convention on Human Rights, European Court of Human Rights, Council of Europe, art. 8, https://www.echr.coe.int/Documents/Convention_ENG.pdf
[9] General Data Protection Regulation, recital 73

The CJEU has been generally reluctant to give Member States free reign in the name of national security or other crime-prevention measures.[10] Relevant here is the court's ruling in *Digital Rights Ireland and Others* in which a watchdog organization challenged Ireland's legislatively-mandated data retention program. Recognizing the data privacy rights found in Articles 7 and 8 of the Charter, the court held that the Irish data retention program as well as an EU-wide data retention program (Directive 2006/24) were invalid. While Article 52(1) of the Charter provides an exception to the protection of rights enshrined by the document where such an exception is necessary and genuinely meets an objective of general interest, the court found that those conditions were unmet.[11] Although, the case left unclear whether then-current Member State data retention programs were generally legal, leaving some lack of clarity.[12]

The decision established groundwork that reveals what factors can be relevant in such cases, including legislative clarity of circumstances in which the program applies, strict necessity in relation to the pursued interest, and procedural safeguards. The court made clear that in context of what constitutes a proper general interest, crime and terror prevention are encompassed in this category and are viably advanced through the use of data retention.[13] It further concluded that the EU legislature, when establishing such security measures, must make clear the rules "governing the scope and application of the measure."[14] In other words, the legislation that establishes the program must be such that the operations of the program are

---

[10] "The EU General Data Protection Regulation," *Human Rights Watch*, June 6, 2018, https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation
[11] Charter of Rights, art. 52(1)
[12] Bradley-Schmieg, Phil and Jones, Joseph, "CJEU Confirms that National Data-Retention Law May Only Be Adopted Where 'Strictly Necessary,'" *Inside Privacy*, Covington & Burling, January 6, 2017, https://www.insideprivacy.com/international/european-union/cjeu-confirms-that-national-data-retention-laws-may-only-be-adopted-where-strictly-necessary/
[13] *Digital Rights Ireland and Others*, cases C-293/12 and C-594/12, Court of Justice of the European Union, 8 April 2014, sec. 51, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0293&from=en
[14] Ibid, sec. 54

generally foreseeable. When such programs are implemented and derogations from the Charter's privacy rights constraints are sought, these derogations "must apply only in so far as is strictly necessary."[15] The court found that strict necessity was not met because the EU program was functionally indiscriminate in whose data was retained.[16] Furthermore, there were no objective limits outlining when national authorities could access the data.[17]

Schrems – October 2015

The October 2015 decision in *Schrems v. Data Protection Commissioner* is important to note as a particularly bold move by the court. It determined that the United States' protections for personal data were inadequate under Charter requirements.[18] Specifically, it looked at a certain data transfer scheme and determined that as data of EU citizens reached the US, the US could "process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security."[19] The court thus demanded that the data transfer in this case be halted and transferring EU citizen data across the Atlantic to the U.S. was found to be inconsistent with EU law. There are two factors that make this important. First, it struck down a Decision by the European Commission called Safe Harbour which had initially determined that US safeguards were sufficient under EU standards.[20] Furthermore, it was a ruling which implicated US and EU

---

[15] Ibid, sec. 52
[16] Ibid, sec. 58
[17] Ibid, sec. 60
[18] *Schrems v. Data Protection Commissioner*, case C-362/14, Court of Justice in the European Union, 6 October 2015, sec. 24-26, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62014CJ0362&from=EN
[19] "The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid," Press Release No 117/5, Court of Justice of the European Union, 6 October, 2015, https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf
[20] "Max Schrems v. Data Protection Commissioner (CJEU - "Safe Harbor")," Electronic Privacy Information Center, https://epic.org/privacy/intl/schrems/

commercial and political interests. The point here is that the CJEU has been doing more than paying lip service to digital privacy rights and is willing to take on serious cases.

Tele2 and Others - December 2016

The ambiguities left by *Digital Rights Ireland* were in part resolved by the combined cases of *Tele2 and Others*. The decision clarified that Member State data retention and surveillance programs could be valid but refined the necessary conditions. Reaffirming *Digital Rights Ireland*, the court ruled that data retention programs are valid only if "strictly necessary" for accomplishing the relevant security interests.[21] It further confirmed that only "serious crime" could possibly justify such programs.[22] The implication of these two requirements, beyond prohibiting generalized, indiscriminate data retention, is that there must be some identifiable connection between the individual whose data is retained and the prevention of serious crime.[23] In order to ensure that these conditions are satisfied when national law enforcement authorities seek retained data, the court demands "that access of the competent national authorities to retained data should, as a general rule, except in cases of validly established urgency, be subject to a prior review carried out either by a court or by an independent administrative body."[24] The court also established the requirement that the individual whose data is utilized be notified "under the applicable national procedures, as soon as that notification is no longer liable to jeopardise the investigations being undertaken by those authorities."[25]

European Court of Human Rights

Zakharov – December 2015

---

[21] *Tele2 and Others*, cases C-203/15 and C-698/15, Court of Justice in the European Union, 21 December, 2016, sec. 96, http://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&doclang=en
[22] Ibid, sec. 102
[23] Ibid, sec. 106-111
[24] Ibid, sec. 120
[25] *Case of Roman Zakharov v. Russia*, no. 47143/06, European Court of Human Rights, 4 December 2015, sec. 121, http://hudoc.echr.coe.int/eng?i=001-159324

Similar cases have come up in the ECHR, with the 2015 *Case of Roman Zakharov v. Russia* decision serving as the leading Grand Chamber opinion. Critically, the court established a requirement similar to that of the *Tele2*: that verifiable, individualized reasonable suspicion is required in instances of surveillance.[26] This was an important development following decisions in *Weber and Savaria v. Germany*, where the Third Section viewed the transfer of data to law enforcement agencies absent suspicion as problematic, and *Liberty and Ors v. United Kingdom* where the Fourth Section did not address the issue.[27]

Specifically, the court outlines that a surveillance-authorizing actor "must be capable of verifying the existence of a reasonable suspicion against the person concerned."[28] Throughout the opinion, the court is fundamentally concerned with blocking surveillance mechanisms which are amenable to potentially arbitrary and abusive use.[29] Indeed, the authorizing agencies "must also ascertain whether the requested interception meets the requirement of 'necessity in a democratic society', as provided by Article 8 § 2 of the Convention, including whether it is proportionate to the legitimate aims pursued, by verifying, for example whether it is possible to achieve the aims by less restrictive means." This language is similar to that which is used by the CJEU.

In another move that resembles the CJEU's case law, the *Zakharov* court notes that one way to limit the concerns about arbitrariness is through judicial authorization of interception beforehand, the requirement of ex-post notice, and that the implementation of the surveillance program be foreseeable.[30] In *Zakharov*, though there was judicial authorization, the court was not

[26] Ibid, sec. 260
[27] Nyst, Carly, "European Human Rights Court Deals a Heavy Blow to the Lawfulness of Bulk Surveillance," *Just Security*, December 9, 2015, https://www.justsecurity.org/28216/echr-deals-heavy-blow-lawfulness-bulk-surveillance/
[28] *Case of Roman Zakharov*, sec. 260
[29] Ibid, sec. 302
[30] Ibid, sec. 228, 234, 267

satisfied with its capacity to confirm reasonable suspicion due to other procedural irregularities.[31] The court also notes that "the national law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures."[32] This court also determined, as the *Tele2* court did, that in order for the surveillance program to operate in a way that respects rule of law principles, notifying the citizen being surveilled at a reasonable point is critical as it provides an opportunity to seek legal remedy.[33] Furthermore, the court also established that the law permitting surveillance must "be foreseeable as to its effects" thus implicating the clarity with which the law's details must be made public.[34]

***Szabo* – January 2016**

The Fourth Section court reiterated these expectations in the *Case of Szabo and Vissy v. Hungary*, where it also shed more light on what "necessary" and "proportionate" mean. [35] There the court held that a Hungarian anti-terror law did not abide by the Convention's Article 8 privacy protections. The opinion explains that, in secret surveillance cases, not only must the given legislative mechanism be "necessary in a democratic society,"[36] but, referencing *Digital Rights Ireland*, that it also pass the "strict necessity" test.[37] The court develops here a two-prong test: the surveillance must be "strictly necessary" for the "general consideration" of "safeguarding the democratic institutions" and "as a particular consideration, for the obtaining of vital intelligence in an individual operation."[38] So the court in this case reaffirms the *Zakharov*

[31] Ibid, sec. 260-267
[32] Ibid, sec. 243
[33] Ibid, sec. 234
[34] Ibid, sec. 228
[35] *Case of Szabo and Vissy v. Hungary*, no. 37138/14, European Court of Human Rights, 12 January 2016, http://hudoc.echr.coe.int/eng-press?i=001-160020
[36] Ibid, sec. 59
[37] Ibid, sec. 72-73
[38] Ibid, sec. 73

requirement of individualized, reasonable suspicion. Given that the Hungarian law did not require the national agency, "to produce supportive materials, or, in particular, a sufficient factual basis" then there is no way it could have been able to assess the "necessity of the proposed measure."[39] Indeed, "[f]or the Court, only such information would allow the authorizing authority to perform an appropriate proportionality test."[40]

The *Szabo* court also affirmed that judicial authorization based on sufficient facts is probably the clearest way to ensure compliance with the requirements outlined above.[41] Referencing the *Zakharov* decision, the court noted the lack of judicial authorization in the Hungarian muss surveillance system and determined that such oversight "would serve to limit the law enforcement authorities' discretion."[42] Nonetheless, though it recognized that in some instances sufficiently-independent non-judicial bodies may be capable of lawful authorizations, the court indicated a clear preference for judicial authorization: "judicial control offering the best guarantees of independence, impartiality and a proper procedure…Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny."[43] Thus, either judicial authorization or an authorizing body independent of the executive appeared essential to the court.

***Centrum for Rattvisa* – June 2018**

In *Centrum for Rattvisa*, the court largely applied the approaches developed in *Zakharov* in finding a Swedish surveillance system to be adequate. However, the case is notable in that the court gave particular attention to the broad discretion provided to states in fighting terrorism and

---

[39] Ibid, sec. 71
[40] Ibid
[41] Nyst, Carly, "The European Court of Human Rights Constrains Mass Surveillance (Again), *Just Security*, January 22, 2016, https://www.justsecurity.org/28939/ecthr-constrains-mass-surveillance/
[42] *Case of Szabo and Vissy v. Hungary* , sec. 73
[43] Ibid, sec. 77

cross-border crime.[44] Recognizing "present-day threats…as well as the increased sophistication of communications technology," the court explained that states have wide discretion in determining what sort of security regimes they wish to implement.[45] Although, of course, the operation of such regimes is limited by the above reasoning to that which is "necessary in a democratic society."[46] This decision is important to note as an indication of the general deference the court may give to states as it relates to these programs, as well as a confirmation that the appropriateness of a given system relates to the contemporary status of global security.

Big Brother Watch – September 2018

This recognition of a wider scope of state discretion in determining the necessity of a surveillance program becomes particularly poignant in the *Case of Big Brother Watch and Others v. United Kingdom*. The First Section determined that, while there was no judicial authorization nor was the authorizing body independent of the executive, certain substantive processes used in authorization passed the court's scrutiny. While the court here reiterated that judicial authorization is "highly desirable,"[47] it also appeared to depart from a clear rule and adopt a standard which looks to the potential for abuse.[48] In this case, "pre-authorization scrutiny of warrant applications" and "extensive post-authorization scrutiny," could be sufficient.[49] But, as will be addressed below, the issue with any standard is that future application by courts is made more unpredictable.

---

[44] *Case of Centrum For Rattvisa v. Sweden*, sec. 197
[45] Ibid
[46] Ibid, sec. 180-81
[47] *Case of Big Brother Watch and Others v. United Kingdom*, nos. 58170/12, 62322/14 and 24960/15, European Court of Human Rights, 13 September 2018 (referral to Grand Chamber 04 February 2019), http://hudoc.echr.coe.int/eng?i=001-186048
[48] Christakis, Theodore, "A Fragmentation of EU/ECHR Law on Mass Surveillance: Initial Thoughts on the Big Brother Watch Judgement," *European Law Blog*, September 20, 2018, http://europeanlawblog.eu/2018/09/20/a-fragmentation-of-eu-echr-law-on-mass-surveillance-initial-thoughts-on-the-big-brother-watch-judgment/
[49] *Case of Big Brother Watch and Others v. United Kingdom*, sec. 381

Comparing the Case Law

It does seem that in critical respects, the CJEU and the ECHR align in their approach to mass surveillance programs as they relate to privacy rights. Both require the adoption of safeguards which are meant to act as checks against potential agency abuse. Both have previously recognized the need for individualized suspicion insofar as there ought to be a relationship between an investigation and the particular data being obtained or held. The courts also indicate a strong preference for ex-post notification of surveillance and clear laws that provide for foreseeable implementation.

Although, there appears to be is less alignment following *Big Brother Watch*. There, the ECHR indicates that ex-post notification of the surveilled subject is no longer a requirement, given the nature of bulk surveillance.[50] Similarly, the court reaffirmed the security value of bulk surveillance, seemingly shying away from concerns about the unpredictability inherent in such surveillance programs.[51] Additionally, it seemed to move away from the requirement that there be prior authorization by a court or independent body of the data gathering, although that was a critical component of the *Zakharov* and Vissy decisions.[52] Thus, the court in *Big Brother Watch* appeared to loosen some of the legal expectations in the context of mass surveillance.[53]

While *Big Brother Watch* was lauded as a success amongst privacy rights advocates, given that the end result was favorable to their cause,[54] the shift to more of a standard with respect to procedural checks introduces some instability to the ECHR regime. Standards are of course notoriously slippery and can more readily produce inconsistencies in the case law. In this

[50] Ibid, sec. 317
[51] Ibid, sec. 384-86
[52] Christakis, "A Fragmentation of EU/ECHR Law on Mass Surveillance"
[53] Ibid
[54] Ibid

instance, it seems that "substance prevails over form."[55] Thus it is not entirely clear where the ECHR law stands, and it will have to be seen whether the CJEU follows suit.

While this is a body of law that will continue to shift in important ways, especially as geopolitical concerns over terrorism do, the *Big Brother Watch* decision indicates that it is the CJEU which may be more committed to the rules that have been laid down. This is consistent with the foundational documents protecting individual rights that each court interprets. The Convention, which is interpreted by the ECHR, has an article devoted to a general privacy right.[56] The Charter, which is within the purview of the CJEU, goes further, however, and instantiates protections for personal digital data specifically.[57] Admittedly, the substantive difference this implies may not be major insofar as the Convention is an older document by about five decades, before digital concerns were salient. There is of course no doubt that the ECHR recognizes the right to the protection of digital data as an extension of the broader privacy rights. Nonetheless, the explicit nature of the Charter on this point may lend itself more to the development of clear rules by the CJEU.

Another explanation might be that the CJEU is responsive to, or at least structurally related to, as an institutional matter, the European Parliament which has over recent years taken serious steps to increase the strength of data privacy protection. The most obvious example of this is the passing of the GDPR. The Council of Europe does not have an equivalent political body which might influence the ECHR.

On-going Cases and Implications

[55] Ibid
[56] European Convention on Human Rights, art. 8
[57] Charter of Rights, art. 7-8

As cited by Privacy International in a brief in a current case ongoing against the French Data Network in the CJEU, the three CJEU cases considered above form the nexus of case law which determines the CJEU's requirements with respect to the protections of citizen data and thus should be looked to in making decisions.[58] In addition to this case, there is another filed regarding the United Kingdom; both are likely to test the court's commitment to the conditions developed in *Tele2*. The United Kingdom's Investigatory Powers Tribunal has filed for a preliminary ruling, asking for a clearer description of how the *Tele2* requirements play out in the context of what they call the "essential necessity" of their bulk surveillance program.[59] It noted that a domestic national court had determined the requirements "would frustrate the measures taken to safeguard national security by the [Security and Intelligence Agencies], and thereby put the national security of the United Kingdom at risk."[60] Thus the question is poignant: how might the requirements hold up when there is already a determination that they will impede national security?

Given that the ECHR has recently indicated deference in *Centrum for Rattvisa* and *Big Brother Watch* to state agencies regarding how they determine their systems, this would be a particularly important ruling by the CJEU. The question has been put sharply as the Tribunal phrases it in a way that precisely pits the security concerns, which are supposed to be in the purview of individual states, against the safeguards which European courts are requiring. Given

[58] Brief Filed By Privacy International, Court of Justice of the European Union, cases nos. C-511/18 and C-512/18, page 3, https://privacyinternational.org/sites/default/files/2019-01/French_data_retention_PI_submission_to_the%20CJEU_english_translation.pdf

[59] Reference for a preliminary ruling from the Investigatory Powers Tribunal - London (United Kingdom) made on 31 October 2017 – Privacy International v Secretary of State for Foreign and Commonwealth Affairs and Others, case C-623/17, http://curia.europa.eu/juris/document/document.jsf?text=&docid=198575&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=563720

[60] Ibid

that considerations of national security exert significant influence, the CJEU would likely have to rather directly repudiate the *Tele2* requirements if it were to rule in the U.K.'s favor.

Conclusion

While the CJEU and the ECHR had been relatively consistent in what they have required of state surveillance programs as it relates to privacy rights, the *Big Brother Watch* case may have changed that. The cases that come in the next few years will be essential in establishing where the law stands. But, given that the case law is starting to become robust on this topic, as courts work out where they stand, it is likely to inform how GDPR Article 23(1) issues would be adjudicated.