vaccination requirements may significantly implicate other rights, such as freedom of movement under Article 2, Protocol No. 4. Nevertheless, the Court's use of the term "social solidarity" seems to send a message that it would not be disproportionate for states to impose compulsory COVID-19 vaccination *in the name of that solidarity*, as having the highest level of vaccination would protect people who are vulnerable to COVID-19, including the elderly, the immunocompromised, and people with comorbidities. At the same time, there is no uniform practice as to how the highest level of COVID-19 vaccination should be achieved. As a result, if a state were to introduce mandatory COVID-19 vaccination, *Vavřička* indicates that such a state would enjoy a wide margin of appreciation under the ECHR. This is further underpinned by the observation that the Court tends to grant a particularly wide margin of appreciation in the field of bioethics.[9] On our reading, unless the measure would be clearly disproportionate (such as the imposition of a blanket obligation without possibilities of exemptions for those with contraindications), the ECtHR would probably accept mandatory vaccination for COVID-19 to be in accordance with the ECHR.

Ignatius Yordan Nugraha,
Juncal Montero Regules, and
Merel Vrancken
Hasselt University
doi:10.1017/ajil.2022.36

Personal data—national security—intelligence—international intelligence sharing—surveillance—data privacy—European Convention on Human Rights

Big Brother Watch and Others v. the United Kingdom. App. Nos. 58170/13, 62322/14, 24960/15. Judgment. *At* http://hudoc.echr.coe.int/eng?i=001-210077. European Court of Human Rights (Grand Chamber), May 25, 2021.

On May 25, 2021, the Grand Chamber of the European Court of Human Rights (ECtHR) ruled in joined cases *Big Brother Watch and Others v. the United Kingdom* (*Big Brother Watch*)[1] that some aspects of the United Kingdom's surveillance regime violated the rights to privacy and freedom of expression, guaranteed under Articles 8 and 10 of the European Convention on Human Rights (ECHR).[2] The program enabled the UK authorities to bulk intercept communications data, acquire data from communications service providers, and receive material from foreign intelligence services, all with wide discretion. The ECtHR found that the UK program violated the Convention due to several procedural

[9] Carmen Draghici, The Legitimacy of Family Rights in Strasbourg Case Law: "Living Instrument" or Extinguished Sovereignty? 134 (2017).

[1] Big Brother Watch and Others v. the United Kingdom, App. Nos. 58170/13, 62322/14, 24960/15, Grand Chamber Judgment (Eur. Ct. Hum. Rts. May 25, 2021), *at* http://hudoc.echr.coe.int/eng?i=001-210077.

[2] Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights), ETS 5 (1953), *available at* https://www.echr.coe.int/Documents/Convention_ENG.pdf.

deficiencies. Yet, ultimately, the decision stands for a highly permissive approach to government surveillance.

The Grand Chamber decision marks the end of an eight-year battle spearheaded by sixteen journalists and NGOs following the Edward Snowden revelations about the U.S. and UK's mass surveillance programs in 2013. Across three separate legal challenges, the claimants contended that the surveillance programs under UK's Regulation of Investigatory Powers Act (RIPA) 2000[3] failed to operate "in accordance with the law."[4] The Grand Chamber agreed with the applicants that the regimes for the bulk interception of communications data and the acquisition of intelligence from communication service providers—but not for the receipt of foreign intercept material—violated ECHR. The *Big Brother Watch* decision has significant implications not only for the UK's legal framework for bulk interception programs, but also for data privacy law, the future of mass surveillance programs and intelligence data sharing regimes in the UK, Europe, and beyond. The ruling is particularly relevant now as national governments are increasingly relying on intrusive methods of data collection and contact tracing to prevent the spread of COVID-19.

The case was initially decided by a lower Chamber of the ECtHR in 2018, which held that aspects of the UK's data interception and acquisition systems violated Articles 8 and 10 of the Convention.[5] The Chamber held that bulk interception was not *per se* impermissible under the ECHR[6] and that contracting states' governments enjoy a wide "margin of appreciation" in deciding what is necessary to guarantee national security.[7]

The Grand Chamber agreed. It emphasized that Article 8 permits bulk interception, and devoted attention to the procedural safeguards required of surveillance regimes. The Grand Chamber found that the UK's bulk interception of communications framework, referred to as the "Section 8(4) regime," entailed three "fundamental deficiencies." First, bulk interception was not authorized by a body independent of the executive, but by the secretary of state. Second, the categories of search terms defining the kinds of communications to be examined were not included in the warrant application. And third, the use of specific identifiers ("subject selectors linked to an individual") had not been authorized.[8] Thus, being too broad, the "Section 8(4) regime" failed to satisfy the "quality of law" requirement, rendering it incapable of keeping the rights interference to a degree "necessary in a democratic society."[9]

Moreover, the Grand Chamber unanimously decided that the UK's acquisition of communications data from communication service providers (the "Chapter II regime") also breached Article 8 because it failed to limit access to data solely for the purpose of combatting

[3] Regulation of Investigatory Powers Act 2000 (UK), *at* https://www.legislation.gov.uk/ukpga/2000/23/contents.

[4] The case is three joined applications: Big Brother Watch & Others v. the United Kingdom, App. No. 58170/13; Bureau of Investigative Journalism and Alice Ross v. the United Kingdom, App. No. 62322/14; and Ten Human Rights Organisations and Others v. the United Kingdom, App. No. 24960/15.

[5] Big Brother Watch and Others v. the United Kingdom, App. Nos. 58170/13, 62322/14, 24960/15, Chamber Judgment, 388, 468, 500 (Eur. Ct. Hum. Rts. Sept. 13, 2018), *at* http://hudoc.echr.coe.int/eng?i=001-186048.

[6] *Id.* at 314.

[7] *Id.* at 308.

[8] *Big Brother Watch* (Grand Chamber), *supra* note 1, at 425.

[9] *Id.* at 426.

https://doi.org/10.1017/ajil.2022.35 Published online by Cambridge University Press

"serious crime" and did not require a prior review by a court or an independent administrative body.[10]

The Court further ruled that both the bulk interception of communications[11] *and* the acquisition of data from the service providers[12] had violated Article 10 because of a lack of safeguards in relation to journalistic sources and confidential journalistic material.

Finally, a majority of the Court (twelve to five) decided that the system of information sharing, through which the UK authorities received material from foreign intelligence services, did not violate Articles 8 or 10.[13] In the majority's view, intelligence sharing is permissible provided that there are certain additional safeguards (1) domestic law must clearly articulate the circumstances in which such a transfer may take place; and (2) the transferring state must receive guarantees from the receiving state about secure storage of information and restrict its onward disclosure. This, however, "does not necessarily mean that the receiving State must have comparable protection to that of the transferring State; nor does it necessarily require that an assurance is given prior to every transfer."[14]

Five judges argued, in three separate opinions, that the judgment does not go far enough. For example, Judges Lemmens, Vehabović, and Bošnjak, stated that the judgment does not provide "any clear substantive protection . . . against disproportionate interference" by surveillance regimes,[15] and judicial authorization should be required for bulk interception.[16] Judge Pinto de Albuquerque issued the most far-reaching opinion, rejecting outright the proportionality of mass surveillance programs and criticizing the Court's procedural focus as inadequate toward preventing abuse.[17]

* * * *

Following September 11, 2001, the UK enacted extensive surveillance and data retention regimes which provided law enforcement agencies with intrusive powers to battle the "war on terror."[18] These expansive regimes have been cast as "inevitable" and "vital to the war on terror and defending . . . citizens against a ruthless enemy."[19] The ECtHR has examined many such regimes over the past two decades, including those of Sweden,[20] Hungary,[21]

[10] *Id.* 524–25.

[11] *Id.* at 458.

[12] *Id.* at 528.

[13] *Id.* at 514, 516; *cf.* joint part. diss. op., Lemmens, Vehabović, Ranzoni, Bošnjak, JJ., at 1; part. concur., part. diss. op., Pinto de Albuquerque, J., at 1.

[14] Centrum för Rättvisa v. Sweden, App. No. 35252/08, Grand Chamber Judgment, at 362 (Eur. Ct. Hum. Rts. May 25, 2021), *at* http://hudoc.echr.coe.int/eng?i=001-210078.

[15] *Big Brother Watch* (Grand Chamber) (joint part. concur. op., Lemmens, Vehabović, Bošnjak, JJ.), *supra* note 1, at 14.

[16] *Id.* (joint part. concur. op., Lemmens, Vehabović, Bošnjak, JJ.) at 23–24.

[17] *Id.* (part. concur., part. diss. op., Pinto de Albuquerque, J.).

[18] Monika Zalnieriute, *A Struggle for Competence: National Security, Surveillance and the Scope of EU Law at the Court of Justice of European Union*, 85 MOD. L. REV. 198 (2022).

[19] White House Press Release, President Applauds Senate for Voting to Renew Patriot Act (2006), *at* https://georgewbush-whitehouse.archives.gov/news/releases/2006/03/20060302-18.html.

[20] *Centrum för Rättvisa* (Grand Chamber), *supra* note 14.

[21] Szabó and Vissy v. Hungary, App. No. 37138/14, Chamber Judgment (Eur. Ct. Hum. Rts. Jan. 12, 2016), *at* http://hudoc.echr.coe.int/eng?i=001-160020.

https://doi.org/10.1017/ajil.2022.35 Published online by Cambridge University Press

Russia,[22] Germany,[23] Moldova,[24] Romania,[25] and (in several instances) the UK, tending to afford states a wide "margin of appreciation" (or zone of discretion) in this area.[26]

Big Brother Watch is the first ECtHR ruling against the UK's mass surveillance programs since the 2013 Snowden revelations about the U.S. and UK electronic surveillance regimes. While the judgment concerns surveillance regimes under RIPA 2000, and the superseding Investigatory Powers Act 2016 (IPA).[27] The Grand Chamber ruling sets a standard against which any other bulk interception regimes will be examined. However, from the perspective of privacy and data protection, that standard is a rather thin one. The Court has endorsed mass-surveillance as, *in principle,* acceptable, by holding that that bulk interception was not *per se* disproportionate, and that judicial authorization was not a requisite for the legality of bulk surveillance, which "is of vital importance to Contracting States in identifying threats to their national security" (with only one dissent on this point).[28]

The *Big Brother Watch* decision therefore reinforces and cements the Court's long-standing liberal approach that governments may continue to deploy mass surveillance regimes where certain (vague) procedural safeguards are incorporated. Citing its earlier decisions in *Weber and Saravia*,[29] *inter alia*, the Court affirmed the "six minimum requirements" for surveillance schemes, known as "six Weber safeguards." These require domestic law to specify: (1) the nature of offenses that may give rise to an interception order; (2) a definition of the categories of people liable to have their communications intercepted; (3) a limit on the duration of interception; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which intercepted data may or must be erased or destroyed.[30] Moreover, the Grand Chamber adds, here, two additional elements in the context of national security: (7) supervision of the implementation of secret surveillance measures; and (8) notification of secret surveillance measures and available remedies.[31] However, where the Court continues to grant states a wide margin of appreciation to uphold national security, vague conformity with the "six minimum requirements" will often not breach Article 8. The international intelligence sharing regime in *Big Brother Watch*, did not, in the majority's view, breach Article 8 because it had "adequate safeguards for the examination, use and storage of the content

[22] Roman Zakharov v. Russia, App. No. 47143/06, Grand Chamber Judgment (Eur. Ct. Hum. Rts. Dec. 4, 2015), *at* http://hudoc.echr.coe.int/eng?i=001-159324.

[23] Uzun v. Germany, App. No. 35623/05, Chamber Judgment (Eur. Ct. Hum. Rts. Sept. 2, 2010), *at* http://hudoc.echr.coe.int/eng?i=001-100293.

[24] Iordachi and Others v. Moldova, App. No. 25198/02, Chamber Judgment (Eur. Ct. Hum. Rts. Feb. 10, 2009), *at* http://hudoc.echr.coe.int/eng?i=001-91245.

[25] Dumitru Popescu v. Romania (No. 2), App. No. 71525/01, Chamber Judgment (Eur. Ct. Hum. Rts. July 26, 2007), *at* http://hudoc.echr.coe.int/eng?i=001-80352 (in French).

[26] *See, e.g.*, Weber and Saravia v. Germany, App. No. 54934/00, Chamber Judgment (Eur. Ct. Hum. Rts. June 29, 2006), *at* http://hudoc.echr.coe.int/fre?i=001-76586.

[27] Investigatory Powers Act 2016 (UK), *at* http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

[28] *Big Brother Watch* (Grand Chamber), *supra* note 1, at 424.

[29] *Weber and Saravia*, *supra* note 26, at 95.

[30] *Big Brother Watch* (Grand Chamber), *supra* note 1, at 335; *Weber and Saravia*, *supra* note 26, at 95.

[31] *Big Brother Watch* (Grand Chamber), *supra* note 1, at 335.

https://doi.org/10.1017/ajil.2022.35 Published online by Cambridge University Press

and communications data received from intelligence partners; for the onward transmission of this material; and for its erasure and destruction."[32]

Big Brother Watch is also the first decision on the legality of international intelligence sharing under the ECHR, and thus will shape the future of intelligence sharing regimes. Here, the Grand Chamber's approach contrasts sharply with the CJEU approach, where the emphasis is on the safeguards provided by the third countries receiving the information. For example, in the *Schrems II* decision, delivered in July 2020, the CJEU invalidated the EU-U.S. Privacy Shield agreement,[33] which enabled transatlantic data transfers between the two regions, due to lack of adequate safeguards in the surveillance framework of the receiving country—the United States.[34] As *Big Brother Watch* concerned the requests and reception of intelligence from foreign countries by the UK (as opposed to transfers of intelligence to foreign countries), the sole focus on legislative safeguards *in* the UK is understandable. However, it remains unclear whether the ECHR requires adequate safeguards in the recipient country, if the UK or another ECHR contracting state shared the data with foreign countries.[35] If the focus remains solely on the legislative framework of the transferring country (e.g., the UK), ignoring the safeguards of the country with whom data is shared (e.g., the United States), such interpretation would leave UK residents vulnerable to the misuse of personal data by U.S. authorities, without a remedy.[36]

The ECtHR's approach is ultimately minimalist and deferential. Not only may governments deploy mass surveillance regimes, they may also share gathered information with other countries as long as "certain safeguards" are in place. For the Grand Chamber, "independent authorisation at the outset" "supervision and independent *ex post facto* review" are the "fundamental" and "cornerstone" safeguards for any bulk interception regime to be compliant with Article 8.[37] Thus, the focus is not on the substantive legality *or* the actual effectiveness of the regime, but solely on procedural safeguards. In fact, the procedures matter so much for the Court that it develops "a wider range of criteria than the six *Weber* safeguards"[38] listed above.

[32] *Id.* at 510.

[33] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, C/2016/4176 OJ L207 (2016), *at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

[34] Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd & Maximillian Schrems, ECLI:EU:C:2020:559, Grand Chamber Judgment (Ct. Just. Eur. Union July 16, 2020), *at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6478357.

[35] *Big Brother Watch* (Grand Chamber), *supra* note 1, at 500–14.

[36] Monika Zalnieriute & Genna Churches, *Rejecting the Transatlantic Outsourcing of Data Protection in the Face of Unrestrained Surveillance*, 80 CAMBRIDGE L.J. 8 (2021); Genna Churches & Monika Zalnieriute, *"Contracting Out" Human Rights in International Law:* Schrems II *and the Fundamental Flaws of US Surveillance Law*, HARV. INT'L L.J. ONLINE (2020), *at* https://harvardilj.org/2020/08/contracting-out-human-rights-in-international-law-schrems-ii-and-the-fundamental-flaws-of-u-s-surveillance-law.

[37] *Big Brother Watch* (Grand Chamber), *supra* note 1, at 350.

[38] *Id.* at 361.

https://doi.org/10.1017/ajil.2022.35 Published online by Cambridge University Press

These safeguards, as the Grand Chamber explains, are part of the "global assessment of the operation of the regime."[39] But it is not clear if any of the requirements are mandatory.[40] It rather seems that non-compliance with one or several is not fatal. As Judge Pinto de Albuquerque argues in his dissent, these are expressed in "inadmissibly vague" terms.[41] Judges Lemmens, Vehabović, and Bošnjak held that the new criteria do not clearly serve as "self-standing minimum standards," nor do they "set any minimum safeguards themselves" in domestic law, failing to provide for "any clear substantive protection of an individual against disproportionate interference" with their rights.[42]

The *Big Brother Watch* majority's lax and proceduralist approach reinforces what I call the "inevitability" of mass surveillance narrative, by not questioning the effectiveness or proportionality of blanket surveillance regimes, and rather *assuming* their necessity and efficiency for ensuring national security.[43] The Court's commitment to the inevitability narrative is also clearly visible in of the parallel judgment of *Centrum för Rättvisa v. Sweden*, delivered on the same day, asserting that "in present-day conditions, no alternative or combination of alternatives would be sufficient to substitute for the bulk interception power."[44] Judge Pinto de Albuquerque's lone dissent in *Big Brother Watch* represents the alternative vision, in noting that bulk interception is "proven to be ineffective for the prevention of terrorism . . . [it] is not only dangerous for the protection of human rights but also a waste of resources."[45]

Until recently the CJEU has pushed back against the inevitability rhetoric, frequently siding with privacy activists in the wake of the 2013 Snowden revelations in many strong pro-privacy judgments.[46] However, the CJEU's recent reversals suggest

[39] *Id.* at 360.

[40] *Big Brother Watch* (Grand Chamber) (part. concur., part. diss. op., Pinto De Albuquerque, J.), *supra* note 1, at 32.

[41] *Id.* (part. concur., part. diss. op., Pinto De Albuquerque, J.) at 2.

[42] *Id.* (joint part. concur. op., Lemmens, Vehabović, Bošnjak, JJ.) at 13–14.

[43] Monika Zalnieriute, *A Dangerous Convergence: The Inevitability of Mass Surveillance in European Jurisprudence*, EJIL:*Talk!* (June 4, 2021), *at* https://www.ejiltalk.org/a-dangerous-convergence-the-inevitability-of-mass-surveillance-in-european-jurisprudence.

[44] *Centrum för Rättvisa*, Grand Chamber Judgment, *supra* note 14, at 365.

[45] *Big Brother Watch* (Grand Chamber) (part. concur., part. diss. op., Pinto De Albuquerque, J.), *supra* note 1, at 11.

[46] Joined Cases C-293/12 and C-594/12, Digital Rights Ireland Ltd. v. Minister for Communications, ECLI:EU:C:2014:238, Grand Chamber Judgment (Ct. Just. Eur. Union Apr. 8, 2014), *at* https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0293&from=EN (invalidating an EU data retention directive); Opinion 1/15 of the Court (Grand Chamber) ECLI:EU:C:2017:592, 15 (Ct. Just. Eur. Union July 26, 2017), *at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62015CV0001%2801%29 (rejecting indiscriminate national data retention regimes); Case C-362/14, Schrems v. Data Protection Commissioner, EU:C:2015:650, Grand Chamber Judgment (Ct. Just. Eur. Union Oct. 6, 2015), *at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=7622138 (invalidating EU-U.S. data-sharing); Joined Cases C-203/15 and C-698/15, Tele2 Sverige AB v. Post-och telestyrelsen; Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis, ECLI:EU:C:2016:970, Grand Chamber Judgment (Ct. Just. Eur. Dec. 21, 2016), *at* https://curia.europa.eu/juris/document/document.jsf?text=&docid=186492&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=6478357 (rejecting indiscriminate data retention in national contexts); *Schrems II*, *supra* note 34 (invalidating the EU-U.S. Privacy Shield agreement) and, most recently, Case C-623/17 Privacy International, ECLI:EU:C:2020:790, Grand Chamber Judgment, at 623 (Ct. Just. Eur. Union Oct. 6, 2020), *at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=232083&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6063852

https://doi.org/10.1017/ajil.2022.35 Published online by Cambridge University Press

the emergence of a dangerous judicial consensus on the substantive *prima facie* legality of mass surveillance programs. In particular, in *Quadrature Du Net* (2020), the CJEU ruled that the EU does not preclude indiscriminate data *retention* measures when member states can prove legitimate and serious threats to national security.[47] This decision is a significant departure from the CJEU's prior case law insisting that to be proportionate, data *retention* had to be targeted. So why has the CJEU recently changed its mind? Have the "lower" standards adopted by the ECtHR Chamber in *Big Brother Watch* ruling in 2018 influenced the CJEU's laxer approach in *Quadrature Du Net?* Whatever the reason, the European courts now appear to be converging around the "inevitability" narrative of mass surveillance.

The convergence of the two European courts on substantive legality of mass surveillance regimes in Europe will have serious implications for the future development of surveillance programs, data retention, and sharing regimes in Europe and beyond. First, such convergence comes at a crucial time for EU institutions, which are now preparing an e-Privacy Regulation,[48] and discussing an EU e-Evidence package, aimed at facilitating law enforcement agencies' and judicial authorities' cross-border access to electronic evidence.[49]

Second, such convergence provides extra weight to law enforcement in the ongoing discussions and negotiations of data sharing and retention regimes on international level. For example, in 2018 the UN established an open-ended, *ad hoc*, intergovernmental committee of experts tasked to elaborate a comprehensive international convention on cybercrime.[50] The weak judgment in *Big Brother* and convergence of the ECtHR and CJEU—which are often regarded as the most pro-privacy courts in the world[51]—strengthens the position of law enforcement agencies in these ongoing discussions by affirming the *prima facie* legality of mass surveillance measures, and the ECtHR's abstract reasoning provides a lot of room to contracting states' agencies to claim that their blanket, mass-surveillance regimes fall within the "margin of appreciation." This impact is already evident in the updates to the Council of

(finding that mass *transmission* of personal data by communication service providers to intelligence agencies is not compatible with EU law).

[47] Joined Cases C-511/18 La Quadrature Du Net and Others and C-512/18 French Data Network and Others, and Case C-520/18 Ordre des barreaux francophones et germanophone and Others, ECLI:EU:C:2020:791, Grand Chamber Judgment, at 136 (Ct. Just. Eur. Union Oct. 6, 2020), *at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=232084&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=6166350.

[48] Proposal for a Regulation of the European Parliament and of the Council Concerning the Respect for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) (2017), *at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010.

[49] European Commission, Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters (2018), *at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN; European Commission, Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings (2018), *at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A226%3AFIN; European Commission Press Release, Security Union: Commission Facilitates Access to Electronic Evidence (Apr. 17, 2018), *at* https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3343.

[50] Resolution Adopted by the General Assembly on 27 December 2019, Countering the Use of Information and Communications Technologies for Criminal Purposes, UN Doc. A/RES/74/247, *at* https://digitallibrary.un.org/record/3847855?ln=en.

[51] Hielke Hijmans, The European Union as Guardian of Internet Privacy 17–75 (2016).

https://doi.org/10.1017/ajil.2022.35 Published online by Cambridge University Press

Europe's Cybercrime Convention ("Budapest Convention"),[52] which is the only binding international instrument on this issue. (The parties include the United States and the EU member states, except for Ireland and Sweden). The Second Additional Protocol to the Budapest Convention was adopted on November 21, 2021 and provides for enhanced international cooperation, including provisions on direct cooperation of law enforcement authorities with service providers in other jurisdictions.[53]

In conclusion, the ECtHR decision in *Big Brother Watch* will impact the future of surveillance. Currently, mass data interception is expressly prohibited in twenty-three European states. As the three partially dissenting judges noted: "There are rare occasions when the Court adjudicates on a case which shapes the future of our societies. The present one is such an example."[54] The ECtHR's minimalist approach, prioritizing procedural safeguards, as opposed to substantive legality, has also likely influenced the latest CJEU's case law on intelligence and surveillance. The full palette of constitutional and practical implications of such an increasing convergence between the two powerful European Courts remains to be seen, but it is likely that mass surveillance regimes will become increasingly legitimate in the UK, EU, wider Europe, and beyond. As Judge Pinto De Albuquerque warns in his dissenting opinion, "[i]n some corners of Europe, zealous secret services will be strongly tempted to take advantage of the Court's very lax fashion of formulating legal standards and innocent people will pay the price sooner or later."[55]

MONIKA ZALNIERIUTE
Faculty of Law and Justice, UNSW Sydney; Australia
Law Institute of Lithuanian Centre for Social Sciences, Lithuania
doi:10.1017/ajil.2022.35

[52] Convention on Cybercrime, Budapest, CETS No. 185 (2001), *available at* https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf.

[53] Cybercrime Convention Committee (T-CY), Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence, CM(2021)57-final (Nov. 17, 2021), https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4d.

[54] *Big Brother Watch* (Grand Chamber) (joint part. concur. op., Lemmens, Vehabović, Bošnjak, JJ.), *supra* note 1, at 30.

[55] *Id.* (part. concur., part. diss. op., Pinto de Albuquerque, J.) at 15.