WSGR Wilson Sonsini Goodrich & Rosati, LLP
Avocats - Advocaten - Rechtsanwälte

Rue Montoyer 47
1000 Brussels
Belgium

PHONE +32 2 274 57 00
FAX +32 2 274 57 99

www.wsgr.com

5 September 2016

Claudia Westerdiek
Section Registrar
European Court of Human Rights
Council of Europe
F-67075 Strasbourg cedex
France

Re: BREYER v GERMANY, APP. No. 50001/12

Dear Ms. Westerdiek,

I am writing to you on behalf of Privacy International and ARTICLE 19. Please find enclosed the written submissions of Privacy International and ARTICLE 19 in respect of the abovenamed case.

Kind regards,

Cédric Burton
Avocat – Member of the Brussels Bar
Wilson Sonsini Goodrich & Rosati, LLP

PRIVACY INTERNATIONAL

ARTICLE 19

5 September 2016

C. Westerdiek
Section Registrar
European Court of Human Rights
Council of Europe
F-67075 Strasbourg cedex
France

Re: BREYER v GERMANY, APP. No. 50001/12

Dear Ms. Westerdiek,

Please find enclosed the written submissions of Privacy International and ARTICLE 19 in respect of the abovenamed case.

Kind regards,

Tomaso Falchetta
Legal Officer
Privacy International

Gabrielle Guillemin
Senior Legal Officer
ARTICLE 19

IN THE EUROPEAN COURT OF HUMAN RIGHTS APPLICATION NO. 50001/12

B E T W E E N:

PATRICK BREYER and JONAS BREYER

Applicants

-v

GERMANY

Respondent Government

WRITTEN SUBMISSIONS ON BEHALF OF PRIVACY INTERNATIONAL AND ARTICLE 19

INTRODUCTION AND SUMMARY

1. Privacy International and ARTICLE 19 ("the Interveners") provide this written submission in order to elaborate upon the importance of anonymity to the rights of privacy and freedom of expression, which provides necessary context for evaluating the data retention requirements set forth in Section 111 of the German Federal Telecommunications Act (*Telekommunikationsgesetz*, or "TKG", in its versions of 2004 and 2007). This Court granted the Interveners leave to intervene jointly as a third party in this case on 13 July 2016. As directed, these submissions do not comment on the facts or merits of the case.

2. Privacy International is a nonprofit, nongovernmental organisation based in London dedicated to defending the right to privacy around the world.[1] Established in 1990, Privacy International undertakes research and investigations into state and corporate surveillance with a focus on the technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States of America and Europe, including the European Court of Human Rights. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect privacy.

3. ARTICLE 19 is an international human rights organisation that defends and promotes freedom of expression all over the world.[2] Established in 1987, ARTICLE 19 takes its name and mandate from Article 19 of the Universal Declaration of Human Rights. ARTICLE 19 monitors threats to freedom of expression in different regions of the world, as well as national and global trends, and develops long-term strategies to address them. It also advocates for the implementation of the highest standards of freedom of expression both nationally and globally.

4. The Interveners summarise their intervention as follows:

    a. Section 1 provides background on anonymity and its importance to a democratic society;

---

[1] Privacy International, What We Do (2016), https://www.privacyinternational.org/projects.
[2] ARTICLE 19, What We Do (2016), https://www.article19.org/pages/en/what-we-do.html.

b. Section 2 provides a summary of international and domestic legal authorities that advocate for protecting anonymous speech under human rights standards;

c. Section 3 provides a summary of general data retention obligations and how they interfere with anonymity and the rights of privacy and freedom of expression, and provides a framework for analysing such obligations under human rights standards.

THE SIGNIFICANCE OF ANONYMOUS SPEECH

5. Anonymity and anonymous speech has played a foundational role in human history.[3] Anonymity is one of the essential tools available to individuals to mitigate or avert unlawful interferences with their rights to privacy and free expression, and it has long been a means by which individuals could freely enjoy their right to impart and receive information free from state control. As such, anonymity, which has traditionally been linked to the right to privacy and protection of personal data,[4] is also an important safeguard for the exercise of the right to freedom of expression.[5]

6. "At its simplest, anonymity is *the fact* of not being identified and, in this sense, it is part of the ordinary experience of most people on a daily basis, e.g. walking as part of a crowd or standing in a queue of strangers."[6] As such, "an activity can be anonymous even though it is also public."[7] That one can be both public and maintain her identity as secret is the very benefit of anonymity—that is what allows individuals to freely engage in works that critique governments or powerful actors, or expose wrongdoings.[8]

7. It is in this context that this Court has emphasised the importance of anonymity as "a means of avoiding reprisals or unwanted attention. As such, it is capable of promoting the free flow of ideas and information in an important manner, including, notably, on the Internet."[9] The Supreme Court of the United States has also characterised anonymous speech "as an honorable tradition of advocacy and of dissent" and that it acts as "a shield from the tyranny of the majority."[10] It has also identified anonymity's historical significance:

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. The obnoxious press licensing law of England, which was also enforced on the Colonies, was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the

---

[3] See generally *Anonymity as a Legal Right: Where and Why It Matters*, 16 N.C. J.L. & Tech. 311, 317-331 (2015) (discussing the historical importance of anonymity to freedom of expression).
[4] See *Rotaru v. Romania*, Application no. 28341/95 (4 May 2000), para. 42, where the Court stated that anonymity is inherent to an individual's private life as protected by Article 8 of the Convention.
[5] Article 19, Right to Online Anonymity (18 June 2015), at p. 1. Available at https://www.article19.org/data/files/medialibrary/38006/Anonymity_and_encryption_report_A5_final-web.pdf.
[6] *Id.* at p. 10.
[7] *Id.*
[8] Privacy International, Securing Safe Spaces Online, at p. 8. Available at: https://www.privacyinternational.org/sites/default/files/Securing%20Safe%20Spaces%20Online_0.pdf.
[9] *Delfi AS v. Estonia*, Application no. 64569/09 (16 June 2015), para. 147.
[10] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995), at p. 357.

circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers.[11]

8. In other words, anonymity has given individuals throughout history a necessary cloak with which to shield themselves from reprisal—reprisal from the state, their fellow countrymen and women, or, increasingly, would-be oppressors located anywhere in the world. These individuals may be whistleblowers, who seek to expose the latest abuse of power by a government agency or private company. They may be dissidents, who seek to expand the channels of governance to include the dispossessed. They may be sources for journalists, who provide the necessary informational inputs to make democracy work.[12] Or they may be everyday people who are not comfortable discussing their trials and tribulations without the layer of protection that anonymity provides.[13] For all of these speakers, anonymity "protects the freedom of individuals to live their lives without unnecessary and undue scrutiny."[14] If we value anonymity as a tool for an open and diverse conversation in society, we must also value the anonymity between two persons in a telephone conversation. Investigative journalism, whistleblowers and other individuals that are preparing to make a controversial or government-opposing message public should not just be protected once they are standing in the public eye. Without these anonymous sources, many essential news stories would never be published. "Arguing that you don't care about the right to privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say."[15]

9. But "without effective protection of the right to privacy, the right of individuals to communicate anonymously and without fear of their communications being unlawfully detected cannot be guaranteed."[16] That is particularly true in the modern world, where people rely on a growing range of both fixed-location and mobile electronic devices which enhance their possibilities to communicate, participate in and manage their everyday lives. While these devices have greatly expanded human experience—making possible real-time conversations between almost anyone anywhere at any time—they are also capable of collecting and storing data, including personal data such as websites visited, keystrokes that reveal passwords, geographical locations that potentially allow tracking and surveillance of people. This data can reveal sensitive personal information (such as sexual orientation, health, political, and religious preferences). The type and amount of personal data

---

[11] *Talley v. California*, 362 U.S. 60 (1960), at pp. 64-65.

[12] See Privacy International, Submission to the UN Special Rapporteur on freedom of expression – anonymity and encryption in digital communications (February 2015), at p. 2. Available at: http://www.ohchr.org/Documents/Issues/Opinion/Communications/PrivacyInternational.pdf. See also Electronic Frontier Foundation, Anonymity, https://www.eff.org/issues/anonymity.

[13] See Gabriela Coleman, Anonymity Online Serves Us All, N.Y. Times (20 Aug. 2014). Available at: http://www.nytimes.com/roomfordebate/2014/08/19/the-war-against-online-trolls/anonymity-online-serves-us-all. The op-ed discusses equally significant but more common forms of anonymous speech, such as "medical patients and mothers [who] discuss sensitive issues (be they clinical or related to parenting) in pseudonymous forums, . . . [a]nd . . . victims of hate crimes [who] use anonymity to speak out as well: anonymity can empower those who seek consolation and justice to speak out against assailants enabled by the same processes."

[14] Article 19, Right to Online Anonymity, *supra* note 5, at p. 10.

[15] See Edward Snowden with American Civil Liberties Union's Jameel Jaffer, Reddit "Ask Me Anything" Session on 21 May 2015. Available at: https://www.reddit.com/r/IAmA/comments/36ru89/just_days_left_to_kill_mass_surveillance_under/.

[16] Privacy International, Submission to the UN Special Rapporteur, *supra* note 12, at p. 1.

collected is increasing exponentially as computing is now ubiquitous with the apogee of smartphones. The large amount of personal and sensitive data collected via these devices can be used or abused by political authorities against the speaker. Consequently, the right to privacy and to communicate anonymously in our digital economy is of the utmost importance to protect from unlawful government surveillance.[17] It is perhaps unsurprising, then, that "[a]nonymity is a deeply held value for many internet users and has contributed to a robust internet public sphere."[18]

10. While anonymity on the devices we use to access the internet can be supported by technological measures that protect users from identification, those measures are not sufficient on their own.[19] Non-technological means of preserving anonymity—such as by allowing users to sign up for accounts and purchase devices without turning over identifying information—still have a significant role to play.

11. Because of anonymity's importance to the free exchange of ideas and the ability to live a full private life, courts and human rights experts have started evaluating interferences with anonymity under relevant human rights standards—e.g., legality, necessity, and proportionality—and have required strict procedural safeguards to protect people if the interference is to be permitted.[20]

INTERNATIONAL AND DOMESTIC LEGAL AUTHORITIES HAVE MOVED TOWARDS RECOGNISING ANONYMITY AS A RIGHT UNDER THE RIGHTS OF PRIVACY AND FREEDOM OF EXPRESSION

12. In 2003, the Committee of Ministers of the Council of Europe adopted a Declaration on freedom of communication on the Internet.[21] One of the seven principles concerned anonymity:

> In order to ensure protection against online surveillance and to enhance the free expression of information and ideas, member states should respect the will of users of the Internet not to disclose their identity. This does not prevent member states from taking measures and co-operating in order to trace those responsible for criminal acts, in accordance with national law, the Convention for the Protection of Human Rights and Fundamental Freedoms and other international agreements in the fields of justice and the police.

---

[17] See United Nations, Human Rights Council (2014). The right to privacy in the digital age, Report of the Office of the United Nations High Commissioner for Human Rights, 30 June 2014, A/HRC/27/37, para. 1 (discussing the omnipresence of modern digital communications technology). Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A-HRC-27-37_en.doc.

[18] Privacy International, Securing Safe Spaces Online, *supra* note 8, at p. 8.

[19] Encryption of communications is increasingly common and supported by a wide range of platforms, but as the Special Rapporteur on freedom of expression recognised, "encryption protects the content of communications but not identifying factors such as the Internet Protocol (IP) address." United Nations, Human Rights Council (2015). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye (22 May 2015), A/HRC/29/32, at para. 9. Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc. Other "tools such as virtual private networks (VPNs), proxy services, anonymizing networks and software, and peer-to-peer networks" can protect users from much detection, but they are not commonly used. *Id.*

[20] Article 19, Right to Online Anonymity, *supra* note 5, at p. 22-23.

[21] Council of Europe, Declaration on freedom of communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th meeting of the Ministers' Deputies). Available at: http://portal.unesco.org/ci/en/files/25147/11861368651Declaration-Inf(2003)007.pdf/Declaration-Inf(2003)007.pdf.

13. In the commentary supporting the principles, the Committee noted that the "aim of this principle is first and foremost to underline that the will of users to remain anonymous should be respected."[22] The Committee recognised that "users may have a valid reason not to reveal their identity when they have statements published on the Internet" and that "[o]bliging them to do so could restrict excessively their freedom of expression."[23] The Committee also observed that "users need protection against unwarranted on-line surveillance by public or private entities."[24]

14. Since then, the law's treatment of anonymity and anonymous speech has expanded and been refined. This Court had reason to consider the Declaration and the issue of anonymity in *Delfi AS v. Estonia*, Application no. 64569/09 (16 June 2015). There, the injured party had sued a media organisation for damages arising out of anonymous comments instead of suing the commenters themselves. The Court reaffirmed the importance of anonymity to online speech and described various types of anonymity available to users of the internet. It also highlighted certain procedural safeguards that protect the release of identifying information—for example, "[t]he release of such information would usually require an injunction by the investigative or judicial authorities and would be subject to restrictive conditions."[25]

15. International law experts have long argued that interferences with anonymity should be analysed under relevant human rights standards.

16. Both the current and prior Special Rapporteurs to the United Nations on the promotion and protection of the right to freedom of opinion and expression have been steadfast proponents of anonymity as part of the right to freedom of expression. As early as 2011, Special Rapporteur Frank La Rue identified the interplay between the right to privacy and the right to freedom of expression online[26] and emphasised that any interference with anonymity should be subject to the same three part test of legality, necessity, and proportionality as any other interference with freedom of expression.[27]

17. In 2013, Special Rapporteur La Rue elaborated on his 2011 report. He reemphasised the interconnected nature of the right of privacy and that of freedom of expression and noted the need "to ensure the privacy, security and anonymity of communications."[28]

---

[22] *Id.* at p. 12.
[23] *Id.*
[24] *Id.*
[25] *Delfi AS v. Estonia*, para. 148.
[26] United Nations, Human Rights Council (2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 16 May 2011, A/HRC/17/27, at para. 53 ("The right to privacy is essential for individuals to express themselves freely. Indeed, throughout history, people's willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously."). Available at: http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
[27] *Id.* at paras. 24, 59.
[28] United Nations, Human Rights Council (2013), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013, A/HRC/23/40, para 79. Available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

18. Special Rapporteur La Rue rightly noted that "[o]ne of the most important advances facilitated by the advent of the Internet was the ability to anonymously access and impart information, and to communicate securely without having to be identified", but that "in the name of security and law enforcement, gradually States have been eradicating the opportunities for anonymous communication."[29] He specifically identified SIM card or mobile phone registration as one such encroachment, and concluded that "restrictions on anonymity have a chilling effect, dissuading the free expression of information and ideas" which "can also result in individuals' de facto exclusion from vital social spheres, undermining their rights to expression and information, and exacerbating social inequalities."[30] In his recommendations, he stated that "[s]tates should refrain from compelling the identification of users as a precondition for access to communications, including online services, cybercafés or mobile telephony"[31] and he reiterated that surveillance measures must be evaluated under the legality, necessity, and proportionality test.[32] He also reported that users should be notified when they have been subjected to surveillance.[33]

19. The current Special Rapporteur, David Kaye, has built upon in his predecessor's recommendations. He has emphasised the same interconnectedness between anonymity and the rights of privacy and freedom of expression.[34] And he notes anonymity's ability to act as a countermeasure to "unlawful censorship through filtering and other technologies."[35] He again reinforces that interferences with anonymity are subject to a human rights analysis[36], and emphasised that "States should refrain from making the identification of users a condition for access to digital communications and online services and requiring SIM card registration for mobile users."[37] Finally, Special Rapporteur Kaye stressed that there must be a remedy available to individuals affected by such measures and that "[i]n order for the right to a remedy to be meaningful, individuals must be given notice of any compromise of their privacy through, for instance, weakened encryption or compelled disclosure of user data."[38]

20. Like the U.N.'s Special Rapporteurs, Catalina Botero Marina, the Special Rapporteur for Freedom of Expression to the Inter-American Commission on Human Rights, published a report in 2013 making many of the same observations about the importance of anonymity to privacy and freedom of expression. She noted that "online spaces where people's activities and identities are not observed or documented should be promoted" and that this interest "is closely linked to the State's obligation to create a safe environment for the exercise of freedom of expression, as violation of communication

---

[29] *Id.* at para. 47.
[30] *Id.* at para. 49.
[31] *Id.* at para. 88.
[32] *Id.* at para. 83.
[33] *Id.* at para 82.
[34] United Nations, Human Rights Council (2015), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, 22 May 2015, A/HRC/29/32, para. 16. Available at: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.
[35] *Id.* at para. 12.
[36] *Id.* at para. 31 ("Restrictions on encryption and anonymity, as enablers of the right to freedom of expression, must meet the well-known three-part test: any limitation on expression must be provided for by law; may only be imposed for legitimate grounds (as set out in article 19 (3) of the Covenant); and must conform to the strict tests of necessity and proportionality.").
[37] *Id.* at paras. 60.
[38] *Id.* at para. 18.

privacy has a chilling effect and hampers the full exercise of the right to communicate."[39] She also recognised that in certain circumstances "judicial authorities would be authorised to take reasonable measures to determine the identity of the sender engaged in prohibited acts, in order to take proportionate action in response, as provided by law."[40]

21. Other jurisdictions have also developed legal safeguards for interfering with anonymous speech. In 2014, the Canadian Supreme Court reaffirmed the importance of online anonymity in the case of *R. v. Spencer*.[41] Although it fell short of pronouncing anonymity a "right," the Court outlined the importance of anonymity as "the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure."[42] It determined that the police's request for identifying information "engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognised by the Court in other circumstances as engaging significant privacy interests."[43] It concluded that the subscriber had a reasonable expectation of privacy in his subscriber (identifying) information[44], effectively requiring that the police secure a court order in similar situations in the future:

> In my view, in the totality of the circumstances of this case, there is a reasonable expectation of privacy in the subscriber information. The disclosure of this information will often amount to the identification of a user with intimate or sensitive activities being carried out online, usually on the understanding that these activities would be anonymous. A request by a police officer that an ISP voluntarily disclose such information amounts to a search.[45]

22. Similarly, U.S. courts recognise the importance of anonymity, grounded in the First Amendment's protection of freedom of speech. "[I]t is well-established that anonymous speech on the Internet, like other types of anonymous speech, enjoys First Amendment protection."[46] "The ability to speak anonymously on the Internet promotes the robust exchange of ideas and allows individuals to express themselves freely without fear of economic or official retaliation . . . [or] concern about social ostracism."[47]

23. In light of the breadth of international authorities that recognise anonymity and its role in ensuring freedom of expression and the right to privacy, the Interveners submit that this Court should evaluate

---

[39] Inter-American Commission on Human Rights (2013), Freedom of expression and the Internet, Catalina Botero Marina, 31 December 2013, OEA/Ser.L/V/II, para. 23. Available at: http://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf.
[40] *Id.* at para 135.
[41] Available at: http://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do.
[42] *Id.* at para. 48.
[43] *Id.* at para 50.
[44] *Id.* at para. 62.
[45] *Id.* at para. 66.
[46] *Awtry v. Glassdoor, Inc.*, No. 16-mc-80028-JCS, 2016 U.S. Dist. LEXIS 44804 (N.D. Cal. 1 April 2016), at p. 33.
[47] *Id.* at p. 34.

any law that restricts anonymity, like § 111 TKG, under the framework of Articles 8 and 10 of the European Convention on Human Rights.[48]

THE INTERPLAY BETWEEN MANDATORY DATA RETENTION AND ANONYMITY

24. Laws that require telecommunications companies to store identifying information about their consumers interfere with anonymity by facilitating surveillance. In a vacuum, requiring companies to store identifying information about their customers may not seem like such a profound interference with their rights to privacy or freedom of expression. But that calculus changes when that identifying information is tied to phones and other communications technology—these are the devices that individuals carry with them at all times and use as their primary means of communicating and receiving information. Once stored, that identifying information can be used to tie individuals to particular conversations, locations, and times—all the government needs to do is query a database to retrieve a name, and that name can be correlated to other data like phone numbers dialed or GPS information. By associating various data to an individual, the government can paint a precise picture of that person's life. That is why Special Rapporteur Kaye and others speak so strongly against SIM card registration laws.

25. The Interveners do not challenge the well-established principle that surveillance in some form may be necessary in combatting serious crime and genuine threats to national security.[49] But general data retention laws are indiscriminate—they subject *all* individuals to potential surveillance by forcing companies to store identifying information on all their customers. As such, those laws interfere with the public's rights of privacy and freedom of expression and must be analysed under the standards of Articles 8 and 10—that is, they must be subject to the principles of legality, necessity and proportionality. In turn, that means that the laws must incorporate certain safeguards to minimise the risk of abuse.

26. There is a growing recognition by courts in Europe and around the world that judicial authorisation and oversight is one of the most appropriate and effective safeguards against abuse and guarantor of the lawfulness of surveillance measures, and that general mandatory data retention laws should be subject to particular scrutiny. In *Digital Rights Ireland v Minister for Communications & Ors*, for example, the Court of Justice of the European Union ("CJEU") confronted the question of whether Directive 2006/24/EC of the European Parliament and of the Council on the retention of communications data ("Data Retention Directive") was compatible with Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the "Charter") and Article 8 of the Convention. The rationale of the Data Retention Directive was that mandatory retention of data by communications service providers is a surveillance measure justified on the grounds that it is a necessary and effective investigative tool for law enforcement and the protection of national security.[50] The CJEU ruled that the Data Retention Directive caused a "wide-ranging" and "particularly serious" interference with the rights to privacy and data protection, and when questioning the necessity of the measures mandated by the directive, the CJEU noted, inter alia:

---

[48] European Convention on Human Rights, Convention for the Protection of Human Rights and Fundamental Freedoms (Rome, 4.XI.1950). Available at: http://www.echr.coe.int/Documents/Convention_ENG.pdf.
[49] See, e.g., *Klass v. Germany*, Application no. 5029/71 (6 Sept. 1978).
[50] See Recital 9 of the Data Retention Directive, 2006/24/EC (15 March 2006).

> In particular, Directive 2006/24 does not lay down any objective criterion by which the number of persons authorised to access and subsequently use the data retained is limited to what is strictly necessary in the light of the objective pursued. Above all, the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits.[51]

27. Since that decision was handed down, Advocate General Saugmandsgaard Øe has had the opportunity to opine on whether general data retention obligations like the one at issue in this case are per se invalid in light of *Digital Rights Ireland.*[52] After a lengthy discussion and analysis, the Advocate General concluded that such general data retention obligations were not per se invalid, but instead might be compatible with the fundamental rights in EU law if they were subject to strict procedural safeguards.[53]

28. Among other requirements, the Advocate General concluded that the data retention obligation "must be strictly necessary in the fight against serious crime"[54] and that "the obligation must be accompanied by all the safeguards described by the Court in paragraphs 60 to 68 of its judgment of 8 April 2014 in *Digital Rights Ireland.*"[55] Those safeguards include an independent review prior to accessing the data and a limited retention period. The Advocate General also said that "the obligation must be proportionate, within a democratic society, to the objective of fighting serious crime, which means that the serious risks engendered by the obligation, in a democratic society, must not be disproportionate to the advantages which it offers in the fight against serious crime."[56]

29. These are significant requirements, and other experts advocate for even more (such as notice to the individual affected by the request).[57] The TKG, for example, sets up immediate access for the Federal Network Agency without judicial or independent authorisation. Nor does the statute provide for notice to the service providers or the individual concerned. There are certain limited procedural safeguards that govern how *other* agencies handle and store the data once they receive it from the Federal Network Agency, but those only apply after the Federal Network Agency's initial access to

---

[51] *Digital Rights Ireland v Minister for Communications & Ors*, Cases C-293/12 and C-594/12 (8 April 2014), at para. 62. For more on the test of legality, necessity and proportionality, see paras. 39, 54, 55, 52, and 57 to 61; see also *Maximillian Schrems v Data Protection Commissioner*, C-362/14 (6 October 2015), paras. 91-94.

[52] Opinion of Advocate General Saugmandsgaard Øe, Cases C-203/15 and C-698/15 (19 July 2016). Available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=222456. This opinion is not binding, though it is often followed in practice.

[53] *Id.* at para. 7.

[54] *Id.* at para. 263.

[55] *Id.*

[56] *Id.*

[57] See Section 2 *supra* at para. 19.

the data.[58] Moreover, the data is retained pursuant to § 111 para. 4 TKG until "the end of the calendar year following the end of the contractual relationship." But customers frequently extend their contracts with the same provider, which means that this retention period could effectively become indefinite.

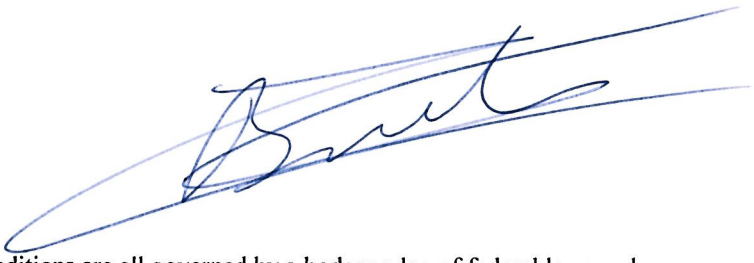
30. Further, there are still serious concerns under the proportionality analysis. As the Advocate General wrote, "it has been consistently held that a measure which interferes with fundamental rights may be regarded as proportionate only if the disadvantages caused are not disproportionate to the aims pursued."[59] "The disadvantages of general data retention obligations arise from the fact that the vast majority of the data retained will relate to persons who will never be connected in any way with serious crime."[60]

31. The blanket retention of identifying information, under laws like the TKG, makes anonymity impossible at a foundational level—individuals know that their identities can be linked to their communications at the government's request. Individuals are therefore less likely to express controversial ideas that challenge the status quo and effect change. These interferences with individuals' privacy and freedom of expression considerably restrict the way that we communicate.[61] Such measures are difficult to justify in a democratic state that is founded on the bedrock of privacy and freedom of expression.

Tomaso Falchetta
Legal Officer
Privacy International
Tel: +44 (0)20 7242 283
tomasof@privacyinternational.org

Gabrielle Guillemin
Senior Legal Officer
ARTICLE 19
Tel: +44 (0)20 7324 2513
gabrielle@article19.org

Cédric Burton
Avocat – Member of the Brussels Bar
Wilson Sonsini Goodrich & Rosati, LLP
Tel: +32 2 274 57 22
cburton@wsgr.com



[58] Which agencies have access and under what conditions are all governed by a hodgepodge of federal laws and ordinances issued by the Federal Ministry of Economic Affairs and Energy, making it all but impossible to predict which agency will access what data when.
[59] *Id.* at para. 247.
[60] *Id.* at para. 252.
[61] See United Nations, Human Rights Council (2014), The right to privacy in the digital age, *supra* note 17, at para. 20 ("Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association. The very existence of a mass surveillance programme thus creates an interference with privacy."); *id.* para. 14 (discussing other rights affected). Incidentally, it is for this reason that the German judgment below is disingenuous when it refers to other registries that show things like car ownership, see German Constitutional Court, 1 BvR 1299/05 (24 January 2012), at para. 138, 152 and 163. Car ownership has little, if anything, to do with speech rights and the ability to express oneself in a democratic society.