Birrer, Alena; He, Danya; Just, Natascha

Conference Paper

The State of State Surveillance in Europe - Findings from a Cross-National Study on Data Retention in 25 Countries

32nd European Conference of the International Telecommunications Society (ITS): "Realising the digital decade in the European Union – Easier said than done?", Madrid, Spain, 19th - 20th June 2023

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Birrer, Alena; He, Danya; Just, Natascha (2023) : The State of State Surveillance in Europe - Findings from a Cross-National Study on Data Retention in 25 Countries, 32nd European Conference of the International Telecommunications Society (ITS): "Realising the digital decade in the European Union – Easier said than done?", Madrid, Spain, 19th - 20th June 2023, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/277946

The State of State Surveillance in Europe – Findings from a Cross-National Study on Data Retention in 25 Countries

Submission to the 32nd European Regional Conference of the International Telecommunications Society, 19th – 20th June 2023, Madrid, Spain

Alena Birrer[1]

Danya He

Natascha Just

Department of Communication and Media Research, Media & Internet Governance Division, University of Zurich, Andreasstrasse 15, 8050 Zurich, Switzerland.

This is a preprint. If you cite this work, please refer to the published version:

Birrer, A., He, D., & Just, N. (2023). The state is watching you—A cross-national comparison of data retention in Europe. *Telecommunications Policy, 47*(4), 1–21. https://doi.org/10.1016/j.telpol.2023.102542

[1] Corresponding author. Department of Communication and Media Research, Media & Internet Governance Division, University of Zurich, Andreasstrasse 15, 8050 Zurich, Switzerland. *E-mail address:* a.birrer@ikmz.uzh.ch

1 Introduction

"We kill people based on metadata"—this statement by the former head of the American National Security Agency (NSA) Michael Hayden captures the potentially severe impacts of communications metadata surveillance. Such data, i.e., information on who communicates with whom, for how long, where, and through which device, have enabled states to identify suspicious patterns in communications (Murray & Fussey, 2019). In recent years, governments have instrumentalized extraordinary events and crises to further expand the mass monitoring of communications metadata, for example during the COVID-19 pandemic (Lyon, 2022) or in the ongoing quest to protect children online (e.g., the European Commission's proposal to require certain online communications service providers to monitor even encrypted private communication, COM(2022) 209 final).

In contrast to traditional forms of state surveillance, the current mass surveillance of communications metadata increasingly takes place without prior suspicion and outsources critical activities to the private sector (Bernal, 2016). A prime example is data retention,[2] which relates to the mandatory storing of communications metadata by providers of electronic communications services and subsequent access to it by public authorities for national-security and criminal-justice purposes (Moser-Knierim, 2014; Whitley & Hosein, 2005). While the English term "data retention" is not clear-cut (Albers & Sarlet, 2022), it is generally applied to mean bulk data retention, which involves the general and indiscriminate retention of communications metadata from all users regardless of prior suspicion (Rojszczak, 2021). The German term "Vorratsdatenspeicherung" hits the bull's eye by pointing to this stockpiling of data in bulk ("auf Vorrat"). Since the early 2000s, European states have gradually established legal frameworks for the retention of communications metadata, which have been heavily disputed. Often prompted by concerns from civil-society organizations, data-retention provisions have been repeatedly struck down by national constitutional courts and the Court of Justice of the European Union (CJEU) for failing to provide sufficient safeguards regarding fundamental rights. To this end and not because of the unconstitutionality of bulk data retention per se, the CJEU repealed the Data Retention Directive (Directive 2006/24/EC, hereinafter "DRD") in 2014, which mandated EU-wide data retention. Since the invalidation of the DRD, the CJEU specified strict conditions regarding data retention and limited its applicability to

[2] Data retention is also relevant in other fields such as airlines, financial institutions, or health (e.g., Bennett, 2005; Kierkegaard, 2011; Milaj & Kaiser, 2017).

cases of demonstrated serious threats to national security. Today, most European countries continue data retention at national level and attempts to resurrect EU-wide data retention are being discussed in the context of the ongoing negotiations for a new ePrivacy Regulation (COM(2017) 010 final), and by the European Commission's "Non-paper on the way forward on data retention" (WK 7294(2021) INIT). In this regard, the CJEU has recently reignited discussions on other forms of data retention, which are intended to mitigate the risks of conventional bulk data retention. However, national implementations of such alternatives practically perpetuate the same problems.

Despite ongoing efforts to expand state surveillance, public and scholarly attention has shifted to corporate surveillance practices by Internet platforms and their data-based business models. Empirical data shows that the public has consistently been more concerned with private companies surveilling their online behavior than with governments (Cole et al., 2012, 2015, 2017–2019). For example, Swiss Internet users' concern about companies controlling their data and violating their privacy ("Big Business") has on average been 14.5 percentage points higher than for governments ("Big Brother") (Latzer et al., 2012, 2013, 2015, 2017, 2019), with a record-high difference of 20 percentage points in 2021 (Latzer et al., 2021b). While this greater concern and awareness regarding corporate data collection does not result in behavior conducive to more privacy self-protection (Büchi et al., 2017)—a phenomenon in line with the "privacy paradox" (Norberg et al., 2007), this lower concern about government surveillance may either result from greater trust in state institutions (despite a general trend of decreasing trust in such institutions (OECD, 2022)) or less knowledge and public awareness about their surveillance practices. For example, user statistics of a German newspaper reveal that articles with "Vorratsdatenspeicherung" in their title consistently attract little readership (Schmidt, 2015), thus indicating that the public does not seem to care about data retention. Similarly, the topic has received short shrift among scholars, notably in the social sciences, and when compared to the vast literature on the perils of data practices of social-media companies (e.g., Mejias & Couldry, 2019; Van Dijck, 2014; Zuboff, 2019). Extant research primarily comes from legal studies, often without consideration of the rich literature on the broader topic of state surveillance. This work often follows a human-rights approach (Latzer & Just, 2020), focusing on individuals' rights to privacy and data protection and rarely considers privacy as a social value (Bennett & Raab, 2003; Büchi et al., 2021; Nissenbaum, 2010; Regan, 1995; Solove, 2015) and the broader societal risks of modern state surveillance.

Against this backdrop, this article argues that the social sciences should not lose sight of modern state surveillance but should direct attention to its wider societal risks by following a

risk-based approach (Baldwin et al., 2012; Black, 2010; Latzer & Just, 2020; OECD, 2010). Current developments within Europe regarding the mass retention of communications metadata underline the need for such attention. This article situates data retention within broader shifts from traditional to modern state surveillance and systematically compares the current policy frameworks for it and attendant policy discussions across Europe based on five major dimensions: (1) *why*, i.e. with what purpose, is data retained; (2) *who* is required to retain data; (3) *what* data is retained and for *how long*; (4) with *what safeguards*; and (5) how is *access* to retained data regulated? Within these five dimensions, special attention is on whether the risks of modern state surveillance, most prominently discriminatory profiling, social sorting, and chilling effects find entry into current data-retention policies and whether the requirements established by the CJEU are considered. A total of 25 European countries were studied to provide a comprehensive and up-to-date overview of data retention in Europe and to uncover similarities and differences among the various countries analyzed (see section 4 for methodological details).

The article first contextualizes data retention within broader shifts from traditional to modern state surveillance and by outlining associated risks (Section 2). Section 3 revisits the history of data retention in Europe as context for current legal frameworks and policy discussions. Section 4 presents results of the comparative analyses on bulk data retention and section 5 discusses recent implementations of other forms of data retention, which are intended to mitigate the risks of the former. The article concludes with key findings, recommendations, and an outlook on future research and developments at EU-level (section 6).

2 Characteristics of modern state surveillance and related risks

The traditional concept of state surveillance has been fundamentally transformed in the digital age, both in terms of how it is conducted and the type of information that is sought (Murray & Fussey, 2019). Generally, state surveillance involves the "monitoring, collecting, and/or processing of personal data by a government" (Eck & Hatz, 2020). Traditional concepts of it refer to a central state, as captured in popular metaphors such as Orwell's (1983) "Big Brother" or Foucault's (1976) interpretation of the "Panopticon". Moreover, it is traditionally bound to a specific suspicion and focuses on communication content (Lyon, 2014). In contrast, modern forms of state surveillance are characterized by a combination of three distinct shifts (Bernal, 2016): (1) from content to communications metadata, (2) from targeted surveillance of specific suspects to mass surveillance of entire populations, and (3) from the state as the panoptic surveillance center to a more pluralized mode of surveillance where key activities are

outsourced to the private sector. These shifts draw attention to several societal risks of state surveillance as explored in the following.

2.1 From content to metadata

Traditionally, state surveillance focused on the content of communication, e.g., by intercepting phone calls or the contents of suspects' letters or e-mails (Human Rights Council of the United Nations, 2016). Meanwhile, the huge volumes of metadata from Internet-based communication are often easier to collect, aggregate, and analyze than content (Bernal, 2016; Landau, 2020). Simply put, "metadata" is contextual data *about* data (Gartner, 2016). In terms of communication, metadata is commonly defined as all information associated with a communication except its substantive content (e.g., Murray & Fussey, 2019; Rojszczak, 2021). Traditionally, this metadata has received less privacy interest than content (Bignami, 2007). Accordingly, governments worldwide justified mass-communications surveillance by arguing they were "just" collecting metadata and not actual content (Memmott, 2013). However, this argument has been widely criticized as communications metadata can reveal extensive insights into a person's behavior, movements, and relationships (Conley, 2015) by leaving distinct digital trails for any given user (Eviette & Simpson, 2021). Communications metadata can also be used to infer highly sensitive personal information such as a person's health status, political affiliation, or sexual orientation, especially when different types of metadata are combined and aggregated (Eviette & Simpson, 2021). Metadata is thus not *less* intrusive, but *differently* intrusive than content (Bernal, 2016). Scholars have demonstrated this revelatory and invasive nature for telephone metadata (e.g., de Montjoye et al., 2013; Mayer et al., 2016) and for internet metadata (e.g., Kapetanios et al., 2021; Landau, 2020). Regarding the latter, consensus is growing that the boundaries between content and metadata are blurred and the distinction is thus outdated (Bellovin et al., 2016; Conley, 2015; Murray & Fussey, 2019; Tokson, 2009). Accordingly, scholars have voiced concerns regarding the potential of profiling—the "systematic and purposeful recording and classification of data related to individuals" (Büchi et al., 2020). More recent technological advances such as data-mining techniques may further exacerbate this risk (Ferguson, 2017). Moreover, the accessibility of communications metadata might incentivize authorities to misuse it for initially unintended purposes (Rucz & Kloosterboer, 2020). For example, communications metadata have been used to monitor compliance with quarantine rules during the COVID-19 pandemic (Privacy International, 2020), which could reinforce normalization of surveillance (Chiusi et al., 2020).

2.2 From targeted to mass surveillance

Throughout the 20th century, most European countries permitted the surveillance of postal and telecommunications traffic by law-enforcement agencies (Sieber & von zur Mühlen, 2016). At the time, communications surveillance was mostly targeted, i.e., directed at specific suspects (Hosein & Palow, 2013; Lyon, 2014). In contrast, modern state surveillance is often applied without distinction or exception and regardless of any previous suspicion, thus operating on a "gather in bulk, access in detail" basis (Bernal, 2016, p. 246). Consequently, data retention moves beyond focusing on specific, previously identified individuals toward broader categories, settings, or patterns of interest (Marx, 2002, 2015). The panoptic concept of surveillance, which first identifies and then monitors the subject, is thus being replaced by the "panspectron", in which "information is gathered about everything, all the time" (Braman, 2009, p. 315). This indiscriminate nature of modern state surveillance thus brings about shifting modes of suspicion (Murray & Fussey, 2019). Moreover, the feeling of being surveilled can result in chilling effects and affect individuals' behavior, autonomy and well-being (Büchi et al., 2022). Accordingly, research found deterring effects of mass surveillance on free speech, e.g., regarding the NSA revelations (Marthews & Tucker, 2017; Penney, 2016; Rainie & Madden, 2015), and shows how mere awareness of data retention may deter people from engaging in private communication (YouGov, 2022). Furthermore, chilling effects regarding online self-expression have slightly increased in recent years (Latzer et al., 2021a).

This shift from targeted to mass surveillance is also symptomatic for a larger "preventive turn" in European security and crime policy (Mitsilegas, 2020; Peeters, 2015) and the increased "culture of control" (Garland, 2001), where suspicious behavior is sought in order to detect and prevent it before it happens (Zedner, 2007). This trend has been considerably afforded by vast technological advances that take effect through a "digital trinity" of socio-technical transformation fueled by processes of algorithmization, platformization, and datafication with significant power shifts regarding access, control, and processing of big data (Latzer, 2022). Apart from data retention, which is often referred to as "preventive" retention (Rojszczak, 2021), other examples include preventive dragnet investigations and the comprehensive use of CCTV and the growing prevalence of predictive policing worldwide (Mugari & Obioha, 2021). Within this shift from targeted to mass surveillance, notions of surveillance as "social sorting" (Gandy, 2021; Lyon, 2002) have become more prevalent, directing attention to the broader societal implications of mass surveillance rather than individual privacy concerns. Modern state surveillance is thus associated with the reshaping of power relations (Harcourt, 2015) and new or intensified forms of exclusion within society (Lyon, 2009), inevitably placing certain

populations under greater suspicion, typically those at the margins of society (Murray & Fussey, 2019). Likewise, people with weaker Internet skills and who attach less importance to privacy are less likely to engage in privacy self-protection (Büchi et al., 2021), making them more vulnerable to communications surveillance.

2.3 From central state actors to privatized state surveillance

While traditional state surveillance was characterized by a central, omnipresent state, the outsourcing of key surveillance tasks to the private sector (McIntyre, 2008) constitutes a third characteristic of modern state surveillance. This shift has been captured in scholarly descriptions e.g., of a "post-panoptic" model of surveillance (Bauman, 2003), which defies central control due to multiplication and diffusion of responsibilities, and "an overlapping and entangled assemblage of government and corporate watchers" (Richards, 2013, p. 1936) transcending the public/private divide. Essentially, key surveillance activities previously under the sole responsibility of the state are increasingly being entrusted to private companies as "surveillance intermediaries" (Hintz, 2014; Rozenshtein, 2018). For example, Amazon partners with US law-enforcement authorities regarding Ring doorbell video footage (Ng, 2022), and investigative authorities worldwide increasingly deploy facial recognition technology from private companies like Clearview AI (Mac et al., 2021). In line with the long-standing literature on the transformation of statehood and shifts from government to governance (e.g., Black, 2001; Latzer, 1999; Ostrom, 1990; Rosenau & Czempiel, 1992; Scott, 2004), the privatization of surveillance (Mitsilegas, 2021; Outlaw III, 2021) thus raises serious accountability and legitimacy questions (e.g., de Londras, 2013; Irion, 2014). The reliance on telecommunications providers for data storage is also associated with inherent risks regarding data security (e.g., Breyer, 2005; Hensel, 2009; Pfitzmann & Köpsell, 2009; Rucz & Kloosterboer, 2020). For example, the European Union Agency for Network and Information Security (ENISA) (2022) documented 168 significant security incidents in the European telecommunications sector in 2021 caused by, among other things, system failures or malicious actions. Recently, hackers have also targeted telecommunications companies worldwide to harvest vast amounts of data (e.g., Harries & Mayer, 2021). Moreover, the transfer of data from private providers to public authorities comes with a risk of data errors (Rucz & Kloosterboer, 2020). The extent of potential consequences became clear in Denmark, where a data-conversion system produced faulty data used as evidence in over 10,000 criminal cases (Henley, 2019). Such issues also become more relevant given that governments and EU institutions increasingly entrust data to (often non-European) cloud providers (European Data Protection Board (EDPB), 2022).

Altogether, the shift from traditional to modern forms of state surveillance and the accompanying risks highlight what is at stake in data retention and what issues should be addressed in regulation. To contextualize the comparative analysis of the current state of data retention, the next section sketches its history and provides an overview of key formative developments at the national and European level.

3 Data retention in Europe—a continuous struggle

The history of data retention in Europe is characterized by a constant back and forth between courts, policymakers, and civil-society organizations, as well as tedious court proceedings and legal reforms. Today, national data-retention laws exist in most European countries. Within the EU, they currently fall under the scope of the ePrivacy Directive (Directive 2002/58/EC), which allows mandatory retention of data for the purposes of safeguarding national or public security and crime investigations (Art. 15(1)). Over the past two decades, data retention has been repeatedly disputed at the national and European level. Often prompted by concerns from human-rights organizations, national constitutional courts and the CJEU have repeatedly struck down data-retention laws. However, the courts did not invalidate data retention per se. Rather, they criticized the specific ways in which national laws were designed from a fundamental-rights perspective. As a result, data retention has never been off the table for good but has repeatedly been on the agenda of policymakers. Accordingly, its history has been compared to a perpetual groundhog day (Hügel, 2021) or a repeated resurrection of the undead (Breyer, 2019; Thierse & Badanjak, 2021). As scholars have already extensively discussed data-retention case law (e.g., Juszczak & Sason, 2021; Mitsilegas et al., 2022; Rojszczak, 2021; Tzanou & Karyda, 2022) and the judicial dialogue across Europe (Zubik et al., 2021), this section only briefly outlines overall developments of data retention in Europe as an important background for understanding its current state. Throughout, special attention is paid to the limits the courts set on data retention, especially regarding the above risks of modern state surveillance.

By the end of the 20th century, some countries were de facto already practicing data retention, e.g., Ireland (McIntyre, 2008)—however, without a legal basis. Legal frameworks for the mandatory retention of communications metadata were then gradually established across Europe since the early 2000s. Among the first countries to introduce it were the Netherlands, the United Kingdom (UK), Ireland and also non-EU countries like Switzerland. A sense of urgency to respond to international terror brought the discussion surrounding data retention to the EU-level (Zubik et al., 2021), resulting in the adoption of the now-invalidated DRD in the

fastest legislative process in EU history up to that date (Alvaro, 2006). The Directive entered into force in 2006 and required all member states to establish mandatory data-retention rules to prevent, investigate, and prosecute serious crime. It constituted a significant paradigm shift in the protection of electronic communications data in Europe, which had previously emphasized the principles of data economy and data minimization (Hoeren, 2012). The adoption of the DRD was therefore highly controversial. The European Data Protection Supervisor (EDPS) (2010) called it the "most privacy invasive instrument ever adopted by the EU" as it placed the entire population under general suspicion. Moreover, the DRD left the parameters for national transposition quite broad, e.g., no definition of key terms such as "serious crime". This lack of specific criteria continues in current national data-retention legislation (see section 4).

Even before all EU member states had transposed the directive, civil-society organizations across Europe began to challenge its implementation. As a result, national constitutional courts abolished data-retention rules, e.g., in Bulgaria (Decision no. 13627 of 11 December 2008), Romania (Decision no. 1258/2009 of 8 October 2009), Germany (Decision of 2 March 2010, BVerfGE 125, 260), and the Czech Republic (Decision of 22 March 2011, Pl. ÚS 24/10). The arguments were largely the same. Data retention was not considered unconstitutional per se, but the specific rules lacked clarity and precision and did not contain sufficient safeguards for the protection of fundamental rights. Some of the courts also highlighted some of the above risks associated with modern state surveillance. For example, the Czech Constitutional Court confirmed that the content-metadata distinction was not appropriate (Decision of 22 March 2011, Pl. ÚS 24/10, para 44). The Romanian Constitutional Court criticized that data retention overturns the presumption of innocence (Decision no. 1258/2009 of 8 October 2009). And the German Federal Constitutional Court highlighted the potential risks of chilling effects, arguing that data retention could evoke a "diffuse, threatening feeling of being watched," detrimental to peoples' fundamental rights (Decision of 2 March 2010, BVerfGE 125, 260, para 212).

These court rulings are of key importance for the longstanding case law of the CJEU regarding data retention (Podkowik et al., 2021). In its landmark judgement of 2014, the CJEU annulled the DRD (joined cases C-293/12 and C-594/12, *Digital Rights Ireland*). Like the national courts, the CJEU did not question data retention in itself but revoked it because of its disproportionate interference with fundamental rights to privacy and data protection and seconded also the objections on the lack of safeguards and objective criteria regarding retention and use of data. Since the invalidation of the DRD, the CJEU specified strict conditions regarding data retention (see e.g., joined cases C-203/15 and C-698/15, *Tele2/Watson*).

Specifically, it held that the number of persons authorized to access retained data must be limited to what is strictly necessary and access must be subject to prior review; data-retention periods must be limited to what is strictly necessary based on objective criteria; and legislation must guarantee a high level of data protection and security, particularly providing for data to be stored within the EU, the destruction of the data at the end of the retention period, and mandatory notification of affected persons after retained data was accessed. This has been interpreted by member states to mean they may well retain data indiscriminately provided that some additional measures regarding access, storage and oversight are in place. More recently however, the CJEU explicitly clarified that bulk data retention for the purpose of fighting (serious) crime and safeguarding public security is unlawful, even if such safeguards are met (C-350/21, Spetsializirana prokuratura, para 60). While the court does allow various other forms of data retention for these purposes (see section 5), it deems bulk data retention only justified in cases of demonstrated genuine serious threats to national security (joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, para 137). As national security is generally within the responsibility of individual member states (Art. 4(2) TEU), governments have attempted to argue that EU law does not apply to data-retention measures in the interest of national security (Mitsilegas et al., 2022). The Court disagrees with this on the grounds that data retention is done by providers of electronic communications services and not directly by public authorities, thus requiring adherence to EU law and CJEU case law on data retention (C-623/17, *Privacy International*; joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*). Notably, this is a contentious issue in the ongoing negotiations on the new ePrivacy regulation. Specifically, the Council of the EU has sought to insert a provision that would effectively overturn this—a prime example of member states' attempts to override CJEU case law unfavorable to them (Rojszczak, 2021). Similarly, the Council has pushed for a provision that would allow bulk data retention for the prosecution of crime (see e.g., Bertuzzi, 2022 for more information on the negotiations between the European Parliament and the Council).

Throughout its judgements, the CJEU repeatedly acknowledged various of the risks of modern state surveillance. It recognized the potential of profiling (joined cases C-293/12 and C-594/12, *Digital Rights Ireland,* para 27) and has started to acknowledge that metadata could be as sensitive as the content of the communication (joined cases C-203/15 and C-698/15, *Tele2/Watson*, para 99). Moreover, the CJEU sharply criticized that data-retention obligations apply to all users without any differentiation, limitation, or exception (joined cases C-293/12 and C-594/12, *Digital Rights Ireland,* para 57), mirroring the concern that modern state

surveillance is not targeted or based on specific suspicion. It further recognized the potential for chilling effects (para 37). More recently, it has also specifically highlighted the need for stronger safeguards where data is subjected to automated processing (joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others*, para 132), which corresponds with the concern that technological innovations exacerbate the risks of data retention. However, the CJEU did not specify the safeguards and reconfirmed that automated analysis of retained data is not per se being challenged (para 176).

Overall, national governments have been reluctant to adapt their legislation to the requirements of the CJEU (see Privacy International, 2017 for a detailed analysis). Some governments and national courts argued that their national regimes were actually compliant with CJEU requirements by interpreting the judgements at their convenience (European Digital Rights (EDRi), 2021), for example in Cyprus (Decision no. 402/2012 of 7 July 2014) or Switzerland (Decision of 9 November 2016, A-4941/2014). Others such as France tried to circumvent CJEU requirements by arguing that national laws were outside of EU competence (Kayali, 2021). Reforms of data-retention laws were mostly forced by national court rulings (see also section 4), instead of being proactively initiated by legislators. In some countries, legal proceedings also led to the abolition of data-retention laws, e.g., in Austria (Decision of 27 June 2014, BGBl I 44/2014), Romania (Decision no. 440/2014 of 8 July 2014), Slovenia (Decision of 3 July 2014, U-I-65/13), Slovakia (Decision of 29 April 2015, Pl. ÚS 10/2014), the Netherlands (Decision of 11 March 2015, ECLI:NL:RBDHA:2015:2498), or more recently in Portugal (Decision no. 268/2022 of 19 April 2022). The national courts followed the CJEU's arguments and also referenced each other, indicative of a sort of federation to shape a common European data-retention standard (Podkowik et al., 2021; Zubik et al., 2021). Notably, both national courts and the CJEU also frequently refer to case law of the European Court of Human Rights (ECHR), highlighting the critical role of human rights in the debate on data retention (Podkowik et al., 2021). As mentioned, some countries have subsequently reintroduced data retention (or tried to), e.g., the Netherlands, while others such as Austria replaced data retention with so-called "data preservation". Here, providers can be required by court order to preserve and give access to certain metadata they already store for other reasons. Such approaches are showcased as correcting alternatives to conventional bulk data retention but essentially perpetuate the same problems (see section 5). Currently, legal or political proceedings regarding data retention are pending in several countries, such as Bulgaria, the Czech Republic, Germany, Italy, the Netherlands, and Switzerland. Thus, after more than 20 years of continuous back and forth, this policy area remains highly debated with no consensus in sight on how to regulate it.

4 A comparison of data retention and attendant policy discussions in Europe

The dynamic history of data retention in Europe makes it difficult to keep up with current rules, especially since the last extensive *comparative* analyses were conducted several years ago (Arnig et al., 2008; Büllingen et al., 2004; European Commission, 2011; Privacy International, 2017). Generally, research has focused on individual countries (e.g., Bug, 2016; Kosta, 2018; McIntyre, 2008; Whitley & Hosein, 2005) or compared just a few (e.g., European Commission, 2020; Riebe et al., 2020). Moreover, research is almost exclusively limited to legal studies and rarely connects with the rich and broad literature on modern state surveillance. This section addresses this gap and provides a comprehensive and up-to-date comparison of the state of data retention in Europe with specific attention to the risks of modern state surveillance. 25 European countries were selected for this analysis, based on national court cases on data retention and knowledge of noteworthy discussions and reforms in recent years. These include all EU member states except for Croatia, Latvia, Lithuania, and Malta, and additionally Switzerland, and the UK due to forerunner status and noteworthy peculiarities in their design of data-retention rules. As of February 2023, 18 of these countries have legislation on bulk data retention (Belgium, Bulgaria[3], Czech Republic, Denmark, Estonia, France, Finland, Germany, Greece, Hungary, Ireland, Italy, Luxembourg, Poland, Spain, Sweden, Switzerland, UK), although Germany is currently refraining from enforcing it[4]. Some have dedicated data-retention laws, while others have integrated such provisions into their telecommunications or data-protection laws. The access to retained data is usually regulated by separate laws (see Appendix A for a list of laws and regulations). The remaining seven countries (Austria, Cyprus, the Netherlands, Portugal, Romania, Slovakia, Slovenia) have all abrogated previous bulk data-retention rules and have therefore not been included in the comparative analysis in this section. Some of these countries (e.g., Austria, Slovakia) have replaced bulk data retention with other forms of data retention, which will be discussed in more detail in section 5.

The policy frameworks for bulk data retention and attendant policy discussions are compared on five dimensions that reflect the key elements of data-retention policy: (1) *why* is data retained; (2) *who* is required to retain data; (3) *what* data is retained and for *how long*; (4)

[3] The CJEU declared Bulgarian data-retention rules unlawful on 17 November 2022 (C-350/21, *Spetsializirana prokuratura*); however, as of February 2023, however, as of February 2023 no amendments have been made.

[4] The German Federal Networks Agency decided to suspend enforcement of data retention in 2017 due to pending court cases on the matter; on 20 September 2022 the CJEU declared German data-retention rules unlawful (joined cases C-793/19 and C-794/19, *SpaceNet and Telekom Deutschland*), however, as of February 2023, no amendments have been made.

with *what safeguards*; and (5) how is *access* to retained data regulated? These dimensions were further specified by deductive codes from three sources: First, some codes were adopted from a previous evaluation of data-retention implementation across the EU (European Commission, 2011) to allow for comparison with prior insights; second, codes were created to reflect the data-retention requirements established by the CJEU; and third, they were deducted from literature on modern state surveillance to capture whether the above risks are considered. These deductive codes were later supplemented by inductive codes that were identified in the material. An overview of the coding scheme is presented in table B1 in the Appendix. For each country, in-depth qualitative content analyses (Puppis, 2019) of publicly available policy and legal documents were conducted, including data-retention laws that were suspended, are in effect or in draft status, documents from policy-reform processes, court decisions, as well as official reports and press releases from relevant authorities. In a parallel iterative and back-and-forth process, the countries were analyzed and compared to each other. To further contextualize and explicate the descriptive findings and to allow for their wider interpretation, this article resorted to additional sources such as scholarly work, national media coverage as well as policy and law blogs.

Overall, the comparative analyses show that there is a heterogeneous patchwork of different national rules across Europe, indicative of the ongoing struggle on the issue. Moreover, the shortcomings of national data-retention provisions highlighted by previous studies (e.g., European Commission, 2011; Privacy International, 2017) have not yet been adequately addressed. To the contrary, the scope of data retention has often been expanded over the years and even though additional safeguards were adopted, these remain vague and fail to mitigate the risks of modern state surveillance.

This section presents selected results of the comparative analysis along the five dimensions. In addition, key shortcomings of the current state of data retention in Europe are identified and recommendations for future reforms discussed.

4.1 Why? The purposes of data retention

The first dimension tackles the purposes of data retention and provides insights into its justifications, especially regarding the CJEU's position that data retention must be necessary and proportionate for its purpose.

The comparative analysis revealed that despite the CJEU's position that bulk data retention is justified only in cases of specific threats to national security, in practice, it is applied

for various other purposes such as criminal justice[5], safeguarding public security[6], and the search and rescue of persons[7]. In addition, some countries[8] establish the purposes of data retention with reference to the duties of the authorities that can access retained data. Overall, the purposes of data retention are usually not defined further, thus leaving considerable leeway for interpretation and resembling more of a "catch-all category justifying bulk-powers" (Murray & Fussey, 2019, p. 57). This raises the question of whether such purpose limitations have more of a symbolic function than actually limiting data retention (see e.g., Hansjakob, 2018). As regards safeguarding national security, most countries do not require the establishment of specific threats, which again disregards a key CJEU requirement. Only four countries[9] have restricted bulk data retention to particular time periods when specific threats to national security exist—a reaction to court rulings on their national data-retention regimes. However, in practice, they have resorted to general threat assessments and broad statistical information instead of ascertained intelligence about specific threats (Lund, 2022). This has allowed them to repeatedly prolong bulk data-retention orders.

To justify restrictions of fundamental rights, the CJEU further requires that data retention be necessary and proportional to achieve its purpose and these conditions must be based on objective and verifiable criteria. However, only a few countries[10] explicitly require a connection between the data-retention measure and the specified purpose. Moreover, these do not specify what criteria should be used to establish these connections. This lack of clear purpose limitation is a major shortcoming of data-retention provisions, which was criticized by the EU Commission (2011) already over a decade ago. Future reforms should thus make genuine efforts to clarify the meaning of serious threats to national security and introduce independent oversight mechanisms to verify whether the specific threats justify the data-retention measure. Given the overall need for adaptive governance in complex systems, *adaptive approaches* to governance need to be strengthened by including, among other things, feedback mechanisms in the governance process such as periodic reviews and revisions (Latzer, 2013).

---

[5] BG, CH, CZ, DE, EE, ES, FI, GR, IT, LU, PL, SE, UK,

[6] CH, LU, UK

[7] BG, CH, CZ, PL

[8] HU, PL

[9] BE, DK, FR, IE and currently discussed in LU

[10] CH, DE, EE, SE, UK

4.2 Who? Providers required to retain data

The second dimension compares which providers are required to retain metadata about their users. Special attention is paid to whether the question of entrusting private companies with state surveillance activities is addressed in policy-making processes and whether they should be compensated for the costs of data retention.

Generally, providers of electronic communications services and in most countries[11] network operators are required to retain data. However, data-retention laws use different terms to describe such providers and define them with varying levels of detail. Notably, some countries specifically exempt certain providers from mandatory data retention, for example broadcasters (e.g., in the UK), or companies that provide services of negligible importance as determined by their market share and geographic coverage (e.g., in Finland). In Sweden, providers may be exempted for "exceptional reasons", which, however, are not further defined. In other countries such as Switzerland, additional providers such as postal companies are subjected to mandatory data retention. Moreover, there are discussions across Europe whether Over-the-Top providers (OTTs) should have data-retention obligations. For example, in the UK, they have been required to do so since 2016 (Home Office, 2018) and the Swiss government is currently considering codifying data-retention obligations for them (Bundesrat, 2022) after courts had previously stopped such attempts (Decision of 19 May 2020, A-550/2019; Decision of 13 October 2021, A-5373/2020; Decision of 29 April 2021, 2C_544/2020). Some countries introduced mandatory retention of metadata by OTTs outside the scope of their data-retention laws. Hungary, for example, added new rules to its E-Commerce Act in 2016, which require OTTs to retain certain metadata for one year. A similar mechanism was introduced in France in 2021 and is being discussed in Poland. Of great importance here is the European Electronic Communications Code (Directive (EU) 2018/1972, EECC) that introduced a new definition of electronic communications services that include "number-independent interpersonal communication services" such as messaging services. The proposal for the new ePrivacy regulation (COM(2017) 010 final) follows this change in definition and would thus enable EU states to extend the scope of data-retention obligations to OTTs. These developments should be critically discussed in the ongoing negotiations on the ePrivacy regulation because such extensions may allow for an even more extensive mass

[11] BE, BG, CH, CZ, FR, GR, HU, IT, LU, PL, SE, UK

surveillance of communications metadata and thus further exacerbate the risks associated with modern state surveillance.

The analysis further revealed that the issue of entrusting private companies with public surveillance tasks and related questions regarding accountability, legitimacy, data security, and data misuse were generally not touched upon. An exception is Switzerland, where the Federal Council previously acknowledged potential problems of outsourcing sensitive surveillance tasks to the private sector (Hansjakob, 2002). However, this has not stopped them from later introducing mandatory data retention. Another issue is the question of whether private companies should be compensated for the costs they incur. The EU Commission (2011) recommended this to prevent distortions of competition and the passing on of costs to consumers. However, only a minority of countries currently reimburse providers for (some of) the costs related to data retention[12]. In Germany, the constitutional court even argued that the state can impose obligations to safeguard public interests as well as related costs on private companies if they fall within their field of activity and responsibility ("Sach- und Verantwortungsnähe", Decision of 2 March 2010, BVerfGE 125, 260, paras 301-302). Despite this ruling, the currently suspended German data-retention rules include the possibility of cost compensation in cases of hardship. In Sweden, the reimbursement of costs was repealed in 2022 and remains a topic of discussion.

4.3 What and for how long? Data categories and retention periods

The third dimension considers what data is retained and for how long. The analysis focuses specifically on whether the much-criticized content-metadata distinction is being acknowledged and how. In addition, and following the CJEU's requirement that retention periods must be limited to what is strictly necessary, it looks into the explanations for the chosen retention periods.

While rules are quite similar across countries regarding the types of retained data, they differ in the provided detail of what exact data is to be retained. Overall, the types of retained data can be classified into four categories (see also European Commission, 2020): (1) subscriber data, which refers to information used for identifying the sender of a communication such as (user)names, addresses or phone numbers; (2) identification data,[13] which identify the

[12] CZ, (DE), FI, (FR), UK

[13] Some countries categorize this type of data as part of subscriber data or traffic data.

equipment used for a communication, including device identification numbers or IP addresses; (3) traffic data, i.e., information on the date, time, duration and type of a communication, as well as its recipient(s); and (4) location data, referring to information on the location of communication equipment such as cell tower. These categories apply to fixed, mobile and Internet telephony (often including unsuccessful call attempts[14]), SMS, e-mail, and Internet access.

As discussed in section 2, scholars have sharply criticized the common distinction between content and metadata and the unequal treatment thereof when it comes to data protection and privacy. Notably, the analysis shows no acknowledgement of this blurring of boundaries between content and metadata. Instead, many data-retention laws often explicitly highlight that the content of a communication is not affected.[15] In the light of technological advances, policymakers may need to reconsider this distinction, because the relevant question is not *what* data is gathered and whether this data is personal, but *how* the data may be used (Bernal, 2016; Solove, 2023).

In contrast to data categories, retention periods vary significantly across countries. Eleven countries apply a single uniform retention period to all categories of data ranging from six months[16] to one year[17], while others apply different retention periods for different categories of data[18] and/or different purposes of data retention.[19] Several countries have extended their retention periods over the years, most outstanding Italy, which now effectively has a retention period of six years (Maggiore, 2017). In some cases, data-retention legislation itself allows for periodical extensions[20], for example considering the interest of national security, which again leaves considerable room for interpretation. In contrast, only a few countries have shortened retention periods. Germany for example has limited data retention to 4 to 10 weeks (depending on the type of data), attempting to comply with CJEU case law (Deutscher Bundestag, 2015). However, the CJEU has recently clarified that this limited retention period did not make

[14] CZ, DE, DK, ES, FI, PL, SE

[15] BG, CZ, DE, EE, ES, FI, GR

[16] BG, CH, CZ, LU

[17] DK, EE, ES, GR, IE, PL, UK

[18] BE, DE, FI, FR, HU, SE, IT

[19] IT

[20] BE, EE, ES, DK, FR

Germany's data-retention rules less intrusive (joined cases C-793/19 and C-794/19, *SpaceNet and Telekom Deutschland,* para 88).

More importantly, the CJEU requires that retention periods are limited to what is strictly necessary to achieve the purpose. However, as national legislators rarely give reasons for setting a certain retention period (other than referencing the former DRD), retention periods currently do not appear to draw on necessity considerations but are rather set arbitrarily—an issue that needs clarification and justification in future reforms.

4.4 With what safeguards? Data security and data protection

The fourth dimension considers the safeguards in place for data security and data protection. As data retention is inherently sensitive to security breaches and misuse, the CJEU repeatedly ruled that national data-retention rules must have certain minimum standards for this. The analysis also focuses on whether broader societal implications of data retention such as social sorting or chilling effects are taken into account.

In line with the former DRD and the General Data Protection Regulation (Regulation 2016/679, GDPR), all countries have introduced some or all of the following principles related to data security and data protection: (1) providers must ensure the quality and security of data[21]; (2) data retention must be subject to appropriate technical and organizational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, and unauthorized or unlawful storage, processing, access or disclosure[22]; (3) only authorized personnel should be able to access retained data[23]; and (4) retained data must be destroyed at the end of the retention period, except for that retrieved[24]. Other safeguards such as territorial restrictions to data storage have only been adopted in a few countries[25], despite the CJEU's requirement for data to be stored within the EU to guarantee certain levels of protection. Similarly, data-retention laws rarely explicitly provide for notification obligations and user access rights[26] required by the GDPR. Thus, although data-protection and data-security

[21] BE, BG, CH, CZ, DK, EE, ES, FI, FR, GR, HU, IE, LU, PL, SE, UK

[22] BE, BG, CH, CZ, ES, DE, DK, EE, FI, FR, GR, HU, IE, LU, IT, PL, SE, UK

[23] BE, BG, CH, CZ, DE, DK, EE, ES, FI, FR, GR, HU, IE, IT, LU, PL, SE, UK

[24] BE, BG, CH, CZ, DE, DK, FI, FR, GR, HU, IE, IT, LU, PL, SE, UK

[25] DE, EE, GR, HU, SE

[26] only CZ, HU, IT mention this explicitly; others implicitly refer to national or European data protection laws

considerations generally seem on the rise with some countries having introduced additional safeguards over the years[27], data retention is still not subject to the same level of user protection as corporate surveillance practices. Moreover, data-retention laws lack details on how existing safeguards should be implemented. In this context, the ECHR has recently ruled that the mere existence of safeguards was not sufficient and that governments should provide proof of their practical effectiveness (application 70078/12, *Ekimdzhiev and Others v. Bulgaria*). Besides, although most countries have appointed authorities to supervise the principles' application (e.g., the national data-protection authority), sanctioning mechanisms for non-compliance with data security and data protection as well as legal remedies for affected users rarely exist[28]. Overall, it remains open whether the extant safeguards can effectively guarantee data protection and security. Future reforms of data-retention rules should thus focus on clear safeguards, effective sanctioning and oversight mechanisms as well as improved levels of user protection.

Furthermore, from a social-science perspective, discussions of data retention should extend beyond individual privacy and data-protection considerations and take into account its broader societal implications. Specifically, data retention is associated with the potential of chilling effects, social sorting and new or intensified forms of exclusion within society (see section 2). However, the analysis shows that these societal privacy considerations are rarely discussed and not addressed by legal safeguards. One key issue that should receive particular attention is profiling and automated decision-making and how discriminatory effects can be prevented. While the complexity of addressing this issue has been part of a broader ongoing debate, recommendations that have been developed, e.g., in the context of the GDPR, could provide a good starting point, including regular quality assurance checks and algorithmic auditing (Article 29 Data Protection Working Party, 2018).

4.5 How is access to retained data regulated?

The fifth dimension focuses on who has access to retained data and under what conditions. The analysis particularly focuses on whether effective oversight mechanisms mitigate the commonly voiced concern over misuse of data.

Overall, the range of authorities with access to retained data, so-called "competent authorities", has been expanded drastically over the years and differs considerably across

[27] BE, BG, CZ, DE, IT, SE

[28] except for CZ, DE, ES, GR, HU, LU

countries. Usually, police and law enforcement authorities[29] as well as security and intelligence services[30] can request access to retained data. Other competent authorities include judicial authorities such as prosecutors or courts[31]; security forces and military institutions[32]; fiscal and tax authorities[33]; custom and border control authorities[34]; anti-corruption authorities[35]; competition and consumer-protection authorities[36]; and environmental organizations[37]. Furthermore, the COVID-19 outbreak has triggered further expansion, allowing government authorities to access location data to monitor compliance with quarantine and social-distancing rules[38]. Despite the often temporary nature of this extension, irreversible effects are feared (Bozhinova, 2020). Notably, the analysis also revealed that authorities sometimes access retained data without legal basis. In Switzerland, for instance, lost-and-found offices could access certain metadata to identify owners of lost mobile phones (Grossenbacher, 2017). In France, legislation does not specify the competent authorities altogether, leaving considerable leeway for potential misuse. Overall, this seems to confirm the lack of clear safeguards regarding data protection discussed under the previous dimension.

Apart from the range of competent authorities, countries also vary regarding the procedures and oversight mechanisms relating to access. Apart from Poland and the Czech Republic, all countries require prior authorization of access as set out by the CJEU, although different authorities can authorize access. Meanwhile, some countries[39] grant exceptions, whereby providers must give immediate access to retained data in case of emergency. As the conditions for granting such direct access are often unspecified, this again leaves considerable leeway especially during crises and calls into question whether existing oversight mechanisms

[29] BG, CH, CZ, DE, EE, ES, FI, GR, HU, IT, LU, PL, SE, UK

[30] BE, BG, CH, CZ, DE, DK, EE, ES, HU, LU, PL, SE, UK

[31] CZ, EE, GR, HU, IT, LU

[32] BG, CZ, EE, FI, GR, PL, UK

[33] CZ, EE, HU, PL

[34] EE, ES, FI, PL, SE, UK

[35] BG, PL

[36] EE

[37] EE

[38] codified in BG, PL

[39] BG, EE, IE, IT, UK

are sufficient. Besides establishing coherent oversight mechanisms regarding the access to retained data, the broader everyday practices of competent authorities related to data access and use could be subjected to independent oversight and information on it be made publicly available (Murray & Fussey, 2019).

Altogether, the comparative analyses reveal a mixed picture: Although additional safeguards regarding retention of and access to data have been introduced over the years, the vagueness of these rules raises the question of how effective they will be. Moreover, data retention rules are still rarely based on clear indication of necessity and proportionality, thus ignoring one of the core CJEU requirements. Concurrently, national legislators have continuously extended the scope of their data-retention regimes concerning the providers required to retain data, retention periods and competent authorities. In addition, policy discussions often focus on individuals' rights to privacy and data protection while data retention's broader societal privacy implications are widely neglected. Overall, data-retention laws thus currently fail to adequately account for the long-standing CJEU case law on this issue and the broader social risks associated with modern state surveillance.

Given the extensive problems with bulk data retention, it is important to consider what alternative measures exist. In this regard, the comparative analyses indicate renewed discussions surrounding other forms of data retention, which are explored in section 5.

5 Toward other forms of data retention: a wolf in sheep's clothing?

The CJEU has recently reignited discussions surrounding other forms of data retention, which are showcased as correcting alternatives to conventional bulk data retention. In its latest judgements, it elaborated on four such forms (see especially joined cases C-511/18, C-512/18 and C-520/18, *La Quadrature du Net and Others)*: (1) the retention of subscriber data and (2) of IP addresses; (3) preventive "targeted data retention", which limits data retention to certain persons or areas; and (4) expedited data retention, which corresponds to the previously mentioned data preservation, whereby providers can be required to preserve and grant access to stored data. According to the CJEU, these other forms of data retention are more compatible with EU law as they either limit the scope of retained data categories, target specific persons or areas, or forego indiscriminate bulk-retention mechanisms altogether. While some of these approaches have previously been discussed or even adopted in some countries, the CJEU judgments, arguably assuming a "quasi-legislative" role (Tzanou & Karyda, 2022), evoked recent reforms in Belgium, Denmark, France and Ireland. These countries limited conventional data retention to national security purposes (see section 4) and additionally introduced some or

all of the other four data-retention approaches for purposes related to fighting (serious) crime and safeguarding public safety, creating what was coined "a new generation of data retention laws" (Breyer et al., 2022). A similar reform proposal is also being discussed in Luxembourg. Referencing the CJEU, the European Commission (2021) is currently exploring whether and which of these other forms of data retention could provide ways forward with data retention at EU level. Against this backdrop, this section explores the extent to which they provide adequate "alternatives" to conventional bulk data retention in light of the risks associated with modern state surveillance.

5.1 Retention of subscriber data and IP addresses

The first two alternatives suggested by the CJEU are distinct from conventional bulk data retention as they are limited to data categories that are deemed least sensitive and/or indispensable for certain purposes, namely subscriber data ("data relating to the civil identity of users") and IP addresses. For the retention of subscriber data, which includes e.g., (user-)names and addresses, the CJEU even foregoes requirements regarding limits of retention periods or prior judicial review. Regarding IP-address retention, the CJEU acknowledges its potential for profiling but as it may often be the only means to identify perpetrators of criminal offences online—specifically in the fight against sexual abuse of children online—the end justifies the means. Retention of both subscriber data and IP addresses is already in place in most countries as part of conventional bulk data-retention provisions (see section 4). In addition, countries that have limited conventional bulk data retention to national-security purposes (Belgium, Denmark, France, Ireland), have introduced them as complementary measures in the area of criminal procedure. Notably, Denmark "conveniently" interpreted IP addresses as part of subscriber data, which allowed it to effectively circumvent the stricter conditions for IP-address retention of the CJEU (Lund, 2022). In Germany, where the CJEU has ruled that the current data-retention regime is unlawful (see section 4), a proposal to replace it with IP-address retention found no support (Deutscher Bundestag, 2022).

Overall, it seems questionable whether the retention of subscriber data and IP addresses provides an adequate alternative to conventional bulk data retention. First, the assumption that IP addresses could be seen as less sensitive is arguably faulty, especially in light of newer research on the tracking capabilities of the most recent IPv6 standard (e.g., Saidi et al., 2022). Moreover, as noted earlier, classifying data as more or less sensitive may be less reasonable than focusing on how they can be used (Solove, 2023). Another key shortcoming of these two alternatives is that they still operate on a bulk basis, i.e., they apply to every user and in the

absence of prior suspicion. Therefore, they continue to perpetuate one of the key concerns related to modern state surveillance, namely the presumption of innocence.

5.2 Targeted data retention

Targeted data retention, which was already declared lawful by the CJEU in 2016, remedies the indiscriminate nature of conventional bulk data retention by limiting it to certain people (person-based retention) or areas (geographic-based retention). At the same time, it is still a preventive measure, making it distinct from other targeted surveillance that applies only upon concrete suspicion. As regards specific implementation, the CJEU requires targeting to be based on "objective and non-discriminatory criteria", without defining these further (*La Quadrature du Net and Others*, joined cases C-511/18, C-512/18 and C-520/18, para 150). Person-based and/or geographic-based retention for up to 12 months was introduced in Belgium, Denmark, and Ireland. The specific criteria are similar across countries: geographic-based retention concerns areas with certain crime rates as well as critical infrastructures and areas more likely to be exposed to threats to public security, including highways, airports, or buildings of (inter)national institutions. Person-based retention comprises previously convicted serious criminal offenders.

However, this seemingly targeted data retention will effectively apply indiscriminately to the whole population (Breyer, 2022; Lund, 2022), essentially undermining its purpose. For example, the Belgian legislator has explicitly described its new data-retention rules as "targeted in its approach but generalized in its consequences" (Chambre des représentants, 2022, p. 12). Moreover, in contrast to other forms of targeted surveillance that apply only upon concrete suspicion, targeted data retention is still a preventive measure. Therefore, it is still associated with certain risks of modern state surveillance. For example, both the targeting of specific geographical areas and of specific persons have been criticized for potentially reinforcing existing discrimination, as they may disproportionally affect the poorer, working class, and people of color (Berthélémy, 2021). On a more practical level, it could also prove difficult to technically implement such targeted retention (Kelly, 2022). Accordingly, the third option presented by the CJEU appears a similarly inadequate alternative to conventional bulk data retention.

5.3 Expedited data retention (quick freeze)

The fourth option, expedited data retention, refers to a mechanism in which providers are required by court order to preserve and disclose certain metadata they are storing for commercial reasons. Essentially, data has to be "frozen" for a short period of time before the

provider routinely deletes it, thus the common name "quick freeze". Contrary to conventional bulk data retention, data preservation only comes into play upon a criminal suspicion, i.e., it always relates to particular persons for specific reasons. It is therefore considered a more privacy-friendly measure and has received increased attention over the past years. Expedited data retention practically corresponds to data preservation, which was adopted in many European countries throughout the early 2000s given that the Convention of Cybercrime of the Council of Europe ("Budapest Convention") required it (Centre for Strategy & Evaluations Services, 2012). While data preservation was traditionally conceived of as a complementary measure to bulk data retention, discussions later intensified about whether it could replace it altogether, as happened for example in Austria and Slovakia, and is currently proposed in Germany (Dachwitz & Meister, 2022).

As regards the adequacy of expedited data retention as an alternative to conventional bulk data retention, it must be noted that in practice, risks of discriminatory profiling, social sorting, and chilling effects may not be mitigated entirely, because investigatory authorities will often be able to access the same data (Matter, 2019). Moreover, what constitutes a justified suspicion and whether it is proportional to the measure remains unclear, as long as laws do not require clear necessity and proportionality conditions, alongside questions regarding data protection and data security (see section 4).

To summarize, the four "alternative" forms of data retention must be seen as variations of conventional bulk data retention that appear inadequate to reduce all of the risks of modern state surveillance, especially when combined to form even more encompassing surveillance systems. Given their approval by the CJEU, they will also likely be harder to challenge than conventional bulk data retention, thus giving states even more leeway regarding communications surveillance. This is not to say that alternative forms of data retention should not be explored in the future; they should however be subjected to the same level of scrutiny as conventional bulk data retention, especially since there is also a lack of empirical evidence on their workings and effectiveness.

6 Conclusion

This article has analyzed data retention as a prime example of shifts from traditional to modern state surveillance. Data retention focuses on communications metadata instead of content, is designed to cover whole populations and not specific targets of interest and outsources critical surveillance tasks to the private sector. Accordingly, data retention is associated with many risks, including discriminatory profiling, social sorting, or chilling effects. The comparative

analysis has revealed that after two decades of heated debate, national data-retention provisions across Europe still fail to adequately take these risks into account. Specifically, they do not provide effective safeguards regarding data security and data protection as well as precise criteria for the necessity and proportionality of data retention. Moreover, they lack effective sanctioning and oversight mechanisms and continue to reinforce the much-debated content-metadata distinction. Data retention is also still not subject to the same level of user protection as corporate surveillance practices, with user access rights and notification obligations largely missing. At the same time, legal frameworks as well as attendant policy discussions do not account for data retentions' broader societal privacy implications. While some of these shortcomings could in theory be easily addressed by reforms of national data-retention laws, various circumstances indicate that this will be difficult to realize in practice. Governments have generally been reluctant to bring their data-retention regimes in line with CJEU requirements, and they have continuously found loopholes to escape obligations. Their positions on the reforms currently underway also suggest that they are hardly willing to deviate from this. While harmonization of rules, for example by the instrument of European regulation, may provide partial remedies, this may be compromised partly by the observable trend in policymaking of principles-based regulation (Baldwin et al., 2012; Black, 2007), which has been characteristic of recent European reforms. Principles-based regulation refrains from detailed prescriptive rules and instead relies on broadly stated principles such as accountability, transparency, fairness, liability or justification, which are definable and adaptable during policy implementation (Latzer & Just, 2020). While this aligns well with the here-advocated adaptive policy approach (Latzer, 2013), it is important to ensure that appropriate arrangements are in place to make it work, including periodic reviews, audits, or independent oversight. In this policy area specifically, additional reliance on risk-based approaches may be fruitful (Baldwin et al., 2012; Black, 2010). These focus on the control of risks associated with data retention from a public-interest perspective and include systematic risk identification and assessments as well as appraisals of the appropriate mode of governance (e.g., regarding the outsourcing of critical activities to the private sector) (Latzer et al., 2019). In addition, giving access to the mechanisms of collection and use of data to independent researchers may help shed light on the workings of data retention, its effectiveness, and associate risks.

In addition to the shortcomings of national data-retention legislation, the scope of data retention has seen continuous expansion, justified e.g., by the fight against the COVID-19 pandemic. This illustrates the importance to question governments' efforts to expand surveillance during crises. Finally, the analyses indicate that the supposed "alternatives" to bulk

data retention (i.e., subscriber data and IP-address retention, targeted data retention and expedited data retention) further perpetuate the risks of modern state surveillance and thus do not provide satisfying solutions, especially when implemented as complementary instead of mutually exclusive measures. Overall, the shortcomings identified are also reflected in other recent developments of communications surveillance at EU level. For example, the European Commission's proposal to oblige certain online communications service providers to monitor all private chats and e-mails for suspicious content (COM(2022) 209 final) has been criticized for its lack of clarity of circumstances under which communication is monitored and its lack of necessity and proportionality standards (European Data Protection Board & European Data Protection Supervisor, 2022; Meineck & Reuter, 2022). Other contentious proposals are the eEvidence regulation (COM(2018) 225 final) and the reform of the Europol Regulation (Regulation 2022/991). The types of legal acts chosen for these proposals, i.e., regulations, point towards the intent to harmonize surveillance measures across Europe.

While this study has provided comprehensive insights into the current state of data-retention in Europe, legal provisions alone never tell the whole story. More research is needed on how data retention actually works "on the ground" (Bamberger & Mulligan, 2015). This calls for more empirical evidence into the workings, effectiveness, and risks of bulk and other forms of data retention, which will be key for living up to the broader societal implications of modern state surveillance and may provide the basis for more precise criteria for data retention.

Acknowledgements

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Appendix A. Laws and regulations per country

Belgium

Code d'instruction criminelle [Code of Criminal Procedure]. https://www.ejustice.just.fgov.be/cgi_loi/change_lg_2.pl?language=nl&nm=1808111701&la=N

Loi du 30 novembre 1998 organique des services de renseignement et de sécurité [Law on the Intelligence and Security Services]. https://www.ejustice.just.fgov.be/doc/rech_f.htm

Loi relative à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités [Data Retention Law]. https://www.ejustice.just.fgov.be/doc/rech_f.htm

Loi relative aux communications électroniques [Electronic Communications Act]. https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&table_name=wet&cn=2005061332

Bulgaria

ЗАКОН ЗА ЕЛЕКТРОННИТЕ СЪОБЩЕНИЯ [Electronic Communications Act]. https://lex.bg/laws/ldoc/2135553187

НАКАЗАТЕЛНО-ПРОЦЕСУАЛЕН КОДЕКС [Code of Criminal Procedure]. https://lex.bg/laws/ldoc/2135512224

Czech Republic

Zákon o elektronických komunikacích [Electronic Communications Act]. https://www.zakonyprolidi.cz/cs/2005-127

Zákon o trestním řízení soudním [Code of Criminal Procedure]. https://www.zakonyprolidi.cz/cs/1961-141

Denmark

Bekendtgørelse af lov om elektroniske kommunikationsnet og -tjenester [Act on Electronic Communications Networks and Services]. https://www.retsinformation.dk/eli/lta/2014/128

Bekendtgørelse af lov om rettens pleje [Administration of Justice Act]. https://www.retsinformation.dk/eli/lta/2021/1835

Bekendtgørelse om generel og udifferentieret registrering til og med den 29. Marts 2023 og opbevaring til og med den 29. Marts 2024 af trafikdata [Data Retention Order 2023-2024], BEK nr 381 af 29/03/2022 (2022). https://www.retsinformation.dk/eli/lta/2022/381

Lov nr 291 om ændring af retsplejeloven og lov om elektroniske kommunikationsnet og -tjenester [Act amending the Administration of Justice Act and the Act on Electronic Communications Networks and Services], (2022). https://www.retsinformation.dk/eli/lta/2022/291

Estonia

Elektroonilise side seadus [Electronic Communications Act]. https://www.riigiteataja.ee/akt/ESS

Isikuandmete kaitse seadus [Personal Data Protection Act]. https://www.riigiteataja.ee/akt/104012019011

Julgeolekuasutuste seadus [Security Authorities Act]. https://www.riigiteataja.ee/akt/JAS

Kaitseväe korralduse seadus [Estonian Defence Forces Organisation Act]. https://www.riigiteataja.ee/akt/KKS

Kriminaalmenetluse seadustik [Code of Criminal Procedure]. https://www.riigiteataja.ee/akt/106012016019?leiaKehtiv

Politsei ja piirivalve seadus [Police and Border Guard Act]. https://www.riigiteataja.ee/akt/127052022028

Väärteomenetluse seadustik [Code of Misdemeanour Procedure]. https://www.riigiteataja.ee/akt/VTMS

Finland

Laki sähköisen viestinnän palveluista (917/2014) [Act on Electronic Communications Services]. https://www.finlex.fi/fi/laki/ajantasa/2014/20140917

Määräys teletoiminnan tietoturvasta (Viestintävirasto 67 A/2015 M) [Regulation on Information Security in Telecommunications Operations]. https://www.finlex.fi/data/normit/44046/M67A_2015.pdf

Määräys teleyritysten tietojen säilytysvelvollisuudesta viranomaistarpeita varten (Viestintävirasto 53B/2014 M) [Data Retention Regulation]. https://www.finlex.fi/fi/viranomaiset/normi/480001/32675

Pakkokeinolaki (806/2011) [Coercive Measures Act]. https://www.finlex.fi/fi/laki/ajantasa/2011/20110806

Poliisilaki (493/1995) [Police Act]. https://finlex.fi/fi/laki/ajantasa/kumotut/1995/19950493

Rajavartiolaki (578/2005) [Border Guard Act]. https://www.finlex.fi/fi/laki/ajantasa/2005/20050578

Tullilaki (1466/1994) [Customs Act]. https://finlex.fi/fi/laki/ajantasa/kumotut/1994/19941466

France

Code de la défense [Code of Defence]. https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071307

Code de la sécurité intérieure [Code of Interior Security]. https://www.legifrance.gouv.fr/codes/id/LEGITEXT000025503132

Code de procédure pénale [Code of Criminal Procedure]. https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/2023-02-02/

Code des postes et des communications électroniques [Postal and Electronic Communications Code]. https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006070987/

Décret n° 2021-1361 du 20 octobre 2021 relatif aux catégories de données conservées par les opérateurs de communications électroniques, pris en application de l'article L. 34-1 du code des postes et des communications électroniques [Decree on the Categories of

Retained Data]. https://www.legifrance.gouv.fr/loda/id/JORFTEXT000044228877/2023-02-02/

Décret n° 2021-1363 du 20 octobre 2021 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion General Data Retention Order 2021-2022]. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044228976

Décret n° 2022-1327 du 17 octobre 2022 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion [General Data Retention Order 2022-2023]. https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000046437495

Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Data Protection Act]. https://www.legifrance.gouv.fr/loda/id/LEGISCTA000006095896/2023-02-02/

Germany

Gesetz für Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten [Data Retention Law]. https://www.degruyter.com/document/doi/10.1515/9783110274905-024/html

Strafgesetzbuch [Criminal Code]. https://www.gesetze-im-internet.de/stgb/

Strafprozessordnung [Code of Criminal Procedure]. https://www.gesetze-im-internet.de/stpo/

Telekommunikationsgesetz [Telecommunications Act]. https://www.gesetze-im-internet.de/tkg_2021/

Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation [Regulation on the technical and organisational implementation of telecommunications surveillance measures]. https://www.gesetze-im-internet.de/tk_v_2005/BJNR313600005.html

Greece

ΝΟΜΟΣ ΥΠ' ΑΡΙΘ. 3917 Διατήρηση δεδομένων που παράγονται ή υποβάλλο− νται σε επεξεργασία σε συνάρτηση με την παροχή διαθέσιμων στο κοινό υπηρεσιών ηλεκτρονικών επι− κοινωνιών ή δημόσιων δικτύων επικοινωνιών, χρήση συστημάτων επιτήρησης με τη λήψη ή καταγραφή ήχου ή εικόνας σε δημόσιους χώρους και συναφείς διατάξεις [Data Retention Law]. https://www.kodiko.gr/nomothesia/document/128144/nomos-3917-2011

ΝΟΜΟΣ ΥΠ'ΑΡΙΘ. 2225 ΦΕΚ 121/20.07.1994 Για την προστασία της ελευθερίας και ανταπόκρισης και επικοινωνίας και άλλες διατάξεις [Law on the Confidentiality of communications]. https://www.kodiko.gr/nomothesia/document/218950/nomos-2225-1994

ΝΟΜΟΣ ΥΠ' ΑΡΙΘΜ. 4624 Τεύχος Α' 137/29.08.2019 Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις. [Data Protection Law]. https://www.kodiko.gr/nomothesia/document/552084/nomos-4624-2019

Hungary

1994. Évi XXXIV. törvény a Rendőrségről [Police Act]. https://net.jogtar.hu/jogszabaly?docid=99400034.tv

1995. Évi CXXV. törvény a nemzetbiztonsági szolgálatokról [Act on the National Security Services]. https://net.jogtar.hu/jogszabaly?docid=99500125.tv

2003. Évi C. törvény az elektronikus hírközlésről [Act on Electronic Communications]. https://net.jogtar.hu/jogszabaly?docid=A0300100.TV

2010. Évi CXXII. törvény a Nemzeti Adó- és Vámhivatalról [Act on the National Tax and Customs Office]. https://net.jogtar.hu/jogszabaly?docid=a1000122.tv

2011. Évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról—Hatályos Jogszabályok Gyűjteménye [Data Protection Act]. https://net.jogtar.hu/jogszabaly?docid=a1100112.tv

2001. Évi CVIII. törvény az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről [Act on Electronic Commerce and on Information Society Services]. https://net.jogtar.hu/jogszabaly?docid=a0100108.tv

2017. Évi XC. törvény a büntetőeljárásról [Act on Criminal Proceedings]. https://net.jogtar.hu/jogszabaly?docid=a1700090.tv

Ireland

Communications (Retention of Data) Act 2011. https://www.irishstatutebook.ie/eli/2011/act/3/enacted/en/html

Communications (Retention of Data) (Amendment) Act 2022. https://data.oireachtas.ie/ie/oireachtas/act/2022/25/eng/enacted/a2522.pdf

Data Protection Act 2018. https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

Italy

Decreto del Presidente della Republica 22 settembre 1988, n. 447 [Code of Criminal Procedure]. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.del.presidente.della.repubblica:1988-09-22;447

Decreto Legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali) [Data Protection Code]. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196

Decreto Legislativo 30 maggio 2008, n. 109—Normattiva [Legislative Decree on the Implementation of Directive 2006/24/EC]. https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2008-05-30;109

Legge 20 novembre 2017, n. 167 [Provisions for the fulfillment of obligations arising from Italy's membership in the European Union]. https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2017-11-27&atto.codiceRedazionale=17G00180&atto.articolo.numero=0&atto.articolo.sottoArticolo=1&atto.articolo.sottoArticolo1=10&qId=fbeb199f-eba8-4380-8ba5-4c326a398bea&tabID=0.03819234598498489&title=lbl.dettaglioAtto

Luxembourg

Code d'instruction criminelle [Code of Criminal Procedure]. https://www.stradalex.lu/fr/slu_src_publ_leg_mema/toc/leg_lu_mema_180811_3/doc/mema_etat-leg-loi-1808-11-17-n1-jo

Loi du 5 juillet 20161. Portant réorganisation du Service de renseignement de l'État [Act on the Organization of the State Intelligence Service]. https://www.stradalex.lu/fr/slu_src_publ_leg_mema/toc/leg_lu_mema_201607_129/doc/mema_2016A2244A

Loi du 30 mai 2005—Relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et—Portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle [Act on Privacy and Electronic Communications]. https://legilux.public.lu/eli/etat/leg/loi/2005/05/30/n4/jo

Projet de loi relative à la rétention des données à caractère personnel [Draft Data Retention Law]. https://gouvernement.lu/dam-assets/documents/actualites/2023/01-janvier/25-tanson-loi-retention-donnees-caractere-personnel/projet-de-loi-rtention-des-donnes.pdf

Règlement grand-ducal du 24 juillet 2010 déterminant les catégories de données à caractère personnel générées ou traitées dans le cadre de la fourniture de services de

communications électroniques ou de réseaux de communications publics [Regulation on Categories of Retained Data]. https://legilux.public.lu/eli/etat/leg/rgd/2010/07/24/n1/jo

Poland

Prawo telekomunikacyjne z dnia 16 lipca 2004 [Telecommunications Law]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041711800

Rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. W sprawie sposobu technicznego przygotowania systemów i sieci służących do przekazywania informacji— Do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczania danych informatycznych [Regulation on technical preparation of information systems and networks]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20041001023

Rozporządzenie z dnia 28 grudnia 2009 r. W sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania [Regulation on Categories of Retained Data and obligated providers]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20092261828

Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego [Code of Criminal Procedure]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970890555

Ustawa z dnia 6 kwietnia 1990 r. O Policji [Police Act]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19900300179

Ustawa z dnia 9 czerwca 2006 r. O Centralnym Biurze Antykorupcyjnym [Act on the Central Anti-Corruption Bureau]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040708

Ustawa z dnia 9 czerwca 2006 r. O służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego [Act on the Military Counterintelligence Service and the Military Intelligence Service]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20061040710

Ustawa z dnia 12 października 1990 r. O Straży Granicznej [Act on the Border Guard]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU19900780462

Ustawa z dnia 16 listopada 2016 r. Przepisy wprowadzające ustawę o Krajowej Administracji Skarbowej [Act on the National Revenue Administration]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20160001948

Ustawa z dnia 24 maja 2002 r. O Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu [Act on the Internal Security Agency and the Foreign Intelligence Agency]. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu20020740676

Zachęcamy do zapoznania się z projektem ustawy o ochronie wolności użytkowników serwisów społecznościowych [Draft Law on the Protection of Freedom of Expression on the Internet]. https://www.gov.pl/web/sprawiedliwosc/zachecamy-do-zapoznania-sie-z-projektem-ustawy-o-ochronie-wolnosci-uzytkownikow-serwisow-spolecznosciowych

Spain

Ley 11/2022, de 28 de junio, General de Telecomunicaciones [Telecommunications Law]. https://www.boe.es/eli/es/l/2022/06/28/11

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones [Data Retention Law]. https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243

Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal [Criminal Code]. https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal [Data Protection Law]. https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Sweden

Förordning (2022:511) om elektronisk kommunikation Svensk författningssamling [Electronic Communications Decree]. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/forordning-2022511-om-elektronisk-kommunikation_sfs-2022-511

Lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet Svensk författningssamling [Act on the collection of electronic communications data in the intelligence activities of law enforcement authorities]. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2012278-om-inhamtning-av-uppgifter-om_sfs-2012-278

Lag (2022:482) om elektronisk kommunikation Svensk författningssamling [Electronic Communications Act]. https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2022482-om-elektronisk-kommunikation_sfs-2022-482#K

Switzerland

Bundesgesetz vom 18. März 2016 betreffend die Überwachung des Post- und Fernmeldeverkehrs [Federal Act on the Surveillance of Post and Telecommunications]. https://www.fedlex.admin.ch/eli/cc/2018/31/de

Bundesgesetz vom 19. Juni 1992 über den Datenschutz [Data Protection Act]. https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de

Bundesgesetz vom 25. September 2015 über den Nachrichtendienst [Intelligence Service Act]. https://www.fedlex.admin.ch/eli/cc/2017/494/de

Schweizerische Strafprozessordnung vom 5. Oktober 2007 [Code of Criminal Procedure]. https://www.fedlex.admin.ch/eli/cc/2010/267/de

Verordnung vom 15. November 2017 über die Überwachung des Post- und Fernmeldeverkehrs [Ordinance on the Surveillance of Post and Telecommunications]. https://www.fedlex.admin.ch/eli/cc/2018/32/de

United Kingdom

Communications Data Code of Practice. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

Investigatory Powers Act 2016. https://www.legislation.gov.uk/ukpga/2016/25/contents

Telecommunications Act 1984. https://www.legislation.gov.uk/ukpga/1984/12/contents

Appendix B. Coding Scheme

Table B.1. Coding Scheme

***(1) Why* is data retained?**
Purpose♣
national security♣
specific serious threats to national security♠
public security/safety♣
combatting serious crime♣
combatting crime♣
search and rescue of persons♥
defined with reference to the duties of competent authorities♥
Purpose defined♠
yes/no
Necessity condition♠
yes/no
Proportionality condition♠
yes/no
***(2) Who* is required to retain data?**
Obligated entities♣
providers of electronic communications services♣

network operators♣
providers of postal services♥
providers of OTTs♥
Exemptions♥
broadcasters♥
providers of services of negligible importance♥
for “exceptional reasons”♥
Reimbursement of Costs♣
(partial) reimbursement♣
no reimbursement♣
not mentioned♥
Storage may be entrusted to other entity♥
Problems associated with entrusting private companies with “public” tasks♦
accountability♦
legitimacy♦
data security♦
misuse of data♦
***(3) What* data is retained and for *how long*?**
Scope of retained data♣
categories of data listed (subscriber data, identification data, traffic data, location data)♥
specific data types listed♥
Content vs. metadata distinction♦♠
mentioned/not mentioned
Retention period♣
uniform♣: 6 months/12 months
depending on type of data♣
depending on purpose♥
Periodical extensions♣
yes/no
Necessity condition♠
yes/no
Based on precise criteria♠
yes/no
***(4)* With what *safeguards*?**
Data security and data protection principles♣♠♦
quality and security of retained data♣
access limited to authorized persons only♣
protection against unauthorized or accidental destruction and processing♣
destruction of data at the end of the period of retention♣♠
territorial storage restriction♠
user notification♠
user right of access♥
protection against data errors♦
Specification of how principles are implemented♥
yes/no
Supervisory authority♣
yes/no

Sanctioning mechanisms♥
yes/no
Legal remedies for affected persons♥
yes/no
Societal privacy implications♦
discriminatory profiling♦
social sorting♦
chilling effects♦
(5) **How is *access* to retained data regulated?**
Competent authorities♣
police and law enforcement authorities♣
judicial authorities♥
security forces and military institutions♣
security and intelligence services♣
fiscal and tax authorities♣
custom and border control authorities♣
anti-corruption authorities♥
competition and consumer-protection authorities♥
environmental organizations♥
public authorities related to the COVID-19 pandemic♦
no authorities specified♥
Prior judicial review♣♠
yes/no
Direct access in case of urgency♥
yes/no
Access without legal basis♥
yes/no

Note: ♣deducted from European Commission (2011); ♠deducted from CJEU case law; ♦deducted from literature on modern state surveillance; ♥identified during analysis

References

Albers, M., & Sarlet, I. W. (Eds.). (2022). *Personality and Data Protection Rights on the Internet: Brazilian and German Approaches*. Springer International Publishing. https://doi.org/10.1007/978-3-030-90331-2

Alvaro, A. (2006). Die Richtlinie zur Vorratsdatenspeicherung. *Datenschutznachrichten*, *29*(2), 52–55.

Arnig, M., Corrales Compagnucci, M., Forgó, N., Hoppe, N., Jlussi, D., Klügel, C., Kosta, E., & Krügel, T. (2008). *Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung*. RAUV Project (On behalf of the Austrian Federal Ministry of Transport, Innovation and Technology).

Article 29 Data Protection Working Party. (2018). *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*. https://ec.europa.eu/newsroom/article29/items/612053/en

Baldwin, R., Cave, M., & Lodge, M. (2012). *Understanding Regulation: Theory, Strategy, and Practice.* (2nd ed.). Oxford University Press. https://doi.org/10.1093/acprof:osobl/9780199576081.001.0001

Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (1st ed.). The MIT Press.

Bauman, Z. (2003). *Flüchtige Moderne (edition Suhrkamp*). Suhrkamp Verlag.

Bellovin, S. M., Blaze, M., Landau, S., & Pell, S. K. (2016). It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law. *Harvard Journal of Law & Technology*, *30*(1), 1–101.

Bennett, C. J. (2005). What happens when you book an airline ticket? The collection and processing of passenger data post-9/11. In E. Zureik, & M. B. Salter (Eds.), *Global Surveillance and Policing: Borders, security, identity (pp. 113–138)*. Willan Publishing.

Bennett, C. J., & Raab, C. D. (2003). *The Governance of Privacy: Policy Instruments in Global Perspective*. Ashgate.

Bernal, P. (2016). Data gathering, surveillance and human rights: Recasting the debate. *Journal of Cyber Policy*, *1*(2), 243–264. https://doi.org/10.1080/23738871.2016.1228990

Berthélémy, C. (2021, July 26). Europe's Data Retention Saga and its Risks for Digital Rights. *Digital Freedom Fund*. https://digitalfreedomfund.org/europes-data-retention-saga-and-its-risks-for-digital-rights/

Bertuzzi, L. (2022, November 15). *ePrivacy: EU legislators chase compromise on processing electronic communications data*. Www.Euractiv.Com. https://www.euractiv.com/section/data-protection/news/eprivacy-eu-legislators-chase-compromise-on-processing-electronic-communications-data/

Bignami, F. (2007). Privacy and Law Enforcement in the European Union: The Data Retention Directive. *Chicago Journal of International Law*, *8(1)*, 233–255.

Black, J. (2001). Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World. *Current Legal Problems*, *54*(1), 103–146. https://doi.org/10.1093/clp/54.1.103

Black, J. (2007). *Principles based regulation: Risks, challenges and opportunities*. http://eprints.lse.ac.uk/62814/

Black, J. (2010). Risk-based regulation: Choices, practices and lessons learnt. In *OECD Reviews of Regulatory Reform. Risk and Regulatory Policy: Improving the Governance of Risk* (pp. 185-224).

Bozhinova, K. (2020, April 15). Bulgaria: Tracking mobile devices and data protection - Where do we draw the line? *Schoenherr*. https://www.schoenherr.eu/content/bulgaria-tracking-mobile-devices-and-data-protection-where-do-we-draw-the-line/

Braman, S. (2009). *Change of State: Information, Policy, and Power*. MIT Press.

Breyer, P. (2005). *Die systematische Aufzeichnung und Vorhaltung von Telekommunikations-Verkehrsdaten für staatliche Zwecke in Deutschland: Vorratsspeicherung, traffic data retention*. Rhombos-Verlag.

Breyer, P. (2019, June 6). The data retention zombie is back. *Patrick Breyer*. https://www.patrick-breyer.de/en/the-data-retention-zombie-is-back/

Breyer, P. (2022, June 7). 'Targeted' Data Retention: Online map shows what the Belgian government wants to hide. *Patrick Breyer*. https://www.patrick-breyer.de/en/targeted-data-retention-online-map-shows-what-the-belgian-government-wants-to-hide/

Breyer, P., Lund, J., Le Querrec, B., Vobořil, J., & Santos, E.. (2022, June 9). *Stop #DataRetention: Exposing a New Generation of Data Retention Laws*. https://media.ccc.de/v/ccchh-extras-4167-stop-dataretention-exp

Büchi, M., Festic, N., Just, N., & Latzer, M. (2021). Digital inequalities in online privacy protection: Effects of age, education and gender. In E. Hargittai (Ed.), *Handbook of Digital Inequality* (pp. 296–310). Edward Elgar. https://www.elgaronline.com/view/edcoll/9781788116565/9781788116565.00029.xml

Büchi, M., Festic, N., & Latzer, M. (2022). The Chilling Effects of Digital Dataveillance: A Theoretical Model and an Empirical Research Agenda. *Big Data & Society*, *9*(1), 1–14. https://doi.org/10.1177/20539517211065368

Büchi, M., Fosch-Villaronga, E., Lutz, C., Tamò-Larrieux, A., Velidi, S., & Viljoen, S. (2020). The chilling effects of algorithmic profiling: Mapping the issues. *Computer Law & Security Review*, *36*, 1–15. https://doi.org/10.1016/j.clsr.2019.105367

Büchi, M., Just, N., & Latzer, M. (2017). Caring is not enough: The importance of Internet skills for online privacy protection. *Information, Communication & Society*, *20*(8), 1261–1278. https://doi.org/10.1080/1369118X.2016.1229001

Bug, M. (2016). Terrorismusbekämpfung als Waffe gegen Alltagskriminalität – Argumentation und Wirklichkeit der Vorratsdatenspeicherung in Deutschland. *Zeitschrift Für Parlamentsfragen*, *47*(3), 670–692.

Büllingen, F., Gillet, A., Gries, C.-I., Hillebrand, A. & Stamm, P. (2004). Stand und Perspektiven der Vorratsdatenspeicherung im internationalen Vergleich. *WIK Diskussionsbeitrag, No. 261, WIK Wissenschaftliches Institut Für Infrastruktur Und Kommunikationsdienste*.

Bundesrat. (2022). *Teilrevisionen vier Ausführungserlasse des BÜPF (VÜPF, GebV-ÜPF, VD-ÜPF, VVS-ÜPF). Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens*. https://www.newsd.admin.ch/newsd/message/attachments/70208.pdf

Centre for Strategy & Evaluations Services. (2012). *Evidence of Potential Impacts of Options for Revising the Data Retention Directive: Current approaches to data preservation in the EU and in third countries*. http://publications.europa.eu/resource/cellar/5dc1b779-1a1c-4e53-a17f-1fd0fe71e4ad.0001.01/DOC_1

Chambre des représentants. (2022). *Projet de loi relatif à la collecte et à la conservation des données d'identification et des métadonnées dans le secteur des communications électroniques et à la fourniture de ces données aux autorités (DOC 55 2572/001)*. https://www.lachambre.be/FLWB/PDF/55/2572/55K2572001.pdf

Chiusi, F., Fischer, S., & Spielkamp, M. (2020). *Automated Decision-Making Systems in the COVID-19 Pandemic: A European Perspective*. AlgorithmWatch, Bertelsmann Stiftung. https://algorithmwatch.org/wp- content/uploads/2020/08/ADM-systems-in-the-Covid-19-pandemic- Report-by-AW-BSt-Sept-2020.pdf

Cole, J. I., Suman, M., Schramm, P., Lunn, R., Zhou, L., Tang, A. S., & Ognyanova, K. (2012). *The World Internet Project. International Report. Third Edition.* https://www.digitalcenter.org/wp-content/uploads/2012/12/2012wip_report3rd_ed.pdf

Cole, J. I., Suman, M., Schramm, P., & Zhou, L. (2015). *The World Internet Project. International Report. Sixth Edition.* https://www.digitalcenter.org/wp-content/uploads/2013/06/2015-World-Internet-Report.pdf

Cole, J. I., Suman, M., Schramm, P., & Zhou, L. (2017a). *The World Internet Project. International Report. Seventh Edition.* https://www.digitalcenter.org/wp-content/uploads/2017/12/2016-World-Internet-Project-Report.pdf

Cole, J. I., Suman, M., Schramm, P., & Zhou, L. (2017b). *The World Internet Project. International Report. Eighth Edition.* https://www.digitalcenter.org/wp-content/uploads/2018/04/2017-WIP-report.pdf

Cole, J. I., Suman, M., Schramm, P., & Zhou, L. (2018). *The World Internet Project. International Report. Ninth Edition.* https://www.digitalcenter.org/wp-content/uploads/2019/01/World-Internet-Project-report-2018.pdf

Cole, J. I., Suman, M., Schramm, P., & Zhou, L. (2019). *The World Internet Project. International Report. Tenth Edition.* https://www.digitalcenter.org/wp-content/uploads/2019/12/2019-World-Internet-Project-10th-Edition.pdf

Conley, C. (2015). Non-Content is Not Non-Sensitive: Moving Beyond the Content/Non-Content Distinction. *Santa Clara Law Review*, *54*(4), 821–842.

Dachwitz, I., & Meister, A. (2022, October 25). *Quick Freeze: Buschmann legt Alternative zur Vorratsdatenspeicherung vor*. netzpolitik.org. https://netzpolitik.org/2022/quick-freeze-buschmann-legt-alternative-zur-vorratsdatenspeicherung-vor/

de Londras, F. (2013). Privatized counter-terrorist surveillance: Constitutionalism undermined. In F. Davis, N. McGarrity, & G. Williams (Eds.), *Surveillance, counter-terrorism and comparative constitutionalism* (pp. 59–72). Routledge.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., & Blondel, V. D. (2013). Unique in the Crowd: The privacy bounds of human mobility. *Scientific Reports*, *3*(1), 1–5. https://doi.org/10.1038/srep01376

Deutscher Bundestag. (2015). *Deutscher Bundestag—Bundestag beschließt neue Vorratsdatenspeicherung*. Deutscher Bundestag. https://www.bundestag.de/webarchiv/textarchiv/2015/kw42_de_vorratsdatenspeicherung-391654

Deutscher Bundestag. (2022). *Keine Unterstützung für Forderung nach IP-Adressen-Speicherung*. Deutscher Bundestag. https://www.bundestag.de/dokumente/textarchiv/2022/kw39-de-ip-adressen-911398

Eck, K., & Hatz, S. (2020). State surveillance and the COVID-19 crisis. *Journal of Human Rights*, *19*(5), 603–612. https://doi.org/10.1080/14754835.2020.1816163

European Commission. (2011). *Evaluation report on the Data Retention Directive (Directive 2006/24/EC) (COM(2011) 225 final)* (COM(2011) 225; p. 49). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52011DC0225&from=EN

European Commission. (2020). *Study on the retention of electronic communications non-content data for law enforcement purposes: Final report*. https://data.europa.eu/doi/10.2837/384802

European Commission. (2021). *Data retention—Commission services non-paper Contribution to the Council COPEN Working Party meeting of 16 June 2021* [WK 7294/2021 INIT]. https://www.statewatch.org/media/2592/eu-council-data-retention-com-non-paper-wk-7294-2021.pdf

European Data Protection Board (EDPB). (2022, February 15). *Launch of coordinated enforcement on use of cloud by public sector*. https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en

European Data Protection Board (EDPB), & European Data Protection Supervisor (EDPS). (2022). *Joint Opinion 4/2022 on the Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse*. https://edps.europa.eu/system/files/2022-07/22-07-28_edpb-edps-joint-opinion-csam_en.pdf

European Data Protection Supervisor (EDPS). (2010). *The 'moment of truth' for the Data Retention Directive: EDPS demands clear evidence of necessity*. https://edps.europa.eu/sites/edp/files/edpsweb_press_releases/edps-2010-17_data_retention_directive_en.pdf

European Digital Rights (EDRi). (2021, August 2). Europe's Data Retention Saga and its Risks for Digital Rights. *European Digital Rights (EDRi)*. https://edri.org/our-work/europes-data-retention-saga-and-its-risks-for-digital-rights/

European Union Agency for Network and Information Security (ENISA). (2022). *Telecom Security Incidents 2021*. https://www.enisa.europa.eu/publications/telecom-security-incidents-2021

Eviette, M., & Simpson, A. (2021). Towards Models for Privacy Preservation in the Face of Metadata Exploitation. In M. Friedewald, S. Schiffner, & S. Krenn (Eds.), *Privacy and Identity Management* (pp. 247–264). Springer International Publishing. https://doi.org/10.1007/978-3-030-72465-8_14

Ferguson, A. G. (2017). *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press. https://doi.org/10.2307/j.ctt1pwtb27

Foucault, M. (1976). *Überwachen und Strafen: D. Geburt d. Gefängnisses*. Suhrkamp.

Gandy Jr., O. H. (2021). *The Panoptic Sort: A Political Economy of Personal Information* (2nd ed.). Oxford University Press. https://doi.org/10.1093/oso/9780197579411.001.0001

Garland, D. (2001). *The Culture of Control: Crime and Social Order in Contemporary Society*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199258024.001.0001

Gartner, R. (2016). What Metadata Is and Why It Matters. In R. Gartner (Ed.), *Metadata: Shaping Knowledge from Antiquity to the Semantic Web* (pp. 1–13). Springer International Publishing. https://doi.org/10.1007/978-3-319-40893-4_1

Grossenbacher, T. (2017, March 7). Staatliche Überwachung—Fundbüros greifen auf heikle Daten zu. *Schweizer Radio und Fernsehen (SRF)*. https://www.srf.ch/news/schweiz/fundbueros-greifen-auf-heikle-daten-zu

Hansjakob, T. (2002). *Kommentar zum Bundesgesetz und zur Verordnung über die Überwachung des Post- und Fernmeldeverkehrs*. Institut für Rechtswissenschaft und Rechtspraxis IRP-HSG.

Hansjakob, T. (2018). *Überwachungsrecht der Schweiz, Kommentar zu Art. 169 ff. StPO und zum BÜPF.* Schulthess.

Harcourt, B. E. (2015). *Exposed: Desire and Disobedience in the Digital Age*. Harvard University Press.

Harries, J., & Mayer, D. (2021, October 19). LightBasin: A Roaming Threat to Telecommunications Companies. *Crowdstrike.* https://www.crowdstrike.com/blog/an-analysis-of-lightbasin-telecommunications-attacks/

Henley, J. (2019, September 12). Denmark frees 32 inmates over flaws in phone geolocation evidence. *The Guardian*. https://www.theguardian.com/world/2019/sep/12/denmark-frees-32-inmates-over-flawed-geolocation-revelations

Hensel, D. (2009). Die Vorratsdatenspeicherung aus datenschutzrechtlicher Sicht: Die Bildung von Persönlichkeitsprofilen und andere Probleme der Vorratsdatenspeicherung. *Datenschutz und Datensicherheit - DuD*, *33*(9), 527–530. https://doi.org/10.1007/s11623-009-0137-9

Hintz, A. (2014). Outsourcing Surveillance—Privatising Policy: Communications Regulation by Commercial Intermediaries. *Birkbeck Law Review*, *2*(2), 349–368.

Hoeren, T. (2012). *Internet- und Kommunikationsrecht. Praxis-Lehrbuch. 2. Auflage*. Verlag Dr. Otto Schmidt.

Home Office. (2018). *Bulk acquisition of communications data: Code of Practice*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715477/Bulk_Communications_Data_Code_of_Practice.pdf

Hosein, G., & Palow, C. W. (2013). Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques. *Ohio State Law Journal*, *74(6),* 1071–1104.

Hügel, S. (2021, May 26). Vorratsdatenspeicherung: Und täglich grüßt das Murmeltier. *netzpolitik.org*. https://netzpolitik.org/2021/vorratsdatenspeicherung-und-taeglich-gruesst-das-murmeltier/

Human Rights Council of the United Nations. (2013). *Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue* [Data set]. Koninklijke Brill NV. https://doi.org/10.1163/2210-7975_HRD-9970-2016149

Irion, K. (2014). *Accountability Unchained: Bulk Data Retention, Preemptive Surveillance, and Transatlantic Data Protection*. In Rotenberg, M., Horwitz, J., & Scott, J. (Eds.), *Privacy in the Modern Age. The Search for Solutions* (pp. 78–92). The New Press.

Juszczak, A., & Sason, E. (2021). Recalibrating Data Retention in the EU the Jurisprudence of the CJEU – is this the End or the Beginning? *Eucrim*, *4*, 238–266. https://doi.org/10.30709/eucrim-2021-020

Kapetanios, C., Polyzos, T., Alepis, E., & Patsakis, C. (2021). *This is Just Metadata: From No Communication Content to User Profiling, Surveillance and Exploitation.* In G. Tsihrintzis & M. Virvou (Eds.), *Advances in Core Computer Science-Based Technologies. Learning and Analytics in Intelligent Systems* (pp. 277–302). Springer. https://doi.org/10.1007/978-3-030-41196-1_13

Kayali, L. (2021, March 3). France seeks to bypass EU top court on data retention. *POLITICO*. https://www.politico.eu/article/france-data-retention-bypass-eu-top-court/

Kelly, A. (2022, June). Based in reality? *Law Society Gazette*, *116*(5), 20–23.

Kierkegaard, P. (2011). Electronic Health Record: Wiring Europe's Healthcare. *Computer Law & Security Report*, *27(5)*, 503–515. https://doi.org/10.1016/j.clsr.2011.07.013

Kosta, E. (2018). The Retention of Communications Data in Europe and the UK. In L. Edwards (Ed.), *Law, Policy and the Internet* (pp. 193–212). Hart Publishing.

Landau, S. (2020). Categorizing Uses of Communications Metadata: Systematizing Knowledge and Presenting a Path for Privacy. *New Security Paradigms Workshop 2020*, 1–19. https://doi.org/10.1145/3442167.3442171

Latzer, M. (1999). Transformation der Staatlichkeit im Kommunikationssektor: Regulierungsansätze für die Mediamatik. In K. Imhof, O. Jarren, & R. Blum (Eds.), *Steuerungs- und Regelungsprobleme in der Informationsgesellschaft* (pp. 282–296). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-663-12385-9_22

Latzer, M. (2013). Towards an Innovation-Co-evolution-Complexity Perspective on Communications Policy. In M. Löblich & S. Pfaff-Rüdiger (Eds.), *Communication and Media Policy in the Era of Digitization and the Internet* (pp. 15–27). Nomos. https://doi.org/10.5771/9783845243214

Latzer, M. (2022). The Digital Trinity—Controllable Human Evolution—Implicit Everyday Religion. *Kölner Zeitschrift Für Soziologie Und Sozialpsychologie*, *74*(1), 331–354. https://doi.org/10.1007/s11577-022-00841-8

Latzer, M., Büchi, M., & Festic, N. (2019). V*ertrauen und Sorgen bei der Internetnutzung in der Schweiz 2021: Themenbericht aus dem World Internet Project—Switzerland 2019*. Universität Zürich. https://doi.org/10.5167/uzh-176010

Latzer, M., Büchi, M., & Just, N. (2015): V*ertrauen und Sorgen bei der Internet-Nutzung in der Schweiz: Themenbericht aus dem World Internet Project—Switzerland 2015*. Universität Zürich. https://doi.org/10.5167/uzh-122556

Latzer, M., Büchi, M., Festic, N., & Just, N. (2017). V*ertrauen und Sorgen bei der Internetnutzung in der Schweiz 2021: Themenbericht aus dem World Internet Project—Switzerland 2017*. Universität Zürich. https://doi.org/10.5167/uzh-142252

Latzer, M., Büchi, M., Kappeler, K., & Festic, N. (2021a). *Internet und Politik in der Schweiz 2021: Themenbericht aus dem World Internet Project—Switzerland 2021*. Universität Zürich. https://doi.org/10.5167/uzh-211120

Latzer, M., Büchi, M., Kappeler, K., & Festic, N. (2021b). *Vertrauen und Sorgen bei der Internetnutzung in der Schweiz 2021: Themenbericht aus dem World Internet Project—Switzerland 2021*. Universität Zürich. https://doi.org/10.5167/uzh-211159

Latzer, M., & Just, N. (2020). Governance by and of Algorithms on the Internet: Impact and Consequences. In *Oxford Research Encyclopedia of Communication*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228613.013.904

Latzer, M., Just, N., Metreveli, S., & Saurwein, F. (2012). Vertrauen und Sorgen bei der Internet-Nutzung in der Schweiz. Themenbericht aus dem World Internet Project—Switzerland 2011. Universität Zürich. https://doi.org/10.5167/uzh-68886

Latzer, M., Just, N., Metreveli, S., & Saurwein, F. (2013). Vertrauen und Sorgen bei der Internet-Nutzung in der Schweiz. Themenbericht aus dem World Internet Project—Switzerland 2013. Universität Zürich. https://doi.org/10.5167/uzh-86249

Latzer, M., Saurwein, F., & Just, N. (2019). Assessing Policy II: Governance-Choice Method. In H. Van den Bulck, M. Puppis, K. Donders, & L. Van Audenhove (Eds.), *The Palgrave Handbook of Methods for Media Policy Research* (pp. 557–574). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-16065-4_32

Lund, J. (2022, June 15). *The new Danish data retention law: Attempts to make it legal failed after just six days*. *IT-Politisk Forening.* https://itpol.dk/articles/new-Danish-data-retention-law-2022

Lyon, D. (2002). Surveillance as social sorting Computer codes and mobile bodies. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination* (1st ed.). Routledge.

Lyon, D. (2009). Surveillance, power, and everyday life. In C. Avgerou, R. Mansell, D. Quah, & R. Silverstone (Eds.), *The Oxford Handbook of Information and Communication Technologies* (pp. 449–468). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199548798.001.0001

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique. *Big Data and Society*, *1*(2), 1–13. https://doi.org/10.1177/2053951714541861

Lyon, D. (2022). *Pandemic surveillance*. Polity.

Mac, R., Haskins, C., & Pequeño IV, A. (2021, August 25). Clearview AI Offered Free Facial Recognition Trials To Police All Around The World. *BuzzFeed News*. https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table

Maggiore, M. (2017, December 2). *Data retention law in Italy: From bad to worse*. https://www.linkedin.com/pulse/data-retention-law-italy-from-bad-worse-massimo-maggiore/

Marthews, A., & Tucker, C. E. (2017). *Government Surveillance and Internet Search Behavior*. Social Science Research Network. https://doi.org/10.2139/ssrn.2412564

Marx, G. T. (2002). What's New About the 'New Surveillance'? Classifying for Change and Continuity. *Surveillance & Society*, *1*(1), 9–29. https://doi.org/10.24908/ss.v1i1.3391

Marx, G. T. (2015). Surveillance Studies. In *International Encyclopedia of the Social & Behavioral Sciences* (pp. 733–741). Elsevier. https://doi.org/10.1016/B978-0-08-097086-8.64025-4

Matter, L. (2019). Die Vorratsdatenspeicherung auf dem Prüfstand. *sui generis, 258–273*. https://doi.org/10.21257/sg.108

Mayer, J., Mutchler, P., & Mitchell, J. C. (2016). Evaluating the privacy properties of telephone metadata. *Proceedings of the National Academy of Sciences*, *113*(20), 5536–5541. https://doi.org/10.1073/pnas.1508081113

McIntyre, T. J. (2008). Data retention in Ireland: Privacy, policy and proportionality. *Computer Law & Security Review*, *24*(4), 326–334. https://doi.org/10.1016/j.clsr.2008.03.001

Meineck, S., Reuter, M., & Meister, A. (2022, June 29). Geleakter Bericht: EU-Kommission nimmt hohe Fehlerquoten bei Chatkontrolle in Kauf. *netzpolitik.org*. https://netzpolitik.org/2022/geleakter-bericht-eu-kommission-nimmt-hohe-fehlerquoten-bei-chatkontrolle-in-kauf/

Mejias, U. A., & Couldry, N. (2019). Datafication. *Internet Policy Review*, *8*(4), 1–10. https://doi.org/10.14763/2019.4.1428

Memmott, M. (2013, June 7). 'Nobody Is Listening To Your Telephone Calls,' Obama Says. *NPR*. https://www.npr.org/sections/thetwo-way/2013/06/07/189522677/nobody-is-listening-to-your-telephone-calls-obama-says

Milaj, J., & Kaiser, C. (2017). Retention of data in the new Anti-money Laundering Directive—'Need to know' versus 'nice to know'. *International Data Privacy Law*, *7*(2), 115–125. https://doi.org/10.1093/idpl/ipx002

Mitsilegas, V. (2020). The Preventive Turn in European Security Policy: Towards a Rule of Law Crisis? In F. Bignami (Ed.), *EU Law in Populist Times: Crises and Prospects* (pp. 301–318). Cambridge University Press. https://doi.org/10.1017/9781108755641.011

Mitsilegas, V. (2021). The Privatisation of Surveillance in the Digital Age. In V. Mitsilegas & N. Vavoula (Eds.), *Surveillance and Privacy in the Digital Age: European, Transatlantic and Global Perspectives* (pp. 101–158). Hart Publishing.

Mitsilegas, V., Guild, E., Kuskonmaz, E., & Vavoula, N. (2022). Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks. *European Law Journal*, 1–36. https://doi.org/10.1111/eulj.12417

Moser-Knierim, A. (2014). Vorratsdatenspeicherung – Paradigma für die Kollision zwischen Freiheit und Sicherheit. In A. Moser-Knierim (Ed.), *Vorratsdatenspeicherung: Zwischen Überwachungsstaat und Terrorabwehr* (pp. 139–206). Springer Fachmedien. https://doi.org/10.1007/978-3-658-04156-4_4

Mugari, I., & Obioha, E. E. (2021). Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing. *Social Sciences*, *10*(6), 1–14. https://doi.org/10.3390/socsci10060234

Murray, D., & Fussey, P. (2019). Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data. *Israel Law Review*, *52*(1), 31–60. https://doi.org/10.1017/S0021223718000304

Ng, A. (2022, July 13). Amazon gave Ring videos to police without owners' permission. *POLITICO*. https://www.politico.com/news/2022/07/13/amazon-gave-ring-videos-to-police-without-owners-permission-00045513

Nissenbaum, H. (2010). *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press. https://doi.org/10.1515/9780804772891

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

OECD. (2010). *Risk and Regulatory Policy: Improving the Governance of Risk*. OECD. https://www.oecd.org/publications/risk-and-regulatory-policy-9789264082939-en.htm

OECD. (2022). *Building Trust to Reinforce Democracy: Main Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions*. OECD. https://doi.org/10.1787/b407f99c-en

Orwell, G. (1983). *1984 (Nineteen Eighty-Four)*. Houghton Mifflin Harcourt.

Ostrom, E. (1990). *Governing the Commons: The Evolution of Institutions for Collective Action*. Cambridge University Press. https://doi.org/10.1017/CBO9780511807763

Outlaw III, L. T. (2021). Look up and Smile for Daddy Warbucks's Surveillance Plane: Reforming the Standard for Determining When a Private Search Constitutes Government Action, and why it's Needed to Meet the Growing Fourth Amendment Problem of Privatized Surveillance. *Michigan State Law Review*, *2021*(3), 861–930.

Peeters, R. (2015). The price of prevention: The preventative turn in crime policy and its consequences for the role of the state. *Punishment & Society*, *17*(2), 163–183. https://doi.org/10.1177/1462474514560392

Penney, J. (2016). Chilling Effects: Online Surveillance and Wikipedia Use. *Berkeley Technology Law Journal, 31*(1), 117–182.

Pfitzmann, A., & Köpsell, S. (2009). Risiken der Vorratsspeicherung: Grenzen der Nutzungsüberwachung. *Datenschutz und Datensicherheit - DuD*, *33*(9), 542–546. https://doi.org/10.1007/s11623-009-0140-1

Podkowik, J., Rybski, R., & Zubik, M. (2021). Judicial dialogue on data retention laws: A breakthrough for European constitutional courts? *International Journal of Constitutional Law*, *19*(5), 1597–1631. https://doi.org/10.1093/icon/moab132

Privacy International. (2017). *National Data Retention Laws Since the CJEU's Tele-2/Watson Judgement. A Concerning State of Play for the Right to Privacy in Europe*. https://privacyinternational.org/sites/default/files/2017-12/Data%20Retention_2017.pdf

Privacy International. (2020, April 21). *Telco data and Covid-19: A primer*. Privacy International. http://privacyinternational.org/explainer/3679/telco-data-and-covid-19-primer

Puppis, M. (2019). Analyzing Talk and Text I: Qualitative Content Analysis. In H. Van den Bulck, M. Puppis, K. Donders, & L. Van Audenhove (Eds.), *The Palgrave Handbook of Methods for Media Policy Research* (pp. 367–384). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-16065-4_21

Rainie, L., & Madden, M. (2015, March 16). Americans' Privacy Strategies Post-Snowden. *Pew Research Center: Internet, Science & Tech*. https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden/

Regan, P. M. (1995). *Legislating Privacy: Technology, Social Values, and Public Policy*. University of North Carolina Press.

Richards, N. M. (2013). The Dangers of Surveillance. *Harvard Law Review*, *126*(7), 1934–1965.

Riebe, T., Haunschild, J., Divo, F., Lang, M., Roitburd, G., Franken, J., & Reuter, C. (2020). Die Vorratsdatenspeicherung in Europa. *Datenschutz und Datensicherheit - DuD*, *44*(5), 316–321. https://doi.org/10.1007/s11623-020-1275-3

Rojszczak, M. (2021). The uncertain future of data retention laws in the EU: Is a legislative reset possible? *Computer Law & Security Review*, *41*, 1–12. https://doi.org/10.1016/j.clsr.2021.105572

Rosenau, J. N., & Czempiel, E.-O. (Eds.). (1992). *Governance without Government: Order and Change in World Politics*. Cambridge University Press. https://doi.org/10.1017/CBO9780511521775

Rozenshtein, A. Z. (2018). Surveillance Intermediaries. *Stanford Law Review*, *70*, 99–189.

Rucz, M., & Kloosterboer, S. (2020). Data Retention Revisited. *European Digital Rights (EDRi)*. https://edri.org/wp-content/uploads/2020/09/Data_Retention_Revisited_Booklet.pdf

Saidi, S. J., Gasser, O., & Smaragdakis, G. (2022). One bad apple can spoil your IPv6 privacy. *ACM SIGCOMM Computer Communication Review*, *52*(2), 10–19. https://doi.org/10.1145/3544912.3544915

Schmidt, S. (2015, October 18). Warum ich keine Texte zur Vorratsdatenspeicherung lese. *Süddeutsche.de*. https://www.sueddeutsche.de/digital/digitale-ueberwachung-warum-ich-keine-artikel-zur-vorratsdatenspeicherung-lese-1.2696689

Scott, C. (2004). *Regulation in the Age of Governance: The Rise of the Post Regulatory State* (pp. 145–174). Edward Elgar Publishing. https://doi.org/10.4337/9781845420673

Sieber, U., & von zur Mühlen, N. (Eds.). (2016). *Access to Telecommunication Data in Criminal Justice. A Comparative Analysis of European Legal Orders*. Duncker & Humblot.

Solove, D. J. (2015). The meaning and value of privacy. In B. Roessler & D. Mokrosinska (Eds.), *Social Dimensions of Privacy* (1st ed., pp. 71–82). Cambridge University Press. https://doi.org/10.1017/CBO9781107280557

Solove, D. J. (2023). *Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data*. Social Science Research Network. https://doi.org/10.2139/ssrn.4322198

Thierse, S., & Badanjak, S. (2021). The Never-Ending Story of Data Retention in the EU. In S. Thierse & S. Badanjak, *Opposition in the EU Multi-Level Polity* (pp. 11–27). Springer International Publishing. https://doi.org/10.1007/978-3-030-47162-0_2

Tokson, M. J. (2009). The Content/Envelope Distinction in Internet Law. *William & Mary Law Review*, *50*(6), 2105–2176.

Tzanou, M., & Karyda, S. (2022). Privacy International and Quadrature du Net: One Step Forward Two Steps Back in the Data Retention Saga? *European Public Law*, *28*(1), 123–154. https://doi.org/10.54648/euro2022007

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society*, *12*(2), 197–208. https://doi.org/10.24908/ss.v12i2.4776

Whitley, E. A., & Hosein, I. (2005). Policy discourse and data retention: The technology politics of surveillance in the United Kingdom. *Telecommunications Policy*, *29*(11), 857–874. https://doi.org/10.1016/j.telpol.2005.06.012

YouGov. (2022). *Europäisches Parlament Data Retention - all countries - weighted. Feldzeit: 24.-28.12.2021. Durchgeführt von YouGov. Europäisches Parlament.* https://nextcloud.pp-eu.eu/index.php/s/QLkek3QRFLoAdzq

Zedner, L. (2007). Pre-crime and post-criminology? *Theoretical Criminology*, *11*(2), 261–281. https://doi.org/10.1177/1362480607075851

Zubik, M., Podkowik, J., & Rybski, R. (2021). Judicial Dialogue on Data Retention Laws in Europe in the Digital Age: Concluding Remarks. In M. Zubik, J. Podkowik, & R. Rybski (Eds.), *European Constitutional Courts towards Data Retention Laws* (pp. 229–249). Springer International Publishing. https://doi.org/10.1007/978-3-030-57189-4

Zuboff, S. (2019). *The age of surveillance capitalism: the fight for a human future at the new frontier of power (1st ed.)*. PublicAffairs.