

Articles

Pitting Karlsruhe Against Luxembourg? German Data Protection and the Contested Implementation of the EU Data Retention Directive

*By Christian DeSimone**

A. Introduction

Since the 1980s Germany has developed a subtle and complex data protection jurisprudence originally designed to protect individual data subjects from rights abuses by market actors. However, the rights aggressor has increasingly been German and European law enforcement authorities. This evolving corpus of law also exhibits a singularly-German mindfulness of the historical significance of abrogating fundamental rights within constitutional democracy.

In the wake of the 9/11, Madrid, and London Terror attacks, the European Union (EU) expanded a new phase of cooperation in law enforcement emphasizing preventive domestic anti-terrorism measures.¹ While many countries were complicit, the major drivers of more stringent anti-terrorism policy were the United Kingdom and the United States. A key plank of this Anglo-American agenda has been electronic communications surveillance.

In 2006, the EU institutions passed an EU-wide Data Retention Directive² pursuant to which *all* communications traffic data is captured and stored by communications services providers (CSPs) for a period of up to two years. Flexibly-designed to allow for member state subsidiarity, German legislators considerably overstepped the Directive's minimum requirements when they transposed it into German law a year later. Assorted German law enforcement and other agencies are provided access to the data in service of varied state purposes. The law transposing the Directive enormously burdened fundamental rights

* Academic Fulbright Fellow (Germany) 2008-2009, affiliated with the Freie Universität Berlin. Email: christiang.desimone@gmail.com

¹ Francesca Bignami, *Protecting Privacy Against the Police in the European Union: The Data Retention Directive*, 8 CHICAGO JOURNAL OF INTERNATIONAL LAW 233, 234 (2007).

² Hereinafter also referred to as "the Directive," but not to be confused with the EU Data Protection Directive of 1995.

guaranteed by the *Grundgesetz* (Basic Law). Moreover, it failed to meet legal standards of certainty and proportionality and has been declared *verfassungswidrig* (unconstitutional) by the *Bundesverfassungsgericht* (BVerfG - Federal Constitutional Court) in a landmark ruling announced in March 2010.³

Yet, by accepting the basic rights protections of the Directive, the Constitutional Court's decision avoided a potential showdown with the European Court of Justice (ECJ) in Luxembourg.

This paper has two goals: to impart an understanding of the theory and legal application of German data protection and to illustrate the how the German law that sought to transpose the EU Directive conflicted with these norms. Part B surveys the history of German data protection, sketching key jurisprudential underpinnings in two seminal cases. Part C describes the legislative developments associated with the EU Data Retention Directive. Part D discusses the implementation of the Directive and the political and popular challenges it faced. Part E examines the impact the German legislation transposing the Directive would have had on basic rights protected by the *Grundgesetz*. Finally, Part F outlines implications of the recent *BVerfG* ruling on the constitutional complaint that challenged the German law giving domestic force to the Directive.

B. Two Milestones in German Data Protection History

I. Volkszählungsurteil

Two particular *BVerfG* cases stand out for their relevance to *Vorratsdatenspeicherung* (data retention) and significance in German data protection law. The first is the so-called *Volkszählungsurteil* (Population Census Case) of 1983 in which the *BVerfG* created the basic constitutional right to informational self-determination, setting the jurisprudential foundation of German data protection.⁴

In 1982, Helmut Kohl's new ruling coalition of the *Unionsfraktion* (Union faction including the Christian Democratic Union [CDU] and the Bavarian Christian Social Union [CSU])⁵ allied with the Free Democratic Party (FDP), introduced legislation in the *Bundestag* (German federal parliament) calling for a population census for the following year. After the parties settled cost disputes, the bill passed without hitch. This was in stark contrast to

³Data Retention Case, BVerfG, 1 BvR 256/08, from 2 March 2010, available at http://www.bverfg.de/entscheidungen/rs20100302_1bvr025608.html.

⁴Population Census Case, BVerfGE 65, 1 (para. 42).

⁵Christian Democratic Union (national German political party) in political alliance with the Christian Social Union of Bavaria (regional political party).

the ensuing controversy. Public sentiment that the census was an unjust and unnecessary state invasion of privacy led civic groups to file a constitutional complaint challenging the law and to lobby the government to scrap its plans entirely. Among the concerns raised by the opponents were the fear that authorities would trace responses back to particular individuals and that the collected data would be used not only for aggregative statistical purposes but also for the correction of local residential registries.⁶

The resulting *BVerfG* decision upheld the statistical purposes of the census but insisted on procedural safeguards to protect basic rights against abuse. Data transfer to local authorities was deemed unconstitutional because it combined unjustified with justified purposes.⁷ This ruling, widely considered a victory for the anti-census movement, only delayed the population census until 1987; but it also birthed core data protection ideas.

1. Informational Self-Determination

Informational self-determination is at once a basic right legally anchored in—and flowing from—the *Grundgesetz* (Basic Law) and a sociological norm aiming to preserve micro processes of individual development and macro-level social stability from the vicissitudes of modern life. In the *Population Census Case* the *BVerfG* stipulated that this right broadly guarantees the fundamental capacity of individuals to decide for themselves about the disclosure and use of their personal data.⁸

As a legal right, informational self-determination is an instantiation of the general right of personality which guarantees the ability of individuals to freely develop their own character. Developed by the *BVerfG* in 1954, this general right is in turn based upon two fundamental rights identified in the Basic Law: the protection of human dignity⁹ and the right to personal freedom.¹⁰ In contrast to simple conceptions of privacy as a right to be left alone, German constitutional law broadly protects three personal spheres. The *Individualsphäre* (individual sphere) includes protections of rights to self-determination, a right to re-socialization after imprisonment, and a right to know one's biological parents. The *Privatsphäre* (private sphere) includes the inviolability of one's *Kernbereich* (core

⁶ Gerrit Hornung & Christoph Schnabel, *Data Protection in Germany I: The Population Census Decision and the Right to Informational Self-Determination*, 25 *COMPUTER LAW & SECURITY REVIEW* 84, 85(2009).

⁷ *Id.* at 85.

⁸ *Population Census Case*, *supra* note 4, at para. 43.

⁹ See *Grundgesetz*, für die Bundesrepublik Deutschland (GG-Basic Law) May 23, 1949, *Bundesgesetzblatt* (BGBl) 1, art. 1, para. 1 (hereinafter Basic Law) (“The dignity of man is inviolable. To observe and protect it is the duty of all state power.”).

¹⁰ See *id.* at art. 2, para. 2 (“Each person has a right to the free development of their personality to the extent they do not injure the rights of others, contradict the constitutional order or moral law.”).

area/home), protections against various types of defamation, and rights to private correspondence. The *Intimsphäre* (intimate sphere) includes protections of one's innermost feelings and thoughts, including protection of sexual privacy as well as privacy of personal diaries. These areas refer to sets of rights developed by the *BVerfG* as various manifestations of the general right to personality.¹¹

The *Population Census Case* was influenced by the early work of prominent German sociologist Niklas Luhmann.¹² A law student who became a social systems theorist in the tradition of Talcott Parsons, Luhmann saw society as differentiated into sub-systems such as the economy, education, religion, etc. He saw the importance of privacy in promoting the consistency of individual identity as it served to reinforce the separation of societal subsystems that are undermined by the uninhibited flow of personal information across spheres, such as from one's personal sexual life or medical history to the workplace.

German legal philosopher Paul Tiedemann has theorized about the social mechanisms at play in this perspective on privacy. His basic premise is that people rely on common understandings of roles when they encounter each other (role-identity) rather than interfacing with the entirety of who they are (personal-identity). People must operate simultaneously across sub-systems and thereby take on societal roles that are sometimes incompatible (for example, as a public official required to treat everyone equally and as a parent expected to put family members first), which Luhmann argued was a hallmark of industrialized societies. Individuals require a certain degree of control over how they are perceived by others because it is through intentionally including or excluding certain features of personality relative to the role being played that they retain the integrity and consistency of their personal identities. In contrast, if an individual is under constant surveillance, it becomes impossible to modify characteristics around various social roles and people can become estranged from themselves—relegated to their purely public personalities—with no residual private identity.¹³

In the *Population Census Case*, *BVerfG* justices noted the potential ill-effects of data collection schemes that provide no individual or societal data privacy:

A social order—and supporting legal order—in which citizens are no longer able to determine who knows what about them, when, through which opportunity, would be incompatible with the right to informational

¹¹ Christoph Degenhart, *DAS ALLGEMEINE PERSÖNLICHKEITSRECHT, Art. 2 I in Verbindung mit Art. 1 I GG.*, 32 JURISTISCHE SCHULUNG 1, § 361–68 (1992).

¹² See Hornung & Schnabel, *supra* note 6 at 85.

¹³ PAUL TIEDEMANN, *MENSCHENWÜRDE ALS RECHTSBEGRIFF* 391 (2007).

self-determination. Whoever is unsure if their dissenting behavior may be recorded at any time and, as information, permanently saved, will try to avoid attracting attention through such behavior. This would impair not only the personal development chances of individuals, but also the public good, as self-determination is a prerequisite for a free democratic polity based on its citizens' capacities of civic action and collaboration.¹⁴

However, control over one's personal data, as guaranteed by this right, is not absolute. The justices reasoned that "the individual does not have a right in the sense of an absolute unlimited control over his or her data . . . Particular limitations of the right to informational self-determination will be accepted when it is overwhelmingly in the collective interest."¹⁵ There are, nevertheless, considerable requirements for attenuations of the right and any laws enabling them. They must have a legitimate legal basis consistent with the principle of proportionality and a high standard of clarity; their purpose must be legitimate, necessary, and tightly-specified. For involuntary measures, "enabling acts" must be area-specific, precise, administratively sound, and include procedural and organizational measures to prevent data abuse.

2. Principle of Proportionality

The legal principles flowing from the questions of when and how informational self-determination can be legitimately attenuated form the cornerstones of German data protection jurisprudence.¹⁶ While intuitively appealing, the principle of proportionality is a slippery legal concept that finds extraordinarily varied articulation from different courts, even across jurists in the same court.¹⁷ At an abstract level this involves a balancing of the intensity and breadth of the rights incursion with the importance and degree of endangerment of the *Rechtsgut* (legally protected interest) to be served by the

¹⁴ Population Census Case, *supra* note 4, at para. 43.

¹⁵ *Id.* at para. 44.

¹⁶ In February 2008, the BVerfG issued the second most significant ruling in the history of German data protection jurisprudence. The *Online-Durchsuchungsurteil* (Online Searching Case) created a new *basic right to the confidentiality and integrity of information technology systems* in response to Nordrhein-Westfalen's enabling the *Bundesamt für Verfassungsschutz* (State Office for the Protection of the Constitution) to secretly remotely search computer hard drives and private networks using Trojan Horses and other hacking tools.

¹⁷ See Bignami, *supra* note 1, at 12.

measure.¹⁸ The enabling act commonly faces a series of corresponding specific assessments. What are all the negative impacts—direct and indirect, obvious and potential, for the individual and society—of the proposed measure? Is the goal of the measure legitimate? Is the measure adequate to achieving its goal? What is the legal status (for example, constitutionally-protected?) of the associated legally protected interest? How essential is the measure's goal to the protection of the legally protected interest? Are there any equally adequate, but less rights-injuring, policy options?

However, the stylized logic behind the balancing analogy falsely suggests that we can always objectively judge when this equation is in proportion. As an absolute scaling of legal interests and rights is impossible - *a priori*, fine-grain proportionality determinations remain difficult.¹⁹ These formulations are most useful for approximate determinations, particularly of cases of egregious disproportionality.

3. Principle of Purpose-Specification

Introduced in the *Population Census Case* is a clarity imperative dictating that infringements of the basic right of informational self-determination are only constitutional when the requirements and extent of the limitations are clearly regulated so that citizens can adjust their behavior accordingly.²⁰ Extrapolated from this imperative is a purpose-specification principle whereby the goal and extent of the data processing must be fundamentally connected to, with clarity in terms of area and precision, a particular applied purpose.²¹ The data in question must also be necessary and appropriate to its assigned purpose.

The census opinion explicitly states that the involuntary “collection and stockpiling of non-anonymized data for unclear or yet-to-be-determined purposes” is incompatible with the principle of purpose-specification.²² Accordingly, the purpose for which data is processed (such as preventative policing, intelligence-gathering by intelligence services, criminal prosecution of past crimes) must be specified at the time of collection and not exceed the

¹⁸ Gerrit Hornung & Christoph Schnabel, *Data protection in Germany II: Recent Decisions on Online-Searching of Computers, Automatic Number Plate Recognition and Data Retention*, 25 *COMPUTER LAW & SECURITY REVIEW* 115, 119 (2009).

¹⁹ Patrick Breyer, *Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR*, 11 *EUROPEAN LAW JOURNAL* 365, 369 (2005).

²⁰ *Population Census Case*, *supra* note 4, at para. 46.

²¹ In German data protection jurisprudence there is also a principle of data minimization whereby no more data than necessary is to achieve the goals associated with a given purpose are processed. This is thought to be derived directly from the principles of proportionality and purpose-specification.

²² *Population Census Case*, *supra* note 4, at para. 45.

minimum necessary to achieve the purpose. Since the category of purpose commonly coincides with the administrative mandate of a particular state agency, the *BVerfG* also introduced through the *Population Census Case* the notion of an “informational separation of powers”²³ in order to preserve the link between the purpose of a rights-infringement and its underlying legal basis. This is an administrative legal concept whereby various state bodies are considered separate data processors requiring separate legal justifications to process the same data. Administrative and procedural structures are required to facilitate parallel but separate data processing.

In 1995 the European Union was still primarily a confederation formed around the enabling of a common market.²⁴ With an eye towards curbing rights abuses by market actors these basic principles of German data protection law were codified in an EU Data Protection Directive.²⁵ The directive included references to certain rights of the data subject, including rights to notification, access, confidentiality and security of processing; these directly corresponded to obligations of the data controller. The directive also contains an exemption clause that lists the purposes that will justify limitations of these rights and obligations. Chief among them are national security, defense, public security, prosecution of crimes, and protection of the data subject or of the rights and freedoms of others.²⁶

II. Vorbeugende Telekommunikationsüberwachung (Preventative Telephonic Surveillance)

Examination of a recent controversial acoustic surveillance case will illustrate legal standards for acts enabling intervention into fundamental private sphere rights. In July 2005, the *BVerfG* issued a judgment on a constitutional complaint brought against a new law enacted by the German state Lower Saxony governing police surveillance powers. State lawmakers, keen to craft legislation that would not run afoul of the *BVerfG*'s interpretation of the basic rights, took the Court's existing jurisprudence into account in the language of the act. Nevertheless, the law fell short in several key areas.

For the twin purposes of hazard prevention and preliminary criminal prosecution, Lower Saxony state police were to use telephonic surveillance on suspects for whom “facts justify the assumption that they will in the future commit crimes of considerable seriousness.”²⁷ Significantly, this does not hinge on facts proving that a crime is about to occur, but facts

²³ Hornung & Schnabel, *supra* note 6, at 87.

²⁴ Bignami, *supra* note 1, at 2.

²⁵ Directive (EC) No. 95/9 of Oct. 24, 1995, 1995 O.J. (L 281/31).

²⁶ *Id.* at art. 13.

²⁷ BVerfGE 113, 348 (para. 8).

supporting the assumption thereof. These methods would also be used on the “contacts or associates” of suspects to the extent that “it is indispensable for crime prevention or preliminary criminal prosecution.”²⁸ The legislation loosely defined “contacts or associates” as “any person, associated with a potential criminal in such a way that creates the expectation that information about the given crime might be obtained from them.”²⁹

True to the title of the act, *Data Retention through Telephonic Surveillance*, police were interested not merely in listening in, but in the real-time digital capture of communication data. This included telecommunications traffic data, all content data of the communication—including data saved remotely within the network, and physical location data for mobile phones.³⁰ Beyond negative societal effects associated with state-sponsored surveillance, the *BVerfG* considered this a strong intrusion upon liberties protected by the Basic Law because data *content* as well as data traffic were in question, because of the large group targeted by the legislation, and because the law created the possibility that data gathered for one state purpose might later be used for others.³¹

Owing primarily to problems of clarity and proportionality the Court ruled that the law was unconstitutional. The justices found that the state legislators had overstepped their official competence in combining the purposes of preliminary criminal prosecution and crime prevention. In accordance with Article 74 of the Basic Law, responsibilities associated with the former are determined during criminal trials. The decision also stipulates that, as a legal purpose, preliminary criminal prosecution must have criteria distinct from *Gefahrenabwehr* (hazard prevention),³² which is legally connected to concrete situations of public danger, and regular criminal prosecution, linked to actual crimes in the past. Preliminary criminal prosecution is anomalous as an evidence-gathering activity taking place before the crime has occurred; the possibility exists that the anticipated crime will never occur. The Court lamented that the purpose-specification did not more explicitly acknowledge this circumstance.³³

The lack of clarity related to the exact definition of the crime and who could qualify as a suspect; this exacerbated purpose and proportionality problems. The blanket justification requiring facts supporting the assumption that someone will commit a crime of

²⁸ *Id.* at para. 9.

²⁹ *Id.* at para. 49.

³⁰ *Id.* at paras. 12–14.

³¹ *Id.* at para. 148.

³² *Gefahrenabwehr* has been a legally recognized police responsibility in the state of Niedersachsen since 1994.

³³ Press Release, German Federal Constitutional Court, no. 68/2005, § 1(b) (Jul. 27, 2005), available at <<http://www.bundesverfassungsgericht.de/en/press/bvg05-068.html>>.

considerable seriousness in the future was not sufficiently clear. What types of serious crime are being considered? What distinguishes harmless behavior from the sort of criminal behavior in question? The justices saw that no real types of behaviors or events were specified, no features signifying a particular crime. The Court expected a delineated planning process with successive points along a continuum, against which a pattern of action could be easily compared and identified as criminal. They found the justification of “crimes of considerable seriousness” unnecessarily unclear and broad, seeing no reason why characteristics of this category of crime could not be specified. The justices regretted the law’s preclusion of a narrow interpretation of the concept.³⁴ Allowing surveillance of third parties without specifying how, when or by whom it is determined that someone meets the broad qualifying criteria for “contacts or associates” also created ambiguity about how easily non-criminals might be targeted. For example, one can easily imagine the possibility that of all the people in a suspected criminal’s mobile call history, only a small fraction of whom may be true accomplices or have information relating to the future crime in question.

Vagueness about how and against whom these invasive surveillance measures would be used as well as about the meaning of “crimes of considerable weight” contributed to the Act’s disproportionality. The Court found the purposes of the data retention, to prevent and prosecute serious crimes, legitimate. According to the Court’s proportionality test, intrusions upon fundamental liberties may not stand in disproportionate relationship to the purposes they serve. Considering the potential breadth and intensity of the intrusion upon basic constitutional rights, the Court found that only for cases in which collective or individual wellbeing were definitively endangered (such as life and physical safety) would this relationship be proportional. However, the *BVerfG* ruled that the Act was disproportionate precisely because the legislation lacked any such legally protected interest specification or restriction.

A final factor supporting the Act’s unconstitutionality was the lack of any measures preventing state incursion into the home. The Court expected at least procedural safeguards to ensure that communication content from this area would not be exploited, but rather deleted immediately after identification.³⁵

C. Development of the EU Data Retention Directive

Passed in March, 2006, through co-decision between the European Parliament and the European Council, the EU Data Retention Directive principally aimed to promote cooperation in criminal prosecution within the EU. It requires CSPs to retain traffic data pertaining to most types of electronic communications (calls, emails, texts, internet

³⁴ *Id.* at § 2(b).

³⁵ *Id.* at § 2(c).

telephony, social networking communications) for a period of six months to two years. This data includes: information necessary to identify the originator and recipient of communications, information identifying the communication equipment used, the time, duration, and date of communications, and real time geographic coordinates of mobile devices during mobile communications. The Directive does not include any content data, such as the body of an email or transcript of a telephone conversation.

While public impetus for stringent security legislation in the West is often linked to mass-casualty terrorist attacks, this Directive was the product of a discrete political and legislative process within the European Institutions driven by the United Kingdom. One month after the bombings of commuter trains in Madrid, the UK government, along with the French, Swedish, and Irish governments, introduced a joint proposal for a draft Framework decision aiming for an EU-wide system of communications data retention. Its purported goal was to facilitate the investigation of terrorism by law enforcement officials.

Aside from the threat of terrorism, which for many member states is not new, this legislation can be contextualized within longer-term legal and technological trends. Designed in the 1980s and 1990s to prevent abuses by market actors, EU data protection laws were ill-suited to guard against overreach or misuse by law enforcement bodies. Significantly, the Data Protection Directive of 1995 does not apply to data processing to preserve public security. CSPs in Europe have long been legally required to erase communication traffic data when it is no longer needed for billing purposes; this is in contrast to the United States where CSPs customarily store traffic data longer for use in marketing. As communications technology has progressed and proliferated, the variety of communications media and data has increased considerably. This trend has been accompanied by an increase in the perceived usefulness of communications data to law enforcement in crime prevention and a decrease in the marginal perceived privacy interest of these data to their creators.³⁶

The Directive's procedural history was characterized by Anglo-German political maneuvering, jockeying between the institutional actors, ambiguity surrounding its nature and subsequently, the most appropriate pathway for its passage.

Initially, a draft Framework decision was brought forward on the basis of Art. 31(1)(c) and 34(2)(b) of the Treaty on the European Union (TEU) as a "third pillar" measure related to Police and Judicial Co-operation in Criminal Matters (PJCC). This legislative process requires a unanimous vote in the Council (in this case, by Ministers of the Interior), entails shared legislative initiative between Council and Commission, requires only Parliamentary consultation, and gives restricted jurisdiction to EU Courts. In the consultation procedure, the high decision standard earns marginal non-Council institutional involvement. This

³⁶ Bignami, *supra* note 1, at 8.

proposal was made while Ireland had the rotating EU Council presidency and included a retention period with a 12 month minimum and a 36 month maximum.

I. Legal Basis

In June 2005, the European Parliament issued a report criticizing the Council's incorrect choice of legal basis, the disproportionality of the proposed legislation, and its potential infringement of Article 8 of the European Convention on Human Rights.³⁷ The report argued that the legislation should be enacted through Article 95 of the Treaties Establishing the European Communities (TEC) pursuant to “first pillar” single-market powers rather than the justice and home affairs powers of the third pillar. While the primary goal was to enhance cooperative law enforcement, operating in multiple member states could potentially become easier for CSPs because of standardized data retention requirements. This plausible single-market effect provided the legal pretext for switching to first-pillar enactment of the measures using the co-decision procedure. The non-Council European Institutions had a strong interest in first-pillar passage because it would assure their involvement as compared to their relative marginalization in the third-pillar process. Under co-decision the EU Parliament has legislative powers of drafting and amendment (shared with the Council), the EU Commission has monopoly power over legislative initiative, and the EU Court of Justice has broader jurisdiction. Consultative bodies also have greater involvement under the more democratic co-decision procedure. The politics of legislative process trumped legal orthodoxy.

However, two other factors contributed to the switch to first-pillar passage, which represented a substantial loss of Council control over legislative process and content. When the United Kingdom assumed presidency of the EU Council in July, 2005, it was admonished by the Council's legal service (CLS) that legal challenges to the framework decision could be successful, which might ultimately bring compensation claims from CSPs.³⁸ Of greater significance, it ostensibly became clear to the British that Germany and Austria would stymie the required Council unanimity. Brigitte Zypries, German Minister of Justice, asserted in her 2007 Bundestag defense of German implementation of the Directive that “the English have done it—*switched from third to first pillar*—in order to orchestrate a qualified majority vote, and thereby thwart the German veto power.”³⁹

³⁷ Judith Rauhofer, *Just Because You're Paranoid, Doesn't Mean They're Not After You: Legislative Developments in Relation to the Mandatory Retention of Communications Data in the European Union*, 3 SCRIPTED 322, 333 (2006).

³⁸ *Id.* at 334.

³⁹ Minutes of the 124th Session of the German Federal Parliament, 9 November 2007, page 12995, available at <http://www.bundestag.de/dokumente/protokolle/amtlicheprotokolle/2007/ap16124.html> (emphasis added).

II. Data Protection Consultation

The co-decision process was riven with controversy over key provisions of the law. The two main consultative bodies, the Data Protection Working Party ("Working Party"), and the European Data Protection Supervisor ("Supervisor"), aligned with the European Parliament in opposing Commission and the Council positions. A group of national data protection officials established in 1995 to implement the Data Protection Directive, the Working Party had a formal right of consultation that the Data Protection Supervisor lacked. Although the Supervisor's regulatory purview was limited to the use of personal data by the European Community institutions, an opinion was requested by the Commission.

The Supervisor and the Working Party excoriated the first draft of the directive and had reservations about the final version. They based their privacy analysis primarily on Article 8 of the European Convention on Human Rights (ECHR) and data-protection principles in the Council of Europe Convention 108 ("Convention 108").⁴⁰ Influenced by German data protection principles, Convention 108 stipulates that data retained must be necessary and adequate to the stated purpose, accurate and up to date. Further, the amount of data and the retention duration should be the minimum necessary.⁴¹ They found that the Directive met many of the basic necessary conditions. It would be performed by a public authority for a legitimate public purpose.⁴² It would have measures to prevent arbitrary government intrusions. However, they were consistently skeptical of its proportionality. Fundamental questions remained unanswered. Had it been demonstrated that this rights-intrusion was essential to the stated purpose? Would a less invasive alternative work? Was this degree of privacy intervention justified by the public purpose and the usefulness of these data to this purpose?

The data protection watchdogs had the ear of the EU Parliament and influenced their version of the bill as it passed through the co-decision process for reconciliation of the Council and Parliament versions. The most disputed details were the question of regulating police access, the question who would bear the cost burden, the precise purpose specification, the duration and the amount of data retained (key to the proportionality test), and the question whether data should be retained for unsuccessful call attempts.

⁴⁰ Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108.

⁴¹ Bignami, *supra* note 1, at 15.

⁴² See Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 5 E.T.S. 8 (specifying that the right to a private life should not be interfered with except as is necessary in the interests of national security, public safety, economic well-being of the country, prevention of disorder or crime, protection of health or morals, or protection of rights and freedoms of others).

Alexander Alvaro, MEP and prominent member of the German Free-Market Democrats (FDP), was appointed rapporteur for the Parliament's Committee on Civil Liberties, Justice, and Home Affairs. He was the point person for synthesizing, reconciling, and publishing the positions of his Parliamentary Committee, the Working Party, and the Supervisor. His report, adopted by committee on 24 November 2005, proposed EU member state subsidiarity for determination of retention duration (within 6–12 months) and whether to retain data on unsuccessful call attempts. The report called for eliminating voice IP and email data from retention categories and pushed for data access to be subject to “judicial approval” and permitted only for “specified, explicit, and legitimate purposes by competent national authorities.”⁴³ It took the politically controversial position that CSPs should be reimbursed for all “demonstrated additional costs” of legislative implementation, data protection, and access provision.

III. Final Terms

As the legislation traveled through the co-decision process, its specified purpose was gradually sharpened by the Commission and EU Parliament. The mandate of enabling investigation, prevention, and prosecution of all types of criminal activity was limited in the Commission proposal to “serious crime” and “prevention” was removed during reconciliation between the Council Presidency and the Parliament, replaced with the term “detection”. This was in direct response to the Working Party’s criticism that the rights burden of retention was disproportionately heavy relative to the importance of prosecuting crimes that had not yet occurred. They were mindful that preventative surveillance often provides justification for so-called government “fishing” expeditions, whereby law enforcement mines data or eavesdrops without probable cause or warrant until evidence of illegal activity is found.⁴⁴

While the Council had initially pushed for a retention period of up to three 3 years and the Parliament plus watchdogs wanted 6 months to 1 year, the final version contained a compromise with member states determining retention duration within the range of 6 to 24 months.

Maintaining the threat of framework decision passage as leverage, the UK Council presidency insisted that member states not be required to compensate CSPs, that traffic data for all types (including real time location data for mobile telephony, voice IP, email, and social networking traffic) of electronic communication be covered for the original six categories of data, that unsuccessful call attempts be retained, and that any clauses conditioning law enforcement access to retained data be stricken—leaving it for member

⁴³ Rauhofer, *supra* note 37, at 337.

⁴⁴ Bignami, *supra* note 1, at 21.

states to determine through national law.⁴⁵ The final text contained these provisions. Another triumph for the Council presidency was the speed of passage. Taking about two and half months from Directive adoption to Parliamentary approval, it remains one of the fastest-legislated co-decision directives in the history of the European Union.⁴⁶

D. German Implementation and Challenges

I. Transposition

In June, 2007, the German CDU-SPD coalition government drafted the federal law, *Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG* (GNTR - draft law newly regulating telephonic surveillance and other covert investigation measures as well as transposition of Directive 2006/24/EC).⁴⁷ The law implemented parallel changes to the *Strafprozessordnung* (StPO - Federal Code of Criminal Procedure) and the *Telekommunikationsüberwachungsgesetz* (TKG - Federal Telephonic Surveillance Law). It exceeded the legislative requirements of the Directive in several respects. The coalition cabinet considerably broadened the *Zweckbindung* (purpose specification) in their changes to the TKG, adding *prevention of public security hazards* and the *execution of covert agencies' legal duties* to the Directive-stipulated purposes for which the retained data could be processed.⁴⁸

Through changes to the *StPO*, the law broadened the *Zugriffsermächtigung* (Access Authorization) regulating the release of retained data to non-intelligence law enforcement by CSPs. In place of the Directive-stipulated "serious crimes" condition, law enforcement would have access to the data "if facts justify the suspicion that someone has committed a *crime of considerable seriousness* or a *crime using telecommunications*"⁴⁹ (emphasis added). Notably, the "crimes of considerable seriousness" can fall outside the indictable offenses long-established in the *StPO*, interpreted as offenses with a minimum sentence length of at least five years for a conviction.⁵⁰ For a "*crime using telecommunications*,"

⁴⁵ Rauhofer, *supra* note 37, at 338.

⁴⁶ *Id.* at 336.

⁴⁷ See, *supra* note 39, at 12993.

⁴⁸ Telekommunikationsüberwachungsgesetz (TKG- Telecommunications Surveillance Act), Jul. 25, 1996, BGBI. I at 1120, last amended by Sixth Law Amending the Law against Restraints of Competition, Aug. 26, 1998, BGBI. I at 2544, chap. 113B, §§ 2–3 (hereinafter TKG).

⁴⁹ Strafprozessordnung (StPO- Federal Code of Criminal Procedure), Feb. 1, 1877, RGBI. I at 253, chap. 100G, §§ 1–2 (hereinafter StPO).

⁵⁰ See StPO, chap. 100A, § 2 (including subsidy fraud, treason, endangering public security, counterfeiting, sexual crimes, murder, manslaughter, money laundering, among others).

access to retained data could be justified for any crime involving telecommunications provided “investigating the issue or determination of the guilty party’s location would otherwise be unpromising.”⁵¹ Furthermore, state access to sensitive data of *any third party* was permitted when it is deemed “unavoidable on of technical grounds.”⁵² These access standards were sufficiently broad and loose such that, in practice, factually-based suspicion of *any* non-petty crime could meet the criteria. This is considerably different from the EU Directive’s language specifying retention purposes of “*Ermittlung, Feststellung und Verfolgung von schweren Straftaten*,” (investigation, determination, and prosecution of serious crimes).

The GNTR also set broad access standards for the retained data. Four main groups of actors—state prosecutors, the police, the German federal intelligence agencies, and foreign intelligence agencies—would have access to all the retained data points. Access to primary identity information (name, date of birth, address, etc.) of telecommunications and email users is provided via automated electronic request to *any* government office with a possible data interest, such as customs, the office against illicit employment, parking and municipal agencies. There was no indication that these agencies’ access would be conditioned upon demonstrating the legitimacy of their data interest relative to their mandates. The only state purpose for which a judicial warrant was required was criminal prosecution, but the requirement could be skirted in exigent circumstances or obtained afterward.⁵³ Domestic and foreign intelligence services, including the German equivalent of the FBI, required no court approval whatsoever.

II. Bundestag Challenges

Parliamentary debate on the GNTR featured vehement but ineffectual political challenges from party factions outside the Grand Coalition (CDU/CSU and SPD). While stridently condemning the law, these parliamentarians lacked the votes to block it. Jörg van Essen of the FDP stood resolutely against the GNTR, asserting that it overstepped the transposition requirements, particularly in the broadening of the purpose specification, and charged that the law would put German society under general suspicion without any legitimate cause. He condemned it as an “unambiguous violation of the right to informational self-determination.”⁵⁴ Jan Korte of *die Linke* and Jerzy Montag of the Greens also underscored

51 Rotraud Gitter & Christoph Schnabel, *Die Richtlinie zur Vorratsspeicherung und ihre Umsetzung in das Nationale Recht*, 7 MULTIMEDIA UND RECHT 411, 416 (2007).

52 StPO, chap. 100I, § 2.

53 *Pressemappe zum Pressegespräch über die Verhandlung des BVerfGs über die Vorratsdatenspeicherung*, ARBEITSKREIS VORRATSDATENSPEICHERUNG, available at <<http://www.vorratsdatenspeicherung.de/content/view/51/70/lang,de/>>.

54 See, *supra* note 39, at 12996.

the claim that the legislation overstepped the Directive's requirements and hinted at potential nullification by the *BVerfG*.⁵⁵

Meanwhile, Brigitte Zypries of the SPD, also the Justice Minister, and Siegfried Kauder of the CDU/CSU emphasized that the data would be saved by CSPs, not the government, and released to police or public prosecutors in instances of real criminality and with the consent of a judge. They asserted that preservation of national security was ample justification for the rights intrusions resulting from data retention.

The same day as the Bundestag's deliberations, prominent FDP parliamentarian and former Justice Minister Sabine Leutheusser-Schnarrenberger denounced the Directive in a newspaper interview as "Introducing a dangerous paradigm shift in Data Protection."⁵⁶ When asked whether conditioning release of retained data on court order sufficiently fulfilled constitutional requirements, she countered that the right to informational self-determination does not only apply at the point of data release to authorities but that the retention of society's sensitive information constitutes rights infringements unto itself. Therefore, she asserted, the state must clearly delineate on what grounds and for what purposes the data of its citizens is to be retained, saved, processed, and used in criminal investigations or prosecutions.

III. Popular Challenges

German implementation of the EU Data Retention Directive also faced considerable popular challenges. Segments of German media and society received the measure with skepticism, but the vanguard of an emergent anti-retention movement consisted of highly-networked civil and digital rights activists, ideologically-heterogeneous students and academics, and German or European NGOs.

On 31 December 2007, two months after the CDU-SPD lead Bundestag approved the measure, newly-formed privacy NGO *Arbeitskreis Vorratsdatenspeicherung* (Working Group on Data Retention) filed a formal constitutional complaint with the *BVerfG* in Karlsruhe with an unprecedented 34,000 complainants.⁵⁷ The demands of this group included a cutback on many types of surveillance, independent evaluation of the usefulness and harmful impacts of existing surveillance powers, moratorium on new surveillance powers, and new legal guarantees of freedom of electronic information

⁵⁵ *Id.*

⁵⁶ Sabine Leutheusser-Schnarrenberger, *Damit wird ein Paradigmenwechsel eingeleitet*, BERLINER ZEITUNG, Nov. 9 2007.

⁵⁷ As German procedural law does not recognize class-action lawsuits, these were considered as 34,000 separate suits.

exchange and communication. From 2006 to 2009 the group organized ten peaceful demonstrations under the banner of “*Freiheit statt Angst*” (Freedom instead of Fear) in cities across Germany with accumulative participants numbering in the several hundred thousands. The most recent demonstration involved a partnership of 167 civic groups and 25,000 people marching through the borough of Mitte, Berlin.⁵⁸

The success of German groups in raising public awareness of a highly-technical topic, publicizing their rarely-at-odds messages, and organizing successful demonstrations and legal actions can be attributed to an extraordinarily effective use of new networked media to convey resources, ideas, and people around Germany and Europe. German activists organizing around data retention, savvy to their work's supranational legal and civic context, also partnered with such groups as European Digital Rights (Brussels-based NGO), the Electronic Privacy Information Center (US-based NGO), and Destapa el Control (Madrid-based anti-surveillance NGO), among others.

On 11 March 2008, the *BVerfG*, responding to the constitutional complaint, issued a rare temporary injunction allowing communications data to be retained and saved by CSPs, but prohibiting release to law enforcement bodies.⁵⁹ The Court was to use this time to examine and rule on the constitutionality of the GNTR.⁶⁰ This injunction was initially made for a period of six months, but was later renewed. Adding support to NGO claims, in March, 2009, an administrative court in Wiesbaden offered an opinion calling the new data retention law “*ungültig*” (invalid) because it was inconsistent with the proportionality principle.⁶¹ Members of German legal academia subsequently offered similar public opinion statements against the Directive.

Meanwhile, contrary to expectations of German jurists, the Data Retention Directive survived a serious international legal challenge from Ireland. Arguing the Directive should have been based upon Articles 30, 31(1)(c) and 34(2)(b) of the TEU's Title VI (third pillar), rather than Article 95 of the TEC (first pillar), Ireland filed a motion to nullify the Directive

58 Prominent speakers included Rolf Gössner, civil rights activist and lawyer, Dr. Patrick Breyer, jurist and author of the constitutional complaint representing *Arbeitskreis Vorratsdatenspeicherung*, Dr. Hans-Jörg Kreowski, representing the forum of computer scientists for peace and social responsibility, and Dr. Ralf Bendrath, political scientist and well-known blogger.

59 In determining whether to issue an injunction, the court weighs the public interest in the operation of the law's various provisions versus possible negative effects of allowing the provisions to be immediately implemented in the event that the constitutional complaint is well-founded. The *duty of storage* provision was immediately implemented and the *data release* provision suspended because the court linked harmful prejudice to the rights of specific individuals to the latter.

60 BVerfGE 121, 1.

61 Verwaltungsgericht Wiesbaden [VG- administrative court], Case No. 6 K 1045/08.WI, Feb. 27, 2009.

with the European Court of Justice (ECJ).⁶² In February, 2009, with prompting from Advocate General Ives Bot, the ECJ dismissed Ireland's motion—ruling that the Directive was correctly passed pursuant to the internal market EC provisions, and remained valid and binding EU law.⁶³

E. German Constitutional Rights and the GNTR

I. Constitutional-Rights Burden

The burden the GNTR places on rights protected by the German Basic Law fall into three main categories: violations of the privacy of telecommunications, incursions into the right to informational self-determination, and infringement of the professional and competition rights of CSPs.

1. Confidentiality of Telecommunications

Protected by Article 10 of the Basic Law, the *Telekommunikationsgeheimnis* (Right to Confidentiality of Telecommunications)⁶⁴ is heavily burdened by the GNTR. Retention of traffic and location data enables construction of comprehensive mobility and communication profiles for every user of electronic communications technologies. That content data is withheld does not mitigate the rights burden. Each and every person using communications technologies within Germany is treated as a potential criminal suspect. This is particularly problematic for certain professions, such as journalism, medicine, politics, law, or emergency hotlines that involve confidential communication. The *BVerfG* has ruled that communication traffic data ceases to be protected under the Right to Confidentiality of Telecommunications after the communication takes place.⁶⁵ However, this data is then protected by the communicator's right to informational self-determination.

⁶² Case C-301/06, *Ireland v. European Parliament and Council of the European Union*, 2009 E.C.R. I-82, paras. 4–5.

⁶³ Press Release, European Court of Justice, No. 70/08 (Oct. 14, 2008), available at <<http://curia.europa.eu/en/actu/communiqués/cp08/aff/cp080070en.pdf>>.

⁶⁴ See Basic Law at art. 10, paras. 1–2 (“(1) The privacy of correspondence, posts and telecommunications shall be inviolable. (2) Restrictions may be ordered only pursuant to a law.”)

⁶⁵ Press Release, German Federal Constitutional Court, no. 79/2009 (Jul. 15 2009), *Sicherstellung und Beschlagnahme von E-Mails auf dem Mailserver des Providers nicht verfassungswidrig*, available at <<http://www.BVerfG.de/pressemitteilungen/BVerfG09-079.html>>.

2. Informational Self-Determination

The GNTR severely burdens the right to informational self-determination in terms of scope of application as well as comprehensiveness of information retained. If someone is regularly using electronic communications means, which today represents a large segment of the national and European population, then a detailed mapping of their social world is possible. For *any* mobile user, state agents will have close at hand a range of information, including who they call, when, with which device, and from exactly where, or who sent an email to whom and when. It is a misrepresentation to suggest that content information is indiscernible from such traffic. To illustrate how content can be gleaned from traffic data, consider a mobile user who calls an HIV treatment clinic four times in one day or someone who communicates at regular intervals with a psychiatrist's office. Moreover, any scheme of society-wide data retention unavoidably infringes the right of informational self-determination.

3. Fair Compensation for Property Loss

Article 12 of the Federal Constitution protects the right to choose and freely practice a profession but allows professional practice to be legally regulated.⁶⁶ Together with Article 14 protecting private property,⁶⁷ this provides the underlying constitutional basis for the freedom of CSPs to provide their services and their right to fair compensation for property loss associated with GNTR implementation.

It is reasonable to expect some near-term property loss for firms whose servers and other data retention hardware and/or software must be upgraded to accommodate the increased volumes and varieties of data that the Directive obliges them to retain. However, intrusions upon CSP professional rights may be constitutionally permissible *in the service of public welfare* when appropriate, required, and proportional (relative to incursion goals) and so long as retention will not be excessively burdensome or costly to CSPs operating in Germany.⁶⁸ Entrusting private entities with public duties is not, in itself, constitutionally problematic,⁶⁹ nor does it require public reimbursement for private expenses.

66 See Basic Law at art. 12, para. 1 ("All Germans have the right to freely choose their occupation, work place, and training institution. The practice of their occupation can be regulated through law or because of law.")

67 See *id.* at art. 14, paras. 1–3 ("(1) Property and the right of inheritance shall be guaranteed. Their content and limits shall be defined by the laws. (2) Property entails obligations. Its use shall also serve the public good. (3) Expropriation shall only be permissible for the public good . . .").

68 Data Retention Case, *supra* note 4, at para. 301.

69 The constitution does not contain a categorical division between private and public tasks yielding the disallowance of private performance of state obligations - at private-sector cost - in service of public welfare purposes.

While it is difficult to measure expected implementation costs, one estimate places industry-wide costs in the UK alone at €150 million.⁷⁰ Clear signals were sent to the CSPs during Directive drafting that they should pass on any losses to their consumers in the form of higher rates rather than seek government compensation, and that since this would become EU law, no individual firms would be disproportionately impacted.⁷¹ This is inconsistent with German property protections and the possibility that intra-EU variation in Directive transposition creates disproportionate cost burdens for different CSPs.

II. Clarity Shortcomings of the GNTR

Assessed by standards of German constitutional jurisprudence, the GNTR has major clarity shortcomings. These surround purpose and crime specification. According to the principle of purpose-specification, the goal and extent of data retention or processing must be fundamentally bound and limited to a specific applied purpose. Any retention program where the justification for retention can only be determined in contingency runs afoul of the clarity imperative. In this case we have diffuse linkage from the saving of users' data, to release of data from CSPs to government bodies for at least⁷² three purposes: criminal prosecution, hazard prevention, and fulfillment of covert agencies' mandates. These purposes are all legitimate. At issue, however, is the specification of their legal triggers and their relationship to the retention and processing of sensitive data.

It is insufficiently clear whether the measures detailed in the GNTR are necessary and adequate to achieve their goals. A paucity of empirical evidence on the usefulness to law enforcement bodies of telecommunications traffic data, not already retained by CSPs for commercial or billing purposes, in preventing "hazards" and prosecuting "crimes" makes strong cases for its indispensability difficult. Extant empirical information suggests traffic data is sufficiently available to state bodies. It is currently customary for German and European CSPs to save communications data for a period of six months for billing. Traffic data available without state-mandated retention, was famously used in the prosecution of the notorious Madrid bombings of 2004.

The Max-Planck Institute, a non-partisan German research center, carried out a study in 2008 to estimate the share of criminal cases in which traffic data had been requested by German authorities but had already been deleted by CSPs. Of a sample of 467 criminal

⁷⁰ Hans-Jörg Albrecht et. al, *Rechtswirklichkeit der Auskunftserteilung über Telecommunicationsverbindungsdaten nach chapter 100g, 100h StPO*, Max-Planck-Institute for Foreign and International Criminal Law, 2008, at n. 394, available at <<http://www.vorratsdatenspeicherung.de/images/mpi-gutachten.pdf>>.

⁷¹ Rauhofer, *supra* note 37, at 335.

⁷² Data may be given to foreign security agencies without any binding condition on its use.

cases from 2003 and 2004 in which 1,257 traffic data requests had been made, they found a rate of unsuccessful data requests of around 4%. In 2005, 40,000 telecommunications data requests were made, indicating existing heavy law enforcement demand for traffic data. An estimated 600 of the approx. 15,000 criminal cases⁷³ for which data was requested in that year involved failed requests. This would represent only 0.01% of the 4.9 million criminal investigations nationwide in 2005.⁷⁴ This suggests that, for 99.99% of annual criminal investigations, a so-called “quick freeze” process⁷⁵ might be a viable alternative using data currently available. According to a parallel 2005 analysis by the *Bundeskriminalamt* (Federal Office of Criminal Investigation), in that year there were only 381 cases nationwide—0.001% of the 6.4 million annual crimes in Germany—in which unavailable data was requested from CSPs.⁷⁶ The vast majority of these cases were not felonies but were minor cases of fraud.

It is also insufficiently clear what constitutes the “crimes and hazards” warranting data processing. German legislators chose not to adopt or augment the established listing of serious criminal offenses⁷⁷ while failing to specify crimes by class/type or provide any characteristics of the crimes in question. The GNTR should enumerate “crimes and hazards,” or provide concrete processes with recognizable steps distinguishing the criminal or suspicious behaviors warranting surveillance. These standards should also be public and transparent so that citizens can adjust their behavior to avoid becoming surveillance targets. With an eye toward subsidiarity, this degree of ambiguity in the enabling act might be excusable at the level of EU law, but for German national law this fails to satisfy the clarity imperative while contributing to the measure's disproportionality.

In contrast to criminal prosecution, which—relative to crime commission—is an ex-post infringement of rights to informational self-determination and communications privacy, hazard prevention and fulfillment of covert agencies' mandates are ex-anti⁷⁸, raising the rights' burden and the public interest in precise specification of “hazards”. The preventative purposes, while legitimate, overstep the mandate of the EU Directive. Since

⁷³ Using the sample ratio of 2.7 data requests per case and 4% sample failed request rate.

⁷⁴ Hans-Jörg Albrecht et. al, *Rechtswirklichkeit der Auskunftserteilung über Telecommunicationsverbindungsdaten nach chapter 100g, 100h StPO*, MAX-PLANCK-INSTITUTE FOR FOREIGN AND INTERNATIONAL CRIMINAL LAW: KRIMINOLOGISCHE FORSCHUNGSBERICHTE [REPORTS ON RESEARCH IN CRIMINOLOGY] (February 2008), available at <<http://www.vorratsdatenspeicherung.de/images/mpi-gutachten.pdf>>.

⁷⁵ Process whereby all traffic data associated with certain user(s)/IP addresses/number(s) are immediately retained following court order, on a case-by-case basis.

⁷⁶ Gitter & Schnabel, *supra* note 51, at 414.

⁷⁷ *StPO* § 100a, para. 2.

⁷⁸ In cases where the preparation activities are not criminal themselves.

these purposes are coupled with particular federal agencies, legislators should provide procedure-specific elements of offenses, consistent with agencies' mandates, which set standards of foreseeability and preventability.⁷⁹

II. Proportionality Shortcomings of the GNTR

When explaining in the interim injunction why the duty of storage was not suspended, the *BVerfG* noted that comprehensive retention of every German's sensitive data might have an intimidating affect on electronic communication. However, they asserted prejudice to individual freedoms deepen and become specific following data release from CSPs. This dovetails with Coalition politicians' defense that data processing following release—not merely mandating CSP retention—constitutes surveillance. Therefore, they argue, retention itself is not the dystopian caricature of nationwide surveillance its critics charge. And anyway, can't surveillance be justified in the service of other legal interests? Isn't the preservation of national security sufficient legal justification for the rights' burden of retention? Aren't the purposes which the GNTR serves legitimate state concerns?

While it is reasonable to think the most rights-injurious consequences of the retention program would follow processing rather than retention, the GNTR is nevertheless disproportionate. A 2003 *BVerfG* ruling on police locating outstanding fugitives through traffic data from mobiles they used during press interviews stated:

[I]n this respect it does not satisfy constitutional requirements that the capture of connection data serve the general interests of criminal prosecution, much more required are a *crime of considerable weight*, a *concrete criminal suspicion*, and a *sufficiently firm factual basis*.⁸⁰ (emphasis added)

These legal prerequisites, corresponding to their state purpose, must be met prior to retention because data capture is conditional upon them. Consequentialist justifications using legally protected interests like national security may be ostensibly compelling, but are no substitute. Retention apologists might rejoin that these requirements are fulfilled because the *crime of considerable weight* language is in the GNTR Access Authorization. This is false. Access conditions were substantially broadened beyond Directive stipulations. The GNTR retains all data before establishing *any* of the above elements and in preventative circumstances the retained data is processed while the crime itself is contingent. Based on the factual circumstances of a case, authorities must suspect with

⁷⁹ Gitter & Schnabel, *supra* note 51, at 414.

⁸⁰ BVerfGE 107, 299 (para. 75).

sufficient probability, that someone has carried out a concrete crime of considerable weight, *before* her telecommunications traffic data are *retained* and *processed*.⁸¹

Retention is a rights-burdening act in itself. For most Germans, whose data are retained but not processed by authorities, this represents a wide but shallow incursion with a constant risk of processing. For Germans whose data is retained and processed, this represents the burden of retention plus the personal rights incursion with potential for irrevocable impact on one's private and public life. This occurs with the ever-present possibility that the incursion is not connected to the occurrence of any criminal act.

The clarity failings of the law transposing the EU Data Retention Directive worsen its proportionality problems. As stated in the *vorbeugende Telefonüberwachung* (Preventive Telephone Surveillance) ruling, the depth and breadth of the Right to Confidentiality of Telecommunications and *Recht auf Informationelle Selbstbestimmung* (Right to Informational Self-Determination) infringement associated with mass preventative surveillance is such that a limitation to legally protected interests of overwhelming public interest is necessary for surveillance to be proportional.⁸² The GNTR, and the Directive itself, lack any characterization of the legally-protected interests “crimes” and “hazards” might threaten, let alone a binding restriction conditioning data release and processing on the protection of legally protected interests of considerable public concern.⁸³

A second factor contributing to the GNTR's disproportionality is its lack of any provisions recognizing the legal protections of the private and intimate spheres of human life, particularly traffic associated with home communications or communications of inner feelings. Considering the ease with which data traffic can betray data content in conjunction with the legal sanctity of the home, it is technologically feasible and legally prudent to require these sorts of highly sensitive data be deleted immediately after a determination of its intelligence value is made.

F. Implications of the *BVerfG*'s March 2010 Ruling

On 2 March 2010, on the eve of this article's publication, the *BVerfG* announced its long-awaited decision on the *Verfassungsbeschwerde* challenging Germany's statutory scheme implementing the European Directive. The Court's President, Hans-Jürgen Papier, called the ruling “one of the most important of my tenure.”⁸⁴ The *BVerfG* nullified the GNTR and

⁸¹ *Id.* at para. 77.

⁸² Gitter & Schnabel, *supra* note 51, at 416.

⁸³ Considered the most significant of the individual legally protected interests are life, freedom, and bodily health. Universal legally protected interests are legally protected interests assigned the state rather than persons. The weightiest include public security, rule of law, and functional administration of justice.

⁸⁴ Hans-Jürgen Papier, *Gegen die Totalkontrolle*, SÜDDEUTSCHE ZEITUNG, Mar. 3 2010.

ordered data retained under the interim ruling deleted.⁸⁵ The Court found that the GNTR imposed “an especially heavy rights burden...with a dispersion, as yet unseen in our legal system.”⁸⁶ It reached this conclusion in part because the law enables the “production of very expressive personality and mobility profiles for practically every person.”⁸⁷ The Court found the GNTR lacking in data security measures, clearly delimited data applications, transparency, and legal protections. The result was that the Court found the law to be disproportionate and unconstitutional. While largely congruent with the Part E analysis above, the ruling contained stronger-than-anticipated emphases on data security and transparency.

Citing the limited incentives for private telecommunications firms to ensure the security of retained data and the “high danger of illegal access” (given the information value of the data and the breadth of retention, it would be attractive to criminals), the Court found that GNTR requires an especially high level of data security.⁸⁸ Also setting a high standard of transparency, the Court required that notification be made to the data subject when retained data is processed. Data processing without the knowledge of data subjects can only be constitutional, the Court explained, when the purpose of processing is disclosed; secret processing is only to be permitted when the specific case requires it, and then a court order is needed and notification of processing must be made after the fact.⁸⁹ Further, the Court held that release and processing of retained data fundamentally must be under judicial oversight.⁹⁰ When individuals lose the opportunity to stand in their own defense against the processing of their data, they must be offered judicial review after the fact. A proportional form of the GTNR, the Court explained, also would contain effective sanctions against rights abuses.⁹¹

The *BVerfG* set an explicit restriction on purposes of data processing, requiring that they serve “especially high-order concerns of public welfare...to prosecute crimes that threaten these overwhelmingly important interests or avert threats to them.”⁹² Criminal

85 Press Release, German Federal Constitutional Court, no. 11/2010 (Mar. 2 2010), *Konkrete Ausgestaltung der Vorratsdatenspeicherung nicht verfassungsgemäß*, available at <<http://www.bverfg.de/pressemitteilungen/bvg10-011.html>>.

86 Data Retention Case, *supra* note 3 at para. 210.

87 Data Retention Case, *supra* note 3 at para. 211.

88 Data Retention Case, *supra* note 3, at para. 222.

89 Data Retention Case, *supra* note 3, at para. 243.

90 The requests for determination of IP-address are exempted from this. These requests nonetheless require criminal suspicion or concrete danger for specific cases.

91 Data Retention Case, *supra* note 3, at para. 252.

92 Data Retention Case, *supra* note 3, at para. 227.

prosecution requires factually based suspicion of commission of a serious crime. The Court explained that the legislature has flexibility to define the elements of the crimes, using established or new catalogs. However, the qualification of crimes as “serious” must find objective expression as a general clause or references to “crimes of considerable meaning” will be regarded as insufficient.⁹³ The ruling criticized expansion of prosecutorial purposes to any crime “using telecommunications” as trivializing the intended exceptional nature of data processing.⁹⁴

For the prevention of threats, the Court ruled that data may be processed to avert danger to physical safety, life, or liberty of persons, for security of the federal or state governments, or to avert considerable public danger. However, definite facts must be determined that “carry the prognosis of a concrete danger.”⁹⁵ The probability must exist that, without state intervention, certain persons will harm legally protected interests. Moreover, the constitutional requirements for the purpose of preventing threats apply for all preventive purposes, including those of the intelligence agencies.⁹⁶

The Court found no constitutional violation in requiring CSPs to implement data retention at their own cost. The justices asserted the proportionality of the intrusion upon CSP professional rights based on the legitimacy of the public welfare goals of the legislation, the argument that CSPs themselves are the most appropriate implementers because of the heterogeneity of data practices across firms, in light of the fact that these data are so intimately connected their business, the assertion that implementation costs will be incorporated across the industry into pricing schemes leaving no individual firm at a disadvantage, and the lack of evidence suggesting exorbitant cost burdens for providers.⁹⁷ Nonetheless, the Court accepted the possibility that a group of CSPs, particularly small Internet service providers, face excessive cost burdens upon future implementation. Reimbursing CSPs for “demonstrated additional costs” of implementation would not only address this concern, the Court explained, but would bolster private incentive to maintain the necessary high standard of data security.

93 Data Retention Case, *supra* note 3, at para. 228.

94 Data Retention Case, *supra* note 3, at para. 279.

95 Data Retention Case, *supra* note 3, at para. 231.

96 Data Retention Case, *supra* note 3, at para. 232.

97 The bar for disproportionality here is that a group of market actors - not individual firms - faces cost burdens in violation of the *Übermaßverbot* (prohibition of excessive cost); Oil Reservation Case, BverfGE 1 BvR 52,665,667,754/66 (para. 316).

What was the balance of the decision? In the so-called *Solange II* (as-long-as II) decision of 1986, the *BVerfG* reaffirmed an established practice whereby it accepted the basic rights protections of the European Institutions—particularly the ECJ—as consistent with its own standards and declined to test EU law for basic rights compliance.⁹⁸ Reducing threats to the legal integration of the Europe Union, this narrowed the admissibility of constitutional complaints against EU law in Germany. The *BVerfG* might have continued to honor *Solange II* precedent and not stood in the way of the implementation of European Law through the GNTR, which was nonetheless unconstitutional by standards of German jurisprudence. This would have been a boon for German security hawks as they would have gained a back-door method of passing legislation that Germany's Constitutional Court otherwise would nullify.⁹⁹ The *BVerfG* also could have diverged from *Solange II* and ruled that the ECJ no longer adequately protects basic liberties consistent with German law or issued a blanket retention ban, and reasserted its own jurisdiction. Divergence would have presented a supranational legal crisis with adverse impact on European Union integration.

However, the Court found a middle path whereby the Directive-mandated portion of the law was left unchallenged, but the portions of the German implementation legislation that exceeded the terms of the Directive were nullified until brought in line with German constitutional requirements. It continued to honor *Solange II* precedent, maintaining the layered integrity of European legal development.

This landmark ruling made clear that a mass retention scheme was not -in principle- unconstitutional, rather the particular formulation of the regime under the GNTR failed to meet constitutional requirements to make its considerable rights burden proportionate. The justices clearly laid out the jurisprudential requirements for proportionality while also underscoring the degrees of legislative flexibility within standards. Although the decision studiously avoided any comment on the validity of the EU Directive itself, it highlighted that the conclusion that the “exercise of civil freedoms cannot be totally recorded belongs to the German constitutional identity, which Germany must seek to preserve in European and international contexts.”¹⁰⁰

Significantly, justices Schluckebier and Eichberger, both affiliated with the CDU, dissented from the majority opinion primarily because they thought the rights burden of retention was not as severe as the majority.¹⁰¹ Rather than outright nullification, four of the eight justices favored a transitional period during which retention could be suspended while the

98 BVerfGE 73, 339 (para. 4).

99 Hornung & Schnabel, *supra* note 18, at 122.

100 Data Retention Case, *supra* note 3, at para. 218.

101 Data Retention Case, *supra* note 3, at para. 337.

law was repackaged by the *Bundestag*. That the Court ultimately chose instant deletion plus the definitive restriction to serving legally protected interests of the highest order for criminal prosecution and preventative purposes indicates renewed vigor in the *BVerfG*'s defense of the Basic Law in the area of domestic security surveillance and civil freedoms.

Some analysts, however, see this decision as an attempt by the *BVerfG* to forestall an inevitable conflict with the ECJ.¹⁰² To the contrary, immediately following the Constitutional Court's decision, EU Interior Commissioner Cecilia Malmström announced a review of EU Data Retention Directive by year's end to determine its proportionality, effectiveness, costs, and compatibility with the Lisbon Treaty's charter of fundamental rights.¹⁰³ Directive rescission may yet be in store.

102 Heribert Prantl, *Arresting the Cyber Police*, SÜDDEUTSCHE ZEITUNG, Mar. 3 2010 Available at <<http://www.presseurop.eu/en/content/article/202721-arresting-cyber-police>>.

103 Stephanie Bolzan, *EU-Richtlinie zur Datenspeicherung wird überprüft*, DIE WELT, Available at: <<http://www.welt.de/politik/ausland/article6642536/EU-Richtlinie-zur-Datenspeicherung-wird-ueberprueft.html>>.

