The Untold Story of Edward Snowden's Impact on the GDPR

Hallie Coyne

INTRODUCTION

In June 2013, National Security Agency contractor Edward Snowden released a trove of information on classified U.S. Government surveillance methods. U.S. Intelligence chiefs warned that the ripple effects of the leak would be devastating and extensive. Five years later, in June 2018, Joel Melstad, a spokesman for the U.S. National Counterintelligence and Security Center, reported that Snowden's disclosures "have put U.S. personnel or facilities at risk around the world, damaged intelligence collection efforts, exposed tools to amass intelligence, destabilized U.S. partnerships abroad and exposed U.S. intelligence operations, capabilities and priorities."[1] Snowden's attorney, Ben Wizner, believes that these reports are exaggerated and alarmist, arguing that "the mainstream view among intelligence professionals is that every day and every year that has gone by has lessened the value and importance of the Snowden archives."[2] However, Wizner's assessment is regrettably limited in its scope. Importantly, it fails to account for the significant impact that Snowden's leaks had on the development of the European Union's General Data Protection Regulation (GDPR)–a piece of legislation that has fundamentally changed the nature of data privacy in the EU, and the world over.

The connection between Edward Snowden and the GDPR can actually be traced back to the European Parliamentary Committee on Civil Liberties, Justice and Home Affairs[3] (LIBE). This committee has a surprising history because, though its members were exceptionally interested in Snowden's leaks, its ensuing legislative activity has been largely understudied. For example, on October 29, 2013, then-U.S. Director of National Intelligence, James Clapper, appeared before the U.S. House Intelligence Committee to discuss Snowden's revelations.[4] The very next day, LIBE representatives met with senior National Security Council officials at the White House.[5] LIBE had an expansive mandate,[6] an entrenched concern for personal data protection,[7] and a history of treating national intelligence services with suspicion if not outright hostility.

Hallie Coyne is a recent graduate of the Frederick S. Pardee School of Global Studies at Boston University. While at BU, Ms. Coyne studied International Relations and History, with concentrations in International Security, and European Politics. She has been a research assistant on various projects investigating the European Union's institutional history. Ms. Coyne's research interests include transatlantic relations and the future of national security at the intersection of intelligence and emerging cyber capabilities. Before graduating, Ms. Coyne completed internships with the U.S. Embassy in Ottawa, via the Virtual Student Federal Service program (VSFS), and the International Trade Administration, within the U.S. Department of Commerce. She spent a semester at Sciences Po and later attended the Cambridge Security Initiative's 2018 International Security and Intelligence summer program (ISI), where she initiated the research for this paper. Ms. Coyne currently lives in the Washington D.C. area and works in the private sector.

Yet even with this robust background, LIBE operated with remarkable inconspicuousness.

Much of the current academic literature[8] overlooks or ignores the influence of the Snowden leaks on the functioning of the LIBE committee, and by extension, the formation of the General Data Protection Regulation.[9] This paper aims to introduce a new facet to the political contextualization of GDPR, by examining LIBE's pattern of framing data privacy issues in relation to the activity of security services that impact EU citizens. Prior to 2013, LIBE pursued power maximization efforts, exercising some method of informal control over the intelligence services of EU member states, and promoting data privacy and protection. After Snowden's leaks of U.S. intelligence capabilities, LIBE members capitalized on the opportunity to advance many of their goals. Given the breadth of GDPR, and the intentions of its authors, Ben Wizner's estimation of Snowden's dwindling relevance may prove acutely premature.

Methodological and Theoretical Approach

By using a historical review, this paper provides a long-range view of LIBE's engagement with the balance that exists between the EU and its member states at the intersection of data privacy and national security. This paper will not discuss the substantial scholarly work theorizing the development of the EU in its entirety. Similarly, theories in intelligence studies, pertinent though they may be, are beyond the scope of this investigation. A more substantial and analytical approach to address these issues certainly merits further study.

With such limitations in mind, a theoretical basis is still necessary to examine how LIBE's activities might be understood within its existing institutional framework and its broader international context. The traditional challenge of analyzing LIBE's activities via applying state-centric theories is inherent in the very existence of LIBE in the supranational body of the

European Parliament. This is considered a possible explanation for LIBE's comparative anonymity in the many studies completed with the intention of gauging the impact of Snowden's actions because "state-centric theories make it difficult for analysts to detect European [EU] foreign policy on their radars, and they are therefore bound to reject the existence or significance of European foreign policy."[10]

Therefore, the primary analytical framework applied to this historical review is drawn from theories of European integration. Such theories contextualize and seek to explain the behavior of EU institutions and their components. The theory employed is neofunctionalism, and the spillover process it implies. There are three widely accepted dimensions of the concept of spillover, all of which are applicable to this analysis. First, in functional spillover, the "core argument in relation to EU foreign policy is that, as internal policies become integrated, there is also pull towards developing an external dimension."[11] Second, political spillover suggests that as the EU integration process continues, "actor perceptions of state interests become increasingly European, focusing more on common interests."[12] Finally, and most importantly for the purposes of this paper, "institutions created by states have interests in pushing for more integration, termed cultivated spillover."[13]

GDPR is an extension of EU integration because it further harmonizes EU standards for data protection. For example, other dimension of EU policy certainly influenced GDPR's development. This paper specifically examines how the LIBE Committee's work on GDPR translated in part from its parallel interests and activities in the field of EU security policy. The following historical review traces the relevant activities of LIBE to the point of the Snowden leaks, evaluates the extent to which LIBE adjusted its legislative activity in the development of GDPR as a result, and argues that the trends that contributed to LIBE's position on GDPR are still a critical aspect of LIBE policy making today.

PART I: LIBE 1995–2013

Historically, LIBE has struggled to address the real and perceived attacks on civil liberties that mass data processing by intelligence services can produce. There is no EU capacity to cover standard intelligence service activities.[14] As such, the work of national intelligence services is well beyond the control of the European Parliament (EP),[15] and certainly beyond the capacity of LIBE.[16] The GDPR in its final form does not interfere with the processing of data for national security purposes, as member states can introduce derogations where the transfer of private data to third countries is necessary for reasons of public interest, including national security and the prevention and detection of crime amongst others.[17] However, historical limitation on the national security competencies of the EU have not prevented significant parliamentary scrutiny of the work of national intelligence services in the EU and in the US.

A key example of this engagement is the EP's involvement in the Echelon Affair from 1998-2002. The Echelon network system intercepted private and economic communications, developed and managed by the Five Eyes intelligence alliance.[18],[19] Though the EP eventually set up a temporary committee explicitly for the investigation of the Echelon network,[20] LIBE critically re-launched debates in Parliament in 2000 during a "hearing on the European Union and data protection, during which the second text on Echelon was presented, the existence of Echelon having by then been confirmed by American sources."[21]

This early connection between data protection and the activities of intelligence services continued as LIBE, and the EU,[22] developed in the years following 2002. The Treaty of Lisbon increased the power of the EP in the EU legislative process.[23],[24] Still, prior to the Treaty of Lisbon, the operation of EP committees mattered because "most of the discussions [framing the legislation took] place at the committee level, making the leading committee largely responsible for examining the details of the proposal and starting negotiations with the Council and the Commission."[25] In many ways committees are "the central bodies of the institutions,[26] determining the behavior of their members as well as the policy outcomes."[27] In this context, LIBE rapporteurs [28] often criticized attempts to moderate policy proposals for data protection from the Commission as adjusting to "the lowest possible common denominator"[29] and repeatedly called for the introduction of a more extensive data protection framework.[30]

The SWIFT affair began in June 2006 and reinforced LIBE's focus on data protection. European and US media had published the existence of the Terrorist Finance Tracking Program (TFTP), established by the U.S. Administration, which "allow[ed] US authorities to access all the financial data stored by SWIFT (Society for Worldwide Interbank Financial Telecommunications)."[31] The EP adopted a resolution in July 2006, "requiring in particular that the Committee on Civil Liberties, Justice and Home Affairs (LIBE) together with the Committee on Economic and Monetary Affairs (ECON) hold a joint hearing with the private and public parties involved in the affair in order to ascertain what information they may have had."[32] Debates on the SWIFT dossier extended through 2010. When an agreement finally entered into force on February 1, 2010, it required a vote from LIBE. LIBE, exercising the EP's new powers to influence the conclusion of international agreements, established by the Treaty of Lisbon,[33] rejected the agreement. The U.S. rapidly adjusted, inviting "key MEPs, led by the rapporteur and the LIBE committee's chairman, to visit the US."[34]

In September 2011, LIBE had a study completed on "Parliamentary Oversight of Security and Intelligence Agencies in the European Union."[35] The study noted that "over the past decade, the EP has developed a growing interest in national security agencies."[36] Evidence for this included "strong interest in the development of the new regulation on Frontex, the Europol and Eurojust decisions, as well as two temporary committees that examined the activities of national security agencies and made important recommendations in regard to oversight."[37]

Though LIBE began to truly exercise power on the international stage in the 2000s, the EU has an established history of dealing with data protection, dating back to the Data Protection Directive of 1995.[38] In January 2012, the Commission of the European Union released a Proposed Data Protection Regulation, designed, as all EU regulations are,[39] to be directly binding on member states.[40] The LIBE committee subsequently began to formulate the EP's amendments to the General Data Protection Regulation proposal,[41] and on April 12, 2012 LIBE appointed committee member Jan Philipp Albrecht as official rapporteur of the European Parliament for GDPR.[42]

In October 2012, a briefing note produced on Cloud Computing for the LIBE Committee highlighted the loopholes of the U.S. Foreign Intelligence Surveillance Act (FISA),[43] and their consequences for EU citizens' rights and protection.[44] LIBE held a hearing for the presentation of the briefing note to the entirety of the European Parliament, following a session on the EU Cybersecurity strategy on February 20, 2013, and asking for "immediate proposals to meet the LIBE amendment deadline on the Data Protection Regulation."[45] Yet by March, "the level of interest in the note declined, and there seemed only a remote possibility that Parliament would support fundamental revisions of the Data Protection Regulation."[46]

In the months following June 2013, LIBE received approximately 4,000 potential amendments submitted by separate parliamentary committees. Such a dramatic shift in interest suggests that the watershed moment for the progression of GDPR is significantly attributable to NSA contractor Edward Snowden.

PART II: LIBE JUNE 2013 – OCTOBER 2013

On June 5, 2013, Glenn Greenwald published the first of Edward Snowden's disclosures in *The Guardian*.[470] A Resolution of the European Parliament on July 4, 2013 gave LIBE a broad mandate "to engage in fact-finding concerning Snowden's disclosures, and to assess their impact on the fundamental rights of EU citizens."[48] Claude Moraes, appointed the rapporteur for the inquiry, produced the concluding "Moraes Report."[49] A year later, in July 2014, Moraes was elected Chairman of LIBE.[50] Then, in November 2014 while giving a lecture at the London School of Economics, Moraes said: "The next phase of our enquiry has to be on where we take this concept of privacy, where we take the concept of regulation. It is an extremely challenging time... I don't have huge faith in many member states to do this, there's so many vested interests, vested security interests to not do this — but we have to try and do this."[51]

LIBE called for an inquiry, and hearings began in September 2013. These hearings saw "public questioning of a number of important stakeholders in the issue area, including privacy officers, (former) security services staff, EU Commission officials, and IT specialists."[52] Notably absent from these hearings were "those national European security agencies believed to be cooperating with the NSA."[53]

LIBE also requested formal studies following the Snowden leaks, the first of which was completed in September 2013, paralleling the hearings. Titled "The US Surveillance Programs and Their Impact on EU Citizens' Fundamental Rights," the study explored "the scope of surveillance that can be carried out under the 2008 Amendments Act of US Foreign Intelligence Surveillance (FISA) and related practices of US authorities, which have very strong implications for EU data sovereignty and the protection of European citizens' rights."[54]

In October 2013, LIBE drew further correlations between data protection and the operation of security services. This is largely evidenced by another study for the committee titled "National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law."[55] The study concluded that "intelligence communities' understandings and practices of national security and member states' surveillance programmes jeopardize the EU principle of 'sincere cooperation,' as they make it more difficult to carry about the tasks following the Treaties."[56]

Still, pointed studies were not the only results of the Snowden inquiry. SWIFT representatives testified before LIBE in September 2013 during LIBE's investigation. On October 16, 2013 the SWIFT Agreement was officially suspended as a direct result of Snowden's disclosures.[57] This suspension gave GDPR rapporteur Jan Philipp Albrecht the opportunity to draft an unofficial joint motion in which he pointed out that: "Although the Parliament has no formal powers to initiate a suspension or termination of an international agreement, the Commission will have to act if Parliament withdraws its support for a particular agreement."[58] This statement evidences the willingness of LIBE members to find means of pursuing policy agendas despite having comparatively little formal capacity to do so.

The controversy around the revelations of the various NSA programs apparently made an impression on MEP Albrecht. In 2015 Albrecht wrote that "the revelation by Edward Snowden regarding the mass storage and analysis of details relating to our everyday lives by the secret services and their agents within the internet companies only served to demonstrate to us all how far things have already developed and how little regulation or effective control the people and society are able to muster."[59] Albrecht later became the rapporteur for the EU Police Directive,[60] relating to the processing of personal data by competent authorities "for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data."[61]

During the inquiry on October 21, 2013, LIBE voted to adopt the compromise draft for the GDPR. This draft significantly increased potential sanctions for non-compliance, extended the territorial scope of the regulation, reviewed third country data transfers, placed limits on profiling, and introducing new requirements for Data Protection Officers.[62] The compromise draft passed with an impressive majority, with 49 of LIBE members voting in support, one against, and three abstentions.[63] Importantly, the territorial scope expanded at this stage to include those companies operating in the EU with European citizen customers, introducing the extra-territorial reach of the legislation that survived to the finalized version of GDPR of 2016.[64]

This vote represented a significant step in more than two years of discussions and lobbying leading to a plenary legislative resolution on March 12, 2014.[65] Debates in this period took place during the EP's first reading of the legislation.[66] The Council of the European Union agreed on its first reading position on the GDPR in June 15, 2015. The ensuing stages further evidence the LIBE committee's efforts to discuss the processing of personal data for national security matters in concert with the data protection standards required of private corporations.

PART III: LIBE OCTOBER 2013–JANUARY 2017

The importance of data privacy and data protection became increasingly apparent in the public space after 2013. Three instances of LIBE's legislative activities will be used as a lens to evaluate the continuing efforts of LIBE to manage the tenuous relationship it found between security and privacy: the 'anti-FISA' clause of GDPR, the Police Directive, and the ePrivacy Regulation.

After passing the first reading of the EP in 2014, GDPR negotiations progressed to negotiations involving representatives from the EP and the Council of the European Union. Due to LIBE's responsibility for GDPR, their representatives were the primary negotiating team for the EP.[67] By September 2015, Article 43a – nicknamed 'the anti-FISA'[68] – remained a problem.[69] The clause mandated that EU companies should not have to supply Europeans' personal data to non-European countries. It caused broad industry concern, and a letter to legislators from the European Data Coalition explained that Article 43a "unilaterally assum[ed] universal jurisdiction...put[ting] European companies in an unsolvable dilemma and would be in conflict with the concept of interoperability that, while recognizing different privacy concepts, is necessary in international data flows."[70]

Coalition appeals did little to change the mind of legislators. The Industry Coalition for Data Protection (ICDP), which represented companies such as Apple and Google, also sent letters to the top regulation negotiators, including the parliamentary GDPR rapporteur Jan Philipp Albrecht. ICDP argued that Article 43a deliberately created legal conflicts and undermined "both the principles of reciprocity in diplomatic relations as well as the credibility of EU data protection reform."[71] Still, Article 43a came into force as Article 48[72] on "Transfers or disclosures not authorized by Union Law"[73] in the final draft of GDPR.[74]

More broadly, GDPR can be considered in the context of the EU Protection Data Reform Package, a reference to the combined development of GDPR and its significantly less well-known companion, the Police and Criminal Justice Authorities Directive.[75] The EU passed both of pieces of legislation in May 2016; they became applicable to member states in May 2018. Notably, prior to the Police Directive, scholars critiqued data protection in the sector of law enforcement and criminal justice for "offering no stable or uniform legal structure and causing considerable legal uncertainty and inconsistent enforcement of data protection rules."[76]

However, whatever regulation exists in the context of police forces and criminal justice is intrinsically related to the activities of member state security services. Indeed, "There is a close cooperation between law enforcement authorities and intelligence services," as "in the prevention and investigation of crime, these bodies often exchange intelligence with each other."[77] The LIBE-commissioned studies of 2013 used this closeness to justify potential future efforts by LIBE to extend its competencies to the regulation of the activities of member state intelligence services. Justification for this potential extension of EU power pointed to the already present potential spillover of intelligence services activities "into the activities and responsibilities of EU agencies."[78] As such interactions were already taking place, it followed that the EU might have an implied competence to regulate the activities of member state intelligence services.

The actual impact of the Police Directive on the operation of security services is not entirely clear. The Directive does represent the first time that "data protection in the...area of police and judicial cooperation in criminal matters shall be covered by a single legal instrument with direct effect in national legal systems."[79] When compared to GDPR, though, "the final version of the Directive still maintains a number of vague provisions open to interpretations and at times establish[es] low or inadequate data protection standards."[80] The dichotomy of a robust GDPR and a weak Police Directive when LIBE had the primary responsibility for both pieces of legislation suggests that LIBE's final aim of managing the data processing capability of security services has yet to be realized.

Though GDPR and the Police Directive are in force, the EU and LIBE are continuing to legislate on data protection. The question of LIBE's perception of the adequacy of current legislation may be evaluated via future developments of the ePrivacy Regulation.[81] In January 2017 the European Commission tabled a proposal for a regulation on privacy and electronic communications, which would replace the current 2002 e-Privacy Directive if it became law.[82] Once again, LIBE shaped the EP's amendments to the European Commission proposal.

The ePrivacy Regulation focuses on the security of online communications. It remained bogged down in debates at the time of writing.[83] However, the draft the EP approved in May 2018 required "Skype, WhatsApp, iMessage, video games with player messaging and other electronic services that allow private interactions to obtain people's explicit permission before placing tracking codes on users' devices or collecting data about their communications."[84] Once again, Jan Philipp Albrecht shepherded the legislation through the EP.[85] Trade groups and tech companies "have waged a furious, multipronged lobbying campaign to shut down, or at least weaken, the legislation."[86] These efforts include sponsoring studies that are rife with dire economic predictions of the ePrivacy Regulation's impact on business opportunities for years to come.[87]

CONCLUSION

LIBE is in a difficult legal position. Privacy and data protection are fundamental rights affirmed by EU primary and secondary law.[88] Concurrently, the intersection of individual privacy rights and national security requirements is nuanced and complicated territory. LIBE's mandate requires that it take responsibility for legislation that pertains to data privacy and protection.[89] However, when such a position of power is abused, and the complexities of the issues LIBE must address are oversimplified, the potential exists for significant and serious consequences. LIBE continues to frame the US as an unreliable partner for data protection, as evidenced by LIBE's recent resolution to suspend the data exchange deal arranged by the EU-US Privacy Shield, with LIBE Committee Chair and rapporteur Claude Moraes saying "Privacy Shield in its current form does not provide the adequate level of protection required by EU data protection law and the EU Charter."[90] The same resolution that suspended Privacy Shield expressed LIBE concerns regarding the US adoption of the CLOUD Act, "which expands the abilities of American and foreign law enforcement to target and access people's data across international borders without making use of the instrument[s]...which provide for appropriate safeguards and respect the judicial competences of the countries where the information is located."[91] Similarly, the resolution also voiced concern on "those issues related to national security, such as the re-authorization of Section 702 of the Foreign Intelligence Surveillance Act (FISA)."[92] Clearly, the LIBE committee maintains that individual data privacy has been unduly sacrificed for expansive national security aims.

Due to GDPR's current presentation as a model for other countries aiming to develop their own data privacy protection frameworks, this paper's approach allows for a more nuanced view of the political climate in which LIBE operates and GDPR exists. As technological advancements in data processing and analysis create new vulnerabilities and opportunities for both public and private sector entities, it is essential to critically evaluate not only the regulatory standards that exist but also the opinions that inform them.

NOTES

1. Deb Reichmann, "U.S. Expects Fallout From Snowden Leaks for Years to Come," *U.S. News*, June 3, 2018, https://www.usnews.com/news/world/articles/2018-06-03/5-years-on-us-government-still-counting-snowden-leak-costs.
2. Ibid.
3. Hereafter referenced as "LIBE" or "the LIBE Committee."
4. Tracy Connor, "Spy Chief Clapper: We've been snooping on our friends for years," *NBC News*, October 30, 2013, https://www.nbcnews.com/news/us-news/spy-chief-clapper-weve-been-snooping-our-friends-years-flna8C11488415.
5. Ibid.
6. The LIBE Committee holds responsibility in the European Parliament for "the establishment and development of an area of freedom, security and justice while respecting the principles of subsidiarity and proportionality, in particular: (a) measures concerning the entry and movement of persons, asylum and migration, (b) measures concerning an integrated management of the common borders, (c) measures relating to police and judicial cooperation in criminal matters, including terrorism, and substantive and procedural measures relating to the development for a more coherent Union approach to law; (5) the European Monitoring Center for Drugs and Drug Addiction the European Union Agency for Fundamental Rights, Europol, Eurojust, Cepol, the European Public Prosecutors Office, and other bodies and agencies in the same area..." European Parliament. *Draft Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP))*, March 10, 2018, http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf.
7. The LIBE Committee holds responsibility in the European Parliament for "the establishment and development of an area of freedom, security and justice while respecting the principles of subsidiarity and proportionality, in particular: (a) measures concerning the entry and movement of persons, asylum and migration, (b) measures concerning an integrated management of the common borders, (c) measures relating to police and judicial cooperation in criminal matters, including terrorism, and substantive and procedural measures relating to the development for a more coherent Union approach to law; (5) the European Monitoring Center for Drugs and Drug Addiction the European Union Agency for Fundamental Rights, Europol, Eurojust, Cepol, the European Public Prosecutors Office, and other bodies and agencies in the same area..." European Parliament. *Draft Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP))*, March 10, 2018, http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf.
8. Scholarship completed as recently as 2017 and 2018 have begun to include important references to the activities of LIBE. (Valentin Gros, Marieke de Goede, Beste Îsleyen. "The Snowden Files Made Public: A Material Politics of Contesting Surveillance." *International Political Sociology* 11, no. 1 (March 2017): 73-89, and Laima Jančiūtē, "EU Politics and the Making of the General Data Protection Regulation: Consolidation, Policy Networks, and Institutionalism in the Process of Balancing Actor Interests." PhD diss., University of Westminster, 2018.
9. Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, 1–88. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016R0679.
10. Knud Erik Jørgensen, "Introduction: Theorizing European Foreign Policy." In *The SAGE Handbook of European Foreign Policy*, edited by Knud Erik Jorgensen, Aasne Kalland Aarstad, Edith Drieskens, Katie Laatikainen, and Ben Tonra, 77, Los Angeles, London, New Dehli, Singapore, Washington D.C., Boston: SAGE Publications, 2015.
11. Ibid. 90, References made to A. Niemann (2006) *Explaining Decisions in the European Union.* Cambridge: Cambridge University Press, and P.C. Schmitter (1969) 'Three neo-functional Hypotheses about International Integration," *International Organization*, 23(1), 161-166.
12. Ibid., 90.
13. Ibid., 90.
14. "This is affirmed by the treaties that govern the European Union, as "according to Article 4(2) TEU and Article 72 TFEU, data process for 'national security purposes fall outside the scope of the EU laws." (Cristina Blasi Casagran, "Data safeguards for the intelligence collected and shared by Member States." In *Global Data Protection in the Field of Law Enforcement: An EU Perspective,* 164-207. London, UK: Routledge, 2016.) There is also no explicit definition of the term "national security" in the EU laws, so the exception it provides for may be interpreted to the full extent of its potential ability to prevent EU encroachment on the sovereign powers of Member States, Casagran, "Data safeguards for the intelligence collected and shared by Member States," 165.

NOTES

15. Hereinafter referenced as the "EP."
16. The caveat to this is that the EU can sometimes play a coordinating role in national security issues as demonstrated by the Schengen Information System. "Instead, the regulation of national security issues falls under the exclusive competence of the member states. The EU's role in this area would be purely co-ordinative, if any. For instance, one of the few examples of this limited EU role in national security matters is found in the regulation of the Schengen Information System," Casagran, "Data safeguards for the intelligence collected and shared by Member States," 167.
17. European Data Protection Board. "Guidelines 2/2018 on Derogations of Article 49 Under Regulation 2016/679."Adopted on May 25, 2018. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf.
18. The Five Eyes member states are Australia, Canada, New Zealand, the United Kingdom, and the US.
19. Franco Piodi and Mombelli Iolanda, *The ECHELON Affair: The EP and the Global Interception System 1998-2002.* Study. PE 538.877. Brussels: Directorate-General for Parliamentary Research Services, Historical Archives Unit, 4. http://www.europarl.europa.eu/EPRS/EPRS_STUDY_538877_AffaireEchelon-EN.pdf.
20. "At its meeting of 13 April 2000, the Conference of Presidents rejected the proposal to set up a committee of inquiry and approved the creation of a temporary committee: a decision was taken accordingly on 15 June. Both decisions by the Conference of Presidents – rejection of a committee of inquiry and the setting up of the temporary committee – were approved by Parliament on 5 July 2000," Ibid 19.
21. Ibid 13.
22. Hereinafter referenced as the "EU."
23. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, December 13, 2007. *OJ C 306, 17.12.2007,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A12007L%2FTXT.
24. Today, the ordinary legislative procedure applicable to over 80 policy areas which essentially makes the European Parliament the co-legislating body with the Council of the European Union. Before the co-decision procedure was established the European Parliament had significantly less capacity to influence the development of EU legislation.
25. Further, "Even in those cases where it is only consulted, the EP casts a vote on a committee report rather than on the Commission's proposal." Ariadna Ripoll Servent,"Playing the Co-Decision Game? Rules' Changes and Institutional Adaptation at the LIBE Committee." *Journal of European Integration* 34, no. 1 (2012): 58.
26. Ibid. 58.
27. Ibid. 58.
28. Since the Treaty of Lisbon, the role of rapporteurs in the EP's legislative process has undergone significant shifts. An increase in informal negotiations between the EP and the Council of the European Union led to the relative strength of rapporteurs in comparison to committee chairmen, as rapporteurs were often "in a better position to access and steer negotiations, thanks to their direct access to information." Ariadna Ripoll Servent, "Playing the Co-Decision Game? Rules' Changes and Institutional Adaptation at the LIBE Committee," 60.
29. European Parliament. 2008, Report of July 23, 2008 on the proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, A6-0322/2008. Ariadna Ripoll Servent, "Playing the Co-Decision Game? Rules' Changes and Institutional Adaptation at the LIBE Committee," 66.
30. Ibid. 66.
31. European Parliament. "The Interception of Bank Transfer Data from the SWIFT System by the US Secret Services." Public Hearing. October 4, 2006, http://www.europarl.europa.eu/hearings/20061004/libe/programme_en.pdf.
32. Ibid.
33. European Parliament Liaison Office in Ireland. "EP Civil Liberties Committee to vote on EU-US SWIFT Agreement." Press Release. Dublin: European Union, February 3, 2010. http://www.europarl.europa.eu/ireland/en/about-us/ep-civil-liberties-committee-to-vote-on-eu-us-swift-agreement.
34. Hennis-Plasschaert, MEP, interview, March 2010; MEP, interview, July 2010, Referenced in at Ariadna Ripoll. "The role of the European Parliament in international negotiations after Lisbon." *Journal of European Public Policy* 21, no. 4 (2014), 568-586. https://www.tandfonline.com/doi/pdf/10.1080/13501763.2014.886614
35. European Parliament, 2011, *Parliamentary Oversight of Security and Intelligence Agencies in the European Union.* Policy Department C: Citizens' Rights and Constitutional Affairs, accessed at https://fas.org/irp/eprint/europarl.pdf.

NOTES

36. Ibid.
37. Ibid.
38. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, OJ L 281, 23.11.1995, 31–50, https://eur-lex.europa.eu/eli/dir/1995/46/oj.
39. In the EU, a "regulation" is a binding legislative act that must be applied in its entirety across the EU. For more information on the variations in EU legislation see: https://europa.eu/european-union/eu-law/legal-acts_en
40. The Directive had left room for several remaining differences between national laws for data protection, Paul M. Schwartz, "Information Privacy in the Cloud," *University of Pennsylvania Law Review* 161, no. 6 (2013), 1639.
41. Wilhelm, Ernst-Oliver. "A Brief History of the General Data Protection Regulation." *International Association of Privacy Professionals*, last update 2016, https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/.
42. Ibid.
43. Section 702 of Title VII of the Foreign Intelligence Surveillance Act (FISA) "authorizes surveillance directed at non-US persons located overseas who are of foreign intelligence importance," James R. Clapper, and Eric H. Holder, Jr., "Letter re Title VII of the Foreign Intelligence Surveillance Act (FISA)." February 8, 2012, https://www.justice.gov/sites/default/files/ola/legacy/2012/11/08/02-08-12-fisa-reauthorization.pdf.
44. European Parliament. *Fighting Cyber Crime and Protecting Privacy in the Cloud.* Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz, and Amandine Scherrer, PE 462.509, Brussels: Parliament Department C: Citizens Rights and Constitutional Affairs, 2012, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf.
45. In 2012 the LIBE committee commissioned a briefing Note on "Fighting Cybercrime and Protecting Privacy in the Cloud" from the Center for European Policy Studies (CEPS) and the Centre d'Etudes Sur les Conflicts, Liberté et Securité (CCLS). "Sections of the Note clearly asserted that Cloud computing and related US regulations presented an unprecedented threat to EU data sovereignty." (European Commission, "LIBE Committee Vote Backs New EU Data Protection Rules," Press Release, MEMO-13-923, October 22, 2013, http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.) The Note included the February 2013 observation that "So far, almost all the attention on [conflicts of international public law] has been focused on the US PATRIOT ACT, but there has been virtually no discussion of the implications of the US Foreign Intelligence Surveillance Amendment Act of 2008. Section 1881a of FAA for the first time created a power of mass-surveillance specifically targeted at the data of non-US persons located outside the US, which applies to Cloud computing" European Parliament. *Fighting Cyber Crime and Protecting Privacy in the Cloud.* Didier Bigo, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz, and Amandine Scherrer, PE 462.509. Brussels: Parliament Department C: Citizens Rights and Constitutional Affairs, 2012, 35, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2012/462509/IPOL-LIBE_ET(2012)462509_EN.pdf.
46. Ibid. 35.
47. Glenn Greenwald, "Verizon Order: NSA Collecting Phone Records of Millions of Americans Daily." *The Guardian*, June 5, 2013, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.
48. European Parliament, *Resolution on the US National Security Agency Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Privacy.* Joint Motion for a Resolution. RC-B7-0336/2013. Brussels: European Union, July 2, 2013, http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=P7-RC-2013-0336&language=EN.
49. The report was officially titled "LIBE (JHA) Committee Inquiry on Electronic Mass Surveillance of EU citizens," *Claude Moraes,* "Claude Moraes MEP for London Rapporteur of the LIBE Committee Report on Electronic Mass Surveillance of EU Citizens in the European Parliament," Claude Moraes, July 26, 2013, http://www.claudemoraes.com/news/95/25/Claude-Moraes-MEP-for-London-Rapporteur-of-the-LIBE-Committee-Report-on-Electronic-Mass-Surveillance-of-EU-citizens-in-the-European-Parliament.
50. European Parliament, "Claude Moraes," MEPs, accessed on August 11, 2018, http://www.europarl.europa.eu/meps/en/4519/CLAUDE_MORAES_home.html.
51. Natasha Lomas, "Digital Privacy is 'The New Frontier of Human Rights," *Tech Crunch,* November 23, 2014, https://techcrunch.com/2014/11/23/privacy-human-rights-frontier/.
52. Valentina Gros, Marieke de Goede, Beste Îsleyen, "The Snowden Files Made Public: A Material Politics of Contesting Surveillance," *International Political Sociology* 11, no. 1 (March 2017), 74.

NOTES

53. Ibid. 74.
54. European Parliament, *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights.* Caspar Bowden and Didier Bigo, Note. PE 474.405. Brussels: Policy Department C: Citizens' Rights and Constitutional Affairs, September 16, 2013, http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf.
55. European Parliament, *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law*, Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, Amandine Scherrer. Study. PE 493.032. Brussels: Policy Department C: Citizens' Rights and Constitutional Affairs, October 14, 2013, http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf.
56. Ibid.
57. The Greens in the European Parliament, "Suspension of the SWIFT agreement as a result of NSA Surveillance," October 16, 2013, https://www.greens-efa.eu/en/article/suspension-of-the-swift-agreement-as-a-result-of-nsa-surveillance/.
58. European Parliament, *Joint Motion for a Resolution on the Suspension of the TFTP agreement as a result of NSA surveillance*, Joint Motion for a Resolution, RC-B7-0468/2013, Brussels: European Union, October 21, 2013. http://www.europarl.europa.eu/sides/getDoc.do?type=MOTION&reference=P7-RC-2013-0336&language=EN. Referenced in Cristina Blasi Casagran, "Data safeguards for the intelligence collected and shared by Member States," in *Global Data Protection in the Field of Law Enforcement: An EU Perspective*, 184. London, UK: Routledge, 2016.
59. Jan Philipp Albrecht, "Hands off our data!" *Knaur Taschenbuch*, 41, last modified 2015, https://www.janalbrecht.eu/wp-content/uploads/2018/02/JP_Albrecht_hands-off_final_WEB.pdf.
60. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. OJ L 119, 4.5.2016, 89–131, https://eur-lex.europa.eu/legal content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG
61. Ibid.
62. Hogan Lovells, "EU draft Data Protection Regulation: the LIBE Committee Amendments," Briefing Paper, 1. 2013, accessed August 11, 2018, https://www.hldataprotection.com/files/2013/11/EU-Draft-Data-Protection-Regulation-LIBE-Committee-Amendments.pdf.
63. European Commission, "LIBE Committee Vote Backs New EU Data Protection Rules," Press Release, MEMO-13-923, October 22, 2013, http://europa.eu/rapid/press-release_MEMO-13-923_en.htm.
64. According to Article 3 Sections 1 and 2 of the GDPR, the regulation applies if "If the processing of personal data takes place in the context of the activities of an establishment or organization in the EU, regardless of whether the processing itself takes place in the EU (Article 3, Section 1 of the GDPR)," and "If the personal data of individuals who are in the EU is processed by an organization not established in the EU and the processing concerns the offering of goods or services to individuals in the EU, or monitoring the behavior of individuals that takes place in the EU (Article 3, Section 2 of the GDPR)," Matthias Artzt, "Territorial scope of the GDPR from a US perspective," *International Association of Privacy Professionals*, June 26, 2018, https://iapp.org/news/a/territorial-scope-of-the-gdpr-from-a-us-perspective/.
65. European Parliament, "First reading of the European Parliament: European Parliament legislative resolution of March 12, 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading)," A7-0402/2013, Strasbourg: European Union, March 12, 2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT%20TA%20P7-TA-2014-0212%200%20DOC%20XML%20V0//EN. Referenced Eleni Kosta and Kees Stuurman, "The Draft General Data Protection Regulation," in *The Law, Economics and Politics of International Standardization*, edited by Panagiotis Delimatsis, 441, Cambridge: Cambridge University Press, 2015.
66. For a short review of the EU's Ordinary Legislative Process visit: http://www.europarl.europa.eu/external/html/legislativeprocedure/default_en.htm

NOTES

67. In the case of the GDPR negotiations "The Parliament [was] represented by Jan Albrecht, the rapporteur on the legal text, Claude Moraes, the chairperson of the lead Parliament committee (LIBE committee), shadow rapporteurs, political group coordinators and various staff members of the Parliament." For a useful synopsis of the 'trilogue' negotiations process visit: https://privacylawblog.fieldfisher.com/2015/unravelling-the-mysteries-of-the-gdpr-trilogues
68. Neil Ford, "European Data Coalition lobbies against GDPR Article 43a – the 'anti-FISA' Clause." IT Governance, September 3, 2015, https://www.itgovernance.eu/blog/en/european-data-coalition-lobbies-against-gdpr-article-43a-the-anti-fisa-clause.
69. Ibid.
70. European Data Coalition, "Re: International data transfers," August 24, 2015, accessed at: http://europeandatacoalition.eu/wp-content/uploads/2015/06/Coalition-reaction-on-Ch-V3.pdf.
71. David Meyer, "Industry issues plea over data reform," Politico, January 28, 2018, https://www.politico.eu/article/industry-plea-data-reform-protection-privacy/.
72. "The GDPR maintains existing restrictions on the transfers of personal data from the EU to third countries or international organizations. These restrictions are aimed at ensuring that the GDPR's provisions cannot be circumvented by transferring personal data from the EU to a non-EU country with less restrictive data-privacy laws. Pursuant to Article 46, such transfers may only be made to countries that also have adequate data-protection requirements. However, Article 49 of the GDPR also gives member states flexibility to allow the transfer of personal data to third countries absent an adequacy determination if such transfer is "necessary for important reasons of public interest"—for example, if there is a need to transfer health data to a third country in order to deal with an international public-health emergency," Ali Cooper-Ponte, "GDPR Derogations, ePrivacy, and the Evolving European Privacy Landscape," *The Lawfare Institute*, last modified May 25, 2018, https://www.lawfareblog.com/gdpr-derogations-eprivacy-and-evolving-european-privacy-landscape.
73. "Chapter V (Articles 44 through 49) of the GDPR governs cross-border transfers of personal data. Article 45 states the conditions for transfers with an adequacy decision; Article 46 sets forth the conditions for transfers by way of appropriate safeguards in the absence of an adequacy decision; Article 47 sets the conditions for transfers by way of binding corporate rules; Article 48 addresses situations in which a foreign tribunal or administrative body has ordered transfer not otherwise permitted by the GDPR; and Article 49 states the conditions for derogations for specific situations in the absence of an adequacy decision or appropriate safeguards," Meyers, "Industry issues plea over data reform," 2018.
74. Parliament and Council Regulation (EU) 2016/679 of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation). OJ L 119, 4.5.2016, 1–88, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX-:32016R0679.
75. European Commission. "Questions and Answers – Data Protection Reform Package." Press Release. MEMO-17-1441, May 24, 2017, http://europa.eu/rapid/press-release_MEMO-17-1441_en.htm, hereinafter "the Directive."
76. Hielke Hijmans and Alfonso Scirocco, "Shortcomings in EU data protection in the third and the Second Pillars. Can the Lisbon Treaty be expected to help?" *Common Market Law Review* 46, (2009): 1496. Referenced in Thomas Marquenie, "The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework," *Computer Law & Security Review* 33, no. 3 (2017): 325, https://www.sciencedirect.com/science/article/pii/S0267364917300742.
77. Casagran, "Introduction," 5.
78. Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Ragazzi, and Amandine Scherrer, *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law.* Brussels: *Center for European Policy Studies*, November 6, 2013, https://www.ceps.eu/publications/mass-surveillance-personal-data-eu-member-states-and-its-compatibility-eu-law.
79. Marquenie, "The Police and Criminal Justice Authorities Directive," 338.
80. Ibid. 338.
81. European Commission, "Proposal for a Regulation of the European Parliament and of the Council Concerning the Request for Private Life and the Protection of Personal Data in Electronic Communications and Repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)," Brussels, October 1, 2017, http://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2017/0010/COM_COM(2017)0010_EN.pdf.
82. Ibid.

NOTES

83. Reed Smith LLP, "ePrivacy regulation will likely not apply before 2021," *Lexology*, January 28, 2019, https://www.lexology.com/library/detail.aspx?g=23653861-8a4e-4cff-9550-717594099922.
84. Natasha Singer, "The Next Privacy Battle in Europe is Over This New Law," *NYTimes*, May 27, 2018, https://www.nytimes.com/2018/05/27/technology/europe-eprivacy-regulation-battle.html.
85. Ibid.
86. Ibid.
87. Anja Lambrecht, *Measuring the Cost of Europe's E-Privacy Regulation,* Center for European Policy Studies, December 2017, https://www.ceps.eu/sites/default/files/Executive%20Summary%20-%20E-Privacy%20Provisions%20and%20Venture%20Capital%20Investments....pdf.
88. This is reinforced by multiple legal documents, including Article 7 of the Charter of Fundamental Rights (CFR), and Article 8 of the European Convention on Human Rights, which also enshrines the right to privacy. Article 16 of the Treaty on the Functioning of the EU (TFEU) frames "the protection of natural persons in relation to the processing of their personal data [as a] fundamental right," Treaty of Lisbon, 2007.
89. European Parliament, *Rules of Procedure of the European Parliament (2018). XVII. Committee on Civil Liberties, Justice and Home Affairs*, Brussels: European Union, July 2018, http://www.europarl.europa.eu/sides/getLastRules.do?language=en&reference=RESP-LIBE.
90. European Parliament, "Suspend EU-US data exchange deal, unless US complies by 1 September, say MEPs," REF: 20180628IPR06836, Brussels: European Union, July 5, 2018, http://www.europarl.europa.eu/news/en/press-room/20180628IPR06836/suspend-eu-us-data-exchange-deal-unless-us-complies-by-1-september-say-meps.
91. European Parliament, *Draft Motion for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP))*, March 10, 2018, http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf.
92. Ibid.