GLOBAL EMPLOYEE PRIVACY: A CASE STUDY ON THE MINEFIELD OF EMPLOYEE PRIVACY RIGHTS IN THE EU, USA, AND KSA

ADAM EICHELBERGER*

Countries have an urgent need to modernize their employee privacy laws, especially in the wake of the European Union's General Data Protection Regulation (GDPR).[1] This must be done not only to protect individual privacy but to clearly establish employer rules of the road and provide for stability in business transactions. This Note demonstrates why most modern privacy laws are inadequate, both to defend personal privacy and give employers peace of mind, through a comparative analysis of an employee's rights in the United States of America, the European Union (EU), and the Kingdom of Saudi Arabia. Then, this Note presents recommendations for protecting both employers and employees. By examining three different legal systems (common law, civil law, and quasi-religious law), their interactions with regards to employee privacy data, and the gaps between the systems, this Note calls for policy changes to enhance privacy protections both for the employee's benefit and the benefit of the employer managing a global workforce.

While much has been written about the consumer's right to privacy, far less has been said about the employee's right to privacy—including whether that right even truly exists in an international setting. This Note addresses those concerns. In Part I, this Note first considers the types of data employers have on their employees and the implications that data can have in the aggregate (so-called "Big Data").[2] Part I also lays out a hypothetical scenario to frame our examination of the law, setting the table for a detailed discussion of the current state of U.S. and international law.

Part II examines the current laws in the three different legal systems involved in the hypothetical—namely, the privacy and employment laws of the United States, the European Union, the Kingdom of Saudi Arabia, and the relevant international accords. For the United States, this includes a look at both the Federal and the State level, generally, but it is not a deep dive into the various state laws beginning to take shape. For the European Union (EU), this Note considers both the EU at large, and the implementing law of a model member

---

* J.D. Candidate, Indiana University Robert. H. McKinney School of Law, Class of 2022; B.S., Concordia University Wisconsin, 2006. The author was a 10-year Privacy officer and Acquisition Program Manager for the United States Army and former deputy CIO for the HQ United States Air Force A1 Staff over Manpower, Personnel and Services.

1. The GDPR is the European Union's overarching regulation to protect the data privacy of natural persons. *See Data protection in the EU*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en [https://perma.cc/8HJD-H4ZB].

2. Abyson Joseph, *Understanding the Basics of Big Data, Hadoop and SAP 'HANA' VORA*, SAP: Blogs (July 18, 2017), https://blogs.sap.com/2017/07/18/understanding-the-basics-of-big-data-hadoop-and-sap-vora/ [https://perma.cc/33JE-92J7] (explaining that "'Big Data' . . . is big volume of data that inundates a business . . . [m]ost digital process and social media produces Big Data").

state, Germany. Lastly, the Kingdom of Saudi Arabia gives us a look at a legal system different from both a common law and a civil law system to flesh out the comparative analysis.

Next, Part III takes the hypothetical scenario and examines it through the lens of the laws examined in Part II to determine what complementary and conflicting rights an employee has and how they might be enforced. Such analysis also displays any gaps in the law, and what those gaps mean to both employers and employees.

In Part IV, this Note lays out the principal argument: the international laws and U.S. laws around data privacy for employees, and the expectations of employers in protecting those rights, is wholly inadequate. This creates a quagmire of legal uncertainty for international businesses and for their employees. Nations ought to modernize their laws to accomplish the twin goals of protecting individual privacy and easing international commerce through defining risks and managing them.

I. DATA AND PRIVACY

More than at any time in human history data drives the global economy, business and government decision support systems, and prognostications the world over.[3] The type and volume of data collected is often called "Big Data," and it is worth a staggering amount of money (in the aggregate), both to employers and third parties, for reasons both obvious and obscure.[4] Big Data can tell an analyst everything from where someone would prefer to work, for whom he or she would prefer to vote, to the amount someone is willing to pay for various services.[5] This data includes everything from the data apps installed on your phone gather to bulk corporate and machine data such as sensors found on "medical devices, smart meters, road cameras, satellites, games and the rapidly growing 'Internet of Things' [which] generates high velocity, value, volume and variety of data."[6]

Inextricably linked with this data is the right of privacy.[7] While a great deal

---

3. *See* Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018, 12:42 AM), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/ [https://perma.cc/9TTY-VNXW].

4. Joseph *supra* note 2; Stephan Zoder, *How Much Is Your Data Worth?*, FORBES (Aug. 6, 2019, 2:57 PM), https://www.forbes.com/sites/stephanzoder/2019/08/06/how-much-is-your-data-worth/ [https://perma.cc/R8AU-GJCY].

5. *Id*.; Dan Patterson, *How Campaigns Use Big Data Tools to Micro-Target Voters*, CBS NEWS (Nov. 6, 2018, 11:01 AM), https://www.cbsnews.com/news/election-campaigns-big-data-analytics/ [https://perma.cc/F32D-S2MF].

6. Joseph, *supra* note 2.

7. Meera Jagannathan, *Your Employer Has More Confidential Data on you Than Amazon, Apple or Facebook*, MARKETWATCH (Aug. 4, 2019, 11:06 AM), https://www.marketwach.com/story/your-employer-is-tracking-your-every-move-is-it-too-late-to-do-anything-about-it-2019-07-24

of legal scholarship is focused on consumer privacy, much less has been said on employee privacy—and less still on employee privacy in the complex minefield of international law. It seems the legal field, like many employees, may be more comfortable giving up some privacy (perhaps more than realized) "for a paycheck."[8] To understand the full extent of privacy concerns, it is important to know specifically what data employers gather, and how valuable that data is.[9]

Companies track an incredible amount of data on their employees.[10] The type of data tracked varies from company to company, depending on its purpose, but almost universally includes payroll data and tax data (such as Social Security Numbers and bank account information in the United States) for obvious reasons (to pay employees). Other types of data, less universal, include location/geospatial data (such as a computer's IP address), physical location for assets and handlers (such as trucks and drivers), logging hours for truck drivers or other remote assets, etc. Still, other types of data include, as previously quotes, "[s]ensors such as medical devices, smart meters, road cameras, satellites, games and the rapidly growing 'Internet Of Things[.]'"[11] Companies might choose to gather data on employees' traffic patterns in the office through Radio Frequency Identity (RFID) tags inside company badges or individual keystrokes.[12] Some companies even track employee sleep patterns![13] In short, an employer might want to gather data on just about anything, which generates one or more of the four "Vs" of Big Data: velocity, value, volume, and variety.[14]

This data can be gathered by employee-provided means—such as filling out a logbook or a payroll form—or it could be gathered via autonomous means, such as through sensors or Internet of Things applications.[15] Companies gather this data for a variety of purposes, from process improvement, to efficiency analysis, to employee performance evaluations, to purposes previously unimagined. This

---

[https://perma.cc/NJM9-LU3A].

8. *See id*.

9. *Cf.* Joseph, *supra* note 2 (while the article explains that "[t]his kind of data provides invaluable insights into consumer behavior . . . and can be enormously influential in marketing analytics[,]" there is no reason why an employee's data would be considered any less valuable as they may also provide "invaluable insights," for instance as potential consumers or for process improvement).

10. *See generally* Ifeoma Ajunwa et al., *Limitless Worker Surveillance*, 105 CALIF. L. REV. 735 (2017).

11. Joseph *supra* note 2; *see generally* Jacob Morgan, *A Simple Explanation Of 'The Internet Of Things'*, FORBES (May 13, 2014, 12:05 AM), https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#7b6309f51d09 [https://perma.cc/9H9X-B22A] (defining the Internet of Things as what happens when many of your appliances, vehicles, and other devices are all connected, all the time, and capable of sharing data with each other on an unprecedented scale).

12. *See* Ajunwa et al., *supra* note 10, at 742.

13. Jagannathan, *supra* note 7.

14. *See* Joseph, *supra* note 2.

15. *See* Joseph, *supra* note 2.

data has proved transformational to the modern economy.[16] Much of this data is not personal in isolation but can become sensitive when aggregated with other bits of data.[17] In the United States, this kind of sensitive data is, *inter alia*, called Personally Identifiable Information ("PII").[18]

Much of this data is incredibly valuable whether it is personal data or not.[19] This data could also be used for far more than what the employee intended when he or she relinquished the data—if he or she even knew the data was being gathered at all![20] For example, consider that when an employer gathers information on the wear and tear of a truck's tires and locations traversed to maintain more accurate maintenance logs in an enterprise resource planning system, the employer has also gathered, *ipso facto*, a great deal of information, both explicit and implied, as to the quality of the driver (e.g., how the driver handles the asset, speed limits, turning pressure, braking pressure, stress on the truck, etc.). While initially, the employer may only care about the asset (the truck) in gathering the data, the employer may later realize the data reveals information about the driver that can be used to measure the driver's worth (or lack thereof) to employers.

Compounding matters, employers, subject to a few exceptions, can (and sometimes do) sell employee data to third parties.[21] This data, personal or anonymized, is valuable. People want it, and it makes sense if an employer is sitting on something of value to monetize it. For data brokers—people and firms who make their living profiling people using the very data those people

---

16. *See generally* Joseph Kennedy, *Big Data's Economic Impact*, IN THE NATION'S INT., COMM. FOR ECON. DEV., https://www.ced.org/blog/entry/big-datas-economic-impact [https://perma.cc/45P6-MXSV].

17. *What is Personal Data?*, EUR. COMM'N, https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en [https://perma.cc/HYW4-AUK5]; *accord* OFFICE OF MGMT. & BUDGET, M-07-16, SAFEGUARDING AGAINST AND RESPONDING TO THE BREACH OF PERSONALLY IDENTIFIABLE INFORMATION, n.1 (May 22, 2007).

18. Erika McCallister, Tim Grance & Karen A. Scarfone, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, NIST SPECIAL PUBLICATION 800-122, 2-1 (2010) [hereinafter NIST 800-122]. For purposes of this Note, the terms 'PII,' 'privacy data,' 'privacy related data,' 'privacy sensitive data,' and 'personal data' are all used interchangeably.

19. *Cf.* Kennedy, *supra* note 16. Kennedy points out that all the data feeding these Big Data engines could be worth "$3 trillion in value every year[.]" *Id*.

20. Ajunwa et al., *supra* note 10, at 737 (Management at a company installed a monitoring device under every desk. "Management initially justified the equipment as an effort to gather data on energy efficiency and promote environmental sustainability." In truth, "the devices were . . . provid[ing] detailed metrics on worker attendance." (citations omitted)).

21. Tam Harbert, *Watching the Workers*, SOC'Y FOR HUM. RESOURCE MGMT. (Mar. 16, 2019), https://www.shrm.org/hr-today/news/all-things-work/pages/watching-the-workers.aspx [https://perma.cc/7LT7-DFEM]; *see* Bob Sullivan, *EXCLUSIVE: Your Employer May Share Your Salary, and Equifax Might Sell That Data*, NBC NEWS (Jan. 30, 2013, 6:44 AM), https://www.nbcnews.com/technolog/exclusive-your-employer-may-share-your-salary-equifax-might-sell-1B8173066 [https://perma.cc/K7HK-M7HN].

provide—it is quite literally their way of life.[22] This sort of data is not only valuable to the employer and third parties, but also to thieves.[23]

If this were consumer data, the undisclosed sale of it would generate endless concern.[24] Consider, as demand for data increases, it is logical to assume third party sales would increase proportionally. Imagine an employee, otherwise competent and capable, has a terrible boss who eventually removes the employee after finding a sufficient excuse in that employee's data. What happens when third parties sell that data and employers turning to artificial intelligence for faster, smarter, decision making in hiring processes automatically begin filtering out such employees?

Because of these concerns, this Note posits that the same protections and considerations given to consumer data ought to apply to employee data. Employers need to know what risks are involved with employee data, how to manage those risks, and how to navigate complex global human resources issues not only with the data they hold but the jurisdictions in which they hold it. Ideally, this risk analysis would be done before seeking to monetize employee data.

To illustrate the complex weave of privacy concerns, this Note uses a specific setup which will be assumed throughout Part IV. In this hypothetical, the employer is a fictitious company named Fict-Data. Fict-Data is a United States based company that operates globally in a variety of fields and is a mid-to-large business with a revenue of between ten and twenty-five million dollars with just over 250 employees. Its principal place of business is in Indiana, and it is incorporated in Delaware. Fict-Data employs a German citizen by the name of Edrichtet. Fict-Data tracks all kinds of PII on Edrichtet, for various reasons described above. Fict-Data expatriated Edrichtet to the Kingdom of Saudi Arabia for several months.

Three separate legal systems and five different jurisdictions (the EU, Germany, Indiana, Saudi Arabia, and the United States) are now at play. Two of the jurisdictions are common law (Indiana and the United States). Two are civil law (EU and Germany). One is a mixture of civil law and religious law (Saudi Arabia). Buttressing these, some international frameworks and agreements define many the relationships between the countries.

What rights does Edrichtet have over the personal data gathered upon him while he is within Saudi Arabia? Is it even truly his data anymore, or has he surrendered all rights over the data to his employer? Should Edrichtet wish to exercise some control over the data, what rights does he have and what recourse

---

22. *See* Ashley Kuempel, *The Invisible Middlemen: A Critique and Call for Reform of the Data Broker Industry*, 36 NW. J. INT'L L. & BUS. 207, 210 (2016).

23. *Cf.* Nick Ismail, *Risk vs Reward – When Good Data Becomes Dangerous*, INFO.-AGE (Aug. 16, 2016), https://www.information-age.com/good-data-becomes-dangerous-123462179/ [https://perma.cc/L2ZB-V9TX] (while this article is aimed at Big Data being collected on consumers, nothing within it is inapplicable to the same sort of data being held by an employer over an employee—the same dangers apply).

24. Jagannathan, *supra* note 7; *accord* Ismail, *supra* note 23, *and* Marr, *supra* note 3.

is available to him to enforce these rights?

II. CURRENT STATE OF THE LAW

This Note now sets out current United States law (both Federal and State), current European Union—and member nation, German—law, and Saudi Arabian law. This Note sets out the law in that order, looking first at the U.S. common law system, then the EU's civil law system, the Saudi Arabia's unique blend of civil and religious systems.

A. United States

In the United States, there are few real or general protections for an employee's PII and little recourse for employees seeking to access, restrict, or remove their personal data from an employer. This section assumes the reader is familiar with the U.S. legal system and, as such, does not define the U.S. common law system. Instead, it is sufficient to state simply that the United States is a common law system and then dive into federal law. Then, this Note takes a brief look at the various laws different states are attempting to use to bridge this gap.

As this Note looks at the international dimension to privacy data, it does not deep-dive into state and local policy. However, it is important to keep in mind certain concepts of Federalism, such as the Rules of Decision Act and *Erie* doctrine, can complicate matters where a substantive state law needs to be applied in a federal court.[25] This can create a wrinkle when the state's law allows a recourse that federal law has not superseded via the supremacy clause.

Before considering state laws and their wrinkles, the federal framework and options need to be understood, as many of the terms and concepts used in state laws are derived from existing federal regulations.

i. Federally—A Patchwork of Regulation & Unclear Rights

While the United States lacks a general federal protection or rights for employee's PII,[26] there are a few narrow exceptions, such as various nondiscrimination laws (such as the Health Information Privacy and Portability Act, the Americans with Disabilities Act, and others) and requirements imposed on federal agencies and their contractors. Even these exceptions do not, as a rule, grant the employee rights to see his data, destroy his data, or correct his data, nor even to refuse the collection of such data; *ipso facto*, they often effectively undercut expectations of privacy.[27] Instead, the bulk of these protections only

---

25. 28 U.S.C. § 1652 *et seq*. (1948); *see generally* Erie R. Co. v. Tompkins, 304 U.S. 64 (1938).

26. Ajunwa et al., *supra* note 10, at 747 ("The federal laws that have been created for the benefit of workers focus instead on protecting them from employment discrimination while largely disregarding privacy claims.").

27. *Id*. at 748.

Due to the lack of explicit federal protection, most employees are or will be subject to

exist to protect against some form of discrimination and privacy is an afterthought.[28]

While the right to privacy is well established in federal law, [29] it is unclear exactly what types of PII fall under that right and what types do not. Knowing whether this right to privacy applies is important because an invasion of privacy cause of action must generally fall into one of "four analytically distinct torts: (1) intrusion upon seclusion, (2) appropriation of name or likeness, (3) publicity given to private life, [or] (4) publicity placing person in false light."[30] In general, in absence of a specific statutory right, courts seem reluctant to extend privacy rights to cover Big Data.[31] Put another way, without a specific statutory right, or some extremely compelling argument for a fundamental right, there is effectively no legal right for an employee to see, correct, or restrict the use of his or her personal data.

Despite a lack of blanket rights with regards to privacy data, there are several types of privacy data that are specifically protected, and a few sectors of the workforce are similarly protected.[32] Types of protected data include: personal—whether employee or consumer—medical data (protected under the Health Information Protection and Portability Act),[33] "dissemination of information obtained by the Department of Motor Vehicles . . . disclosure of tape rental or sales records[,]"[34] and a few other areas. It is important to note that, with the exception of medical data, all of these laws protect consumers, not employees.

Employees, it seems, are mostly limited to protections around the disclosure of medical data and prohibitions against data being used to discriminate against

---

> employer surveillance. It is well established, for example, that government employees (both federal and state) have no reasonable expectation of privacy at work; the employee's office or work space is subject to search by the employer without permission; and any electronic device provided to the employee by the employer generally remains the property of the employer, meaning that such electronic device could also be subject to search without permission.

Id. (citations omitted).

28. This Note does not cover laws like the children's online privacy protection act, as that does not affect the hypothetical setup described above.

29. *See generally* Griswold v. Connecticut, 381 U.S. 479 (1965) (The foundational case establishing that the Fourteenth Amendment creates a right of privacy); *accord* MARTIN A. WEISS & KRISTIN ARCHICK, CONG. RSCH. SERV., R44257, US-EU DATA PRIVACY: FROM SAFE HARBOR TO PRIVACY SHIELD, 3 (2016) [hereinafter CRS R44257] ("In the United States, respect for privacy is broadly enshrined in our Constitution.").

30. Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 FLA. L. REV. 365, 385 (2019).

31. *Id*.; *see* Kuempel, *supra* note 22, at 221 (2016) (stating that "[c]onsumers have little redress to ameliorate the privacy and discrimination concerns raised by big data." In absence of law to the contrary, it is reasonable to assume this is the same for employees).

32. CRS R44257, *supra* note 29, at 3.

33. 42 U.S.C. § 1320d-6 (2009).

34. Kuempel, *supra* note 22, at 216.

them as a protected class (race, gender, DNA, age, or the like).[35] Putting together these few protections that exist, it seems fair to characterize federal law as impliedly or explicitly allowing all data an employer wishes to collect to be so gathered. Employee protections only trigger after some kind of damage has been done. There is no presumptive ability or right recognized to allow an employee to see his or her data.[36]

One exception exists that covers somewhere in excess of seven million employees: the federal workforce.[37] The Federal Acquisition Regulation (FAR) requires all contracts between the government and a contractor where the contractor is involved in the "design, development, or operation of a system of records on individuals . . ." to insert clauses mandating the protection of PII through compliance with the Privacy Act.[38] The Privacy Act defines "[S]ystem of records" as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual[.]"[39]

In addition to the FAR, other federal laws require contractors and subcontractors to comply with relevant information security and privacy guidance for handling privacy sensitive data.[40] While a variety of guidance exists in each

---

35. *See* Ajunwa et al., *supra* note 10, at 747 *et seq.* (listing various types of protected data that is allowed, either implicitly or explicitly, to be collected and used, merely prohibited from being used to discriminate).

36. Compare this lack of a right to see one's own data to the Fair Credit Reporting Act, where a consumer has the ability to see and dispute his or her credit-agency collected privacy data. 15 U.S.C. § 1681 *et seq*. (1970) ("There is a need to insure [sic] that consumer reporting agencies exercise their grave responsibilities with fairness, impartiality, and a respect for the consumer's right to privacy.").

37. CONG. RSCH. SERV., R43590, FEDERAL WORKFORCE STATISTICS SOURCES: OPM AND OMB, 6 (2019) [hereinafter CRS R43590] (stating there are approximately 4.2 million full-time equivalent federal employees); Neil Gordon, *Contractors and the True Size of Government*, PROJECT ON GOV'T OVERSIGHT (Oct. 5, 2017), https://www.pogo.org/analysis/2017/10/contractors-and-true-size-of-government/ [https://perma.cc/92TH-HWXS] (citing to reports showing an estimated 3.7 million federal contractors).

As the hypothetical in Part I does not concern a federal employee, this Note will only look at regulations affecting federal contractors and subcontracts as Edrichtet, the employee, may be a contractor or subcontractor even without realizing, despite being a foreign national as far as the United States is concerned. *See supra* Part I.

38. 48 C.F.R. § 52.224-2.

39. 5 U.S.C. § 552a(a)(5) (2014). While there is an argument that many contractor owned and operated systems have or are becoming unauthorized systems of record, that argument is beyond the scope of this note.

40. NIST 800-122, *supra* note 18, at 2-1 (stating orgs must identify and control data "under the control of their organization through a third party (e.g., a system being developed and tested by a contractor)"); *accord: see* 5 U.S.C. § 552a (2014) (the Privacy Act); 44 U.S.C. § 3551 *et seq*. (2019) (Federal Information Security Modernization Act of 2014 (FISMA2014)).

agency, they are mostly based on—and often point to—the *Guide to Protecting Confidentiality of PII* (commonly called NIST 800-122), published by the National Institute of Standards & Technology (NIST).[41] NIST 800-122 defines PII broadly as data that traces or distinguishes an individual, including data that is not privacy sensitive in and of itself but becomes privacy sensitive through aggregation (that is, data that is linkable).[42] Further, NIST 800-122 follows the Organisation for Economic Co-operation and Development (OECD)'s fair information practices, including limiting the collection of data and encouraging individual participation, meaning that an employee

> should have the right: (a) to obtain . . . confirmation of whether or not [a] data collector has data relating to him . . . and (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed, or amended.[43]

To date, there are no court cases using NIST 800-122 breaches as showing a breach of privacy, so it remains a legal uncertainty what the standard of care a federal contractor must exercise is. However, even if one can show a breach of the duty of care, the only causes of action explicit in the law authorizing the protection of PII are in the Privacy Act, and it does not grant the employee rights; instead, the Privacy Act forbids willful unauthorized disclosure or maintenance of data without giving proper notice.[44] There are no express causes of action given to an employee over a breach of his or her NIST 800-122 right to have erased.

Lastly, even for sectors that have protections like federal employees and contractors, there are no federal protections for workers to know, have access to, or limit how their companies use personal data with third parties. These third parties are often where the valuable data, or the Big Data, becomes truly valuable to companies.[45] While perhaps an employee could attempt privacy based substantive due process claim around his or her autonomy being impeded over such actions, there is no solid case law to point to suggesting the court would even recognize the action sans some real, concrete, and measurable damage which has happened or is imminent, and not simply "conjectural or hypothetical."[46]

In summation: current federal law is a patchwork of laws, policies, and regulations, kludged together on a sector-by-sector approach that affords little real protection. While the federal government has imposed a much stronger standard for data transparency on itself and its contractors, the right of action does

---

41. *See generally* NIST 800-122, *supra* note 18.

42. NIST 800-122, *supra* note 18, at 2-1.

43. *Id*. at 2-3. NIST 800-122 goes on to cover a risk management of PII in detail, including assessing confidentiality impact levels, none of which are directly relevant here.

44. 5 U.S.C. § 552a(i)(2).

45. *See supra* Part I.

46. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2019) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

not explicitly uphold an employee's ability to challenge data collection and exchange with data brokers. Similarly, legal protections in the United States are focused heavily on preventing discrimination, not protecting individual's rights to data privacy. While an implied right may exist, courts have been reluctant to extend the constitutionally granted right of privacy beyond that which is explicitly authorized.

ii. State Law—Indiana

Where federal laws are silent or set a floor, the states can fill the void or supplement on their own. Fict-Data is an Indiana company, incorporated in Delaware, meaning that an employer must also consider the laws of Indiana (Delaware's laws are silent on data privacy). Liability may not only result from a federal question but could also be a matter of state law in Indiana.

Indiana has two relevant sections of its legal code that offer some measure of protection, although both are vastly weaker than their federal counterparts. One section of the Indiana Code deals with state agencies, and another section deals with how businesses handle privacy data. As with the previous analysis of federal law, Fict-Data may be a State contractor, requiring an examination of both the requirements on contractors for the State and the law with regard to businesses handling privacy data.

For State agencies, Indiana Code protects all persons from the State disclosing any person's Social Security number, except as allowed in the code.[47] However, the same code also explicitly exempts the disclosure of only the last four digits of a person's Social Security number, affirmatively stating that Indiana does not consider releasing those four digits as a breach of a person's PII.[48] This is both weaker and more troubling than federal protections because the only part of a person's Social Security number that has any semblance of uniqueness is the last four (known as the "serial number" portion of the code).[49] Another key difference between Indiana law and federal law is that Indiana contractors are not required to follow the same privacy restrictions binding on State agencies; instead, the State of Indiana de facto requires tighter controls on privacy data for its contractors by requiring its contractors to not have violated Indiana law on

47. IND. CODE § 4-1-10-1 *et seq*; NIST 800-122, *supra* note 18, at n.21 ("Partial identifiers, such as the first few digits or the last few digits of SSNs, are also often considered PII because they are still nearly unique identifiers and are linked or linkable to a specific individual.").

48. IND. CODE § 4-1-10-3.

49. *See The SSN Numbering Scheme*, SOC. SEC. ADMIN., https://www.ssa.gov/history/ssn/geocard.html [https://perma.cc/HQP3-322E]. The Serial Number is the most sensitive portion of a person's Social Security Number. The Area Number and Group Number for the first five digits of a Social Security number are not random; instead, they are a matter of public record and easily known with just a little searching. This means if an actor knows a person's place of birth and year, the first five numbers can easily be ascertained with complete accuracy. Because of this, the last 4 are the part of a person's Social Security Number most in need of protecting. *Id*.

how businesses handle privacy data within the last year.[50]

Indiana law requires anyone doing business in Indiana (except for State agencies) to protect personal information from unauthorized disclosure.[51] However, the meaning of "personal information" is not the same here as it is in the rest of this Note. Instead, Indiana law considers personal information to be limited to a:

> (1) a Social Security number that is not encrypted or redacted; or
> (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted:
> (A) A driver's license number.
> (B) A state identification card number.
> (C) A credit card number.
> (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.
> The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.[52]

This is not as limiting as it seems at first blush. The Indiana Code's definition of personal information is far less encompassing than the language used in NIST publications.[53] Perhaps confusingly, the Indiana Code also redefines PII more than once in other sections of the Code in ways that differ greatly from NIST.[54] Further, Indiana law specifically exempts many types of data covered by federal law.[55] Lastly, unlike several federal laws, Indiana law is not aimed at consumers, but at all personal information, treating employees the same as consumers.[56]

As with federal law, however, a requirement to protect data is only as good as the enforceability of that requirement. Here, Indiana suffers from many of the same problems as the federal government: there are no general protections or rights for an employee to see his or her data, and only the failure to disclose a data breach is a punishable offense with either injunctive relief or a civil penalty of "not more than one hundred fifty thousand dollars" per act, with either action

---

50. IND. CODE § 5-22-3-7.

51. *Id.* § 24-4.9-3-3.5.

52. *Id.* § 24-4.9-2-10.

53. NIST 800-122, *supra* note 18, at 2-1.

54. IND. CODE § 24-4.8-1-10. PII here contains a reference to Title 35 of the Indiana Code where PII is redefined at least twice more, causing the term to become context sensitive and potentially confusing to parse.

55. *Id.* § 24-4.9-3-3.5.

56. *Id.* § 24-4.9-3-1; *but see id.* § 24-4.9-3-1(b) (specifically calling out a special reporting requirement for data breaches on databases holding more than one thousand consumers' information).

being enforceable only by the attorney general.[57] In summation: an employee has the right to know when his or her data has been compromised, but no right to see, correct, or personally seek redress for the misuse of that data under Indiana law.

Indiana's lack of clear liability or enforceability is not unique to the state. In fact, it is frighteningly common, but a few states have taken different approaches, such as Delaware and Connecticut. In these two states, the different approach is simple but important: employers must inform employees of electronic tracking (such as tracking their movements on a cell phone, or GPS positioning).[58] In Delaware's case, this requirement to notify applies only to companies with a place of business within the state and not to businesses merely incorporated there.[59]

Out of all the States in the Union, only California offers a substantially different framework for how individuals and companies are to handle data privacy rights. However, Fict-Data has no connection to California in the hypothetical, so this Note will not cover the California Consumer Privacy Act (CCPA).[60]

B. The European Union

Unlike the common law system of the United States, the European Union and Germany (like most EU member states) are civil law based; that is, these

---

57. *Id.* § 24-4.9-4-2.

58. Ajunwa et al., *supra* note 10, at 743.

59. *See* DEL. CODE TIT. 19, § 705(a) (2019). Recall that Fict-Data is only incorporated in Delaware, as are most other U.S. companies, so this law bears no further examination in this Note.

60. CAL. CIV. CODE § 1798.100 (2019) *et seq*.

California has a comprehensive set of protections for its citizens known as the California Consumer Privacy Act (CCPA). This law applies to businesses doing business in California, gathering personal information on California consumers and requires such businesses to not only notify consumers (who ask) what data the company tracks on them but also allow them to opt out of such data collection and resale. *Id.* § 1798.135 (2019). Violations of the law are punishable by a civil penalty not to exceed $2,500 per violation, or $7,500 for an intentional violation. *Id.* § 1798.155 (2019). No cases yet exist to help illustrate how the CCPA is to be interpreted as the law was just enacted as of January 2020. *Id.* § 1798.198 (2019).

Unlike Indiana law, California's privacy law presumably extends to employees, as long as they are California residents and uses a broad definition of privacy information more akin to the Federal government. *Cf. id.* § 1798.140(g) (2019) (the definition of 'consumer' is "any natural person who is a California resident . . . however identified[;]" a logical extension of this plain-text reading is that all employees who fit that definition are also consumers); *id.* § 1798.140(o) (2019). Read with previous sections, this means any business hiring a California-resident employee would have to provide him or her with an opt out, or else potentially face a potential civil penalty. For employers hoping to lean on a waiver in their employment contracts, a further provision states, "[a]ny provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights . . . shall be deemed contrary to public policy and shall be void and unenforceable." *Id.* § 1798.192 (2019).

jurisdictions have their primary law in constitutions and statutes only.[61] While civil law systems do show some reticence to issue contradictory judgments in court, they are not bound by concepts like stare decisis.[62] As such, this Note looks more to the plain meaning of the statutes and only consults court decisions that help illustrate a point or a trend in how the European or German courts are interpreting statutes.

i. EU—Comprehensive Protections and their Limits

Unlike the United States, the EU does have a comprehensive privacy protection law in the form of the General Data Protection Regulation (GDPR).[63] The EU's legislature used the GDPR to set forth an affirmative stance in its recitals that "the protection of natural persons in relation to the processing of personal data is a fundamental right."[64] However, the same recitals acknowledge that the protection of data "is not an absolute right."[65] So, there is a bit of a gray area in exactly how far one can push the protection of personal data.

The GDPR is a revision and replacement of the Data Protection Directive of 1995, which was intended "to create uniform rules and privacy standards among member countries."[66] However, the legal community in the EU eventually coalesced around certain weaknesses in the Data Protection Directive that made it untenable in the long run: consent was nominal consent (*e.g.*, buried consent terms in a click-through paragraph); unclear definitions of personal data; ineffective measures of transparency; focusing on the process of gathering instead of data use; as well as other weaknesses and incoherencies.[67] Presumably, in replacing the Data Protection Directive, the GDPR was intended to rectify prior errors and establish a strong defense of individual privacy.

The GDPR is very broad in scope and is intended to encompass all PII processed "wholly or partly by automated means" including data merely intended to "form part of a filing system or are intended to form part of a filing system."[68] The GDPR defines its territorial authority as broadly as its scope, covering data controllers established in the EU, even if the data is processed outside the EU,

---

61. HEIDI FROSTESTAD KUEHL & MEGAN A. O'BRIEN, INTERNATIONAL LEGAL RESEARCH IN A GLOBAL COMMUNITY 189 (2018).

62. *See id*. at n.17 (2018).

63. *See generally* Regulation (EU) 2016/679, 2016 O.J. (L 119).

64. *Id.* at 2.

65. *Id.* at 4.

66. Edward Alo, *EU Privacy Protection: A Step Towards Global Privacy*, 22 MICH. ST. INT'L L. REV. 1095, 1105 (2013).

67. *See generally* J.C. Buitelaar, *Privacy: Back to the Roots*, 13 GERMAN L. J. 171, 177-182 (2012) (section C covers many weaknesses of the Data Privacy Directive); *accord cf. id*. at 1117 (2013) (listing the "fragmentation and incoherence under the Privacy Directive[,]" as reasons for the GDPR).

68. Regulation (EU) 2016/679, *supra* note 63, at 32, 34.

and controllers established outside the EU.[69] However, there are some limitations on controllers established outside the EU (such as Fict-Data in this Note's hypo), such that they must either be in a place where an EU member's state law applies, the controller is selling a product to an EU citizen, or the controller is "monitoring [a person's] behavior as far as their behavior takes place within the Union."[70]

Because of the complexity and relative thoroughness of the GDPR, it is helpful to consider the rights and obligations that the GDPR puts on collectors and collected from a cradle-to-grave (or collection-to-disposition) manner. That is, to start the analysis with when a data processor is allowed to collect and end with what happens at the disposal of the data.

Data collection begins in Article 6, where the GDPR also takes a very different approach than U.S. law, stating that processing PII is only lawful if it fits in one of these six principles:

> (1) Processing shall be lawful only if and to the extent that at least one of the following applies:
>
> (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
>
> (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
>
> (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
>
> (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
>
> (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.
>
> Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.[71]

This stands in sharp contrast to the United States, where processing PII is presumed legal unless it is explicitly forbidden or otherwise restricted.[72] Consider this Note's hypothetical: Fict-Data has a need to gather Edrichtet's data. That need could fall under the aforementioned reasons, except subsection (e)—Fict-

---

69. *Id*.
70. *Id.* at 33.
71. *Id.* at 36.
72. *See supra* Part II.A.

Data presumably does not have a public interest argument or official authority.[73] However, even though any given company has an authorized reason to collect, the GDPR does also put one final hard-stop on data gathering where the data reveals "racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership," as well as anything surrounding sex life, sexual orientation, or biometrics used to uniquely identify someone.[74]

While this note previously defined PII, in the context of EU law, it is also important to understand how the Court of Justice of the EU (CJEU) is treating data and metadata (that is, data that tells the data processor or another consumer about the underlying data).[75] Metadata can be as valuable as the underlying data, the CJEU has acknowledged that metadata itself also needs a reason for lawful processing, as described above, in various recent cases.[76] Due to this trend in the CJEU, companies need to consider their metadata, as well as their data.

In the EU, assuming a data collector gets past Article 6, and, thus, has an approved reason to collect the data, the data subject (that is, the person about whom an entity is collecting data), has the right to a few things: (1) the right to view his or her data, (2) the right to correct his or her data, (3) the right to have his or her data erased (the "right to be forgotten"), (4) the right to restrict the use of his or her data, (5) the right to data portability, and (6) the right to object to automated decision making using his or her data.[77] Each of these rights is an important piece of the whole, but they must be carefully attenuated through the employer-employee relationship and not simply any natural person that a company is collecting data on, especially where member nations' laws are concerned as this Note considers in the next subsection.[78] However, as the right to see and correct data are fairly self-explanatory, this Note will not examine them any further. Similarly, the right to data portability can be summarized as a person has the right to see his or her data in a common, readable format, and needs no further examination.[79] Instead, the rights of erasure, restriction, and objection to automation are what require more expounding.

---

73. *See supra* Part I.

74. Regulation (EU) 2016/679, *supra* note 63, at 38.

75. *See supra* Part I; *see generally* Jason Hare, *What Is Metadata and Why Is It as Important as the Data Itself?*, OPENDATASOFT (Aug 25, 2016), https://www.opendatasoft.com/blog/2016/08/25/what-is-metadata-and-why-is-it-important-data [https://perma.cc/RX3R-F2FB] (defining metadata and explaining why it is often as valuable as regular data).

76. Hare, *supra* note 75; *see* Maja Brkan, *The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning*, 20 GERMAN L. J. 864, 873 (2019) ("Metadata can thus reveal information about an individual's sensitive data, whose processing is in principle prohibited by the [GDPR], unless one of the exceptions applies." (citation omitted)).

77. Regulation (EU) 2016/679, *supra* note 63, at 43-46.

78. *See id.* at 84 (member nations can create more specific rules regarding the employer-employee relationship, so long as those rules "include suitable and specific measures to safeguard" the employee's interests, as well as the employer).

79. *See id.* at 45.

On erasure, the GDPR, in Article 17, gives a person the right to have all data erased, so long as one of six broad criteria is met: (1) the PII is "no longer necessary in relation to the purposes for which [it was] collected[,]" (2) the person withdraws consent and there is no other legal ground, (3) the person invokes their right to object and there is no "overriding legitimate grounds for the processing," (4) "the personal data have been unlawfully processed[,]" (5) a member state's law creates a legal obligating allowing for deletion, or (6) the data was collected from a child for information society services.[80] As long as one of those conditions is met, and in the absence of some other exception, the data processor must delete the data.[81] Presumably, a former employee, or an employee moving to another task than the one PII was collected for, could claim there is no longer a need.

However, assuming an employee is correct about the data no longer being necessary, this is where a few exceptions may get in the employee's way. The GDPR limits the right of erasure where the use of the data is necessary to meet "scientific or historical research purpose," which would likely encompass any business process improvement activities.[82] Efficiency studies and productivity improvement have legitimate business purposes and are increasingly facilitated by Big Data analytics, including PII.[83] Where a company can render its employee's data anonymous, this will especially hold true as the Charter of the GDPR explicitly states in paragraph 26, that these "data protection[s] should . . . not apply to personal data rendered anonymous in such a manner that the data subject is . . . no longer identifiable."[84]

The right to restrict means that a person can withdraw consent to having their collected data used in any way, other than mere storage, unless explicitly consented to or the processor must use the data for a legal reason.[85] As with erasure, this right only applies where the person can meet at least one of four listed criteria: (1) data subject is contesting the data accuracy, (2) unlawful processing, (3) controller no longer needs the data, or (4) the data subject exercises their right to object to automated decision-making.[86] In the context of an employer-employee relationship, it is conceivable that any of these could be legitimate reasons for the employee to restrict access to his or her data. Should an employee exercise this right, then all of his or her personal data—remember that would include any data linked to that personal data, this can end up being a very broad cut of data—is frozen and shall not be processed in any way, except as necessary for exercise or defense of legal claims, protection of another's rights,

---

80. *Id.* at 43-44.

81. *Id*.

82. *Cf.* Rustad & Koenig, *supra* note 30, at 396 (noting how Microsoft became GDPR compliant yet was still able to advertise its ability to improve "firms' agility and efficiency" through big data).

83. *See supra* Part I.

84. Regulation (EU) 2016/679, *supra* note 63, at 5.

85. *Id.* at 44.

86. *Id.* at 45.

or "reasons of important public interest[.]"[87] Sadly, there are no cases or further guidance expounding what "reasons of important public interest" might mean.

Lastly, the right to object is bifurcated into two separate rights: the right of a person to object to his or her data being processed, and the right of a person not to be subject to automated decision making about him or her.[88] The first right to object, as it is aimed more at a person's ability to refuse to have his or her data used for direct marketing, is not of concern to this Note because the employer has a legitimate interest in obtaining and processing the data.[89] The GDPR, in Article 22, guarantees a person "the right not to be subject to a decision based solely on automated processing . . . which produces legal effects concerning him or her or similarly significantly affects him or her."[90] However, that right is explicitly attenuated in the light of performing on a contract placed between the data processor and subject, such as an employment contract.[91]

Consider just how many automated processes might be based "solely on automated processing," especially as artificial intelligence and Big Data become more heavily relied upon. Performance management, workforce administration, and workforce planning are all becoming highly automated, to the point where automation systems may start making decisions based on human-fed metrics for what the organization should look like.[92] If an automated tool analyzes the workforce structure, determines three widget turners are no longer necessary, and eliminates the three who, based on metrics put into the system, are below the other widget turners, this right would ostensibly protect those three workers. That decision would be something that significantly affects the three workers. The protection is ostensible because that assumes the workers objected to automated decision-making, and that no human stepped in to give a nominal blessing on the

---

87. *Id*.

88. *Id.* at 45-46.

89. *See id.* at 45. The right to object is as broad as simply asserting, 'I object,' and is similarly broadly defeated by the company asserting a legitimate reason to process data, per Article 21. *Id*. While an employer might use a person's PII for direct marketing purposes, such use would mean the employer is treating the employee as a consumer and all of the relevant consumer safeguards should apply, thus being outside the scope of this Note.

Just the same, if this Note assumed a company lacked a legitimate interest in processing the employee's PII, then the analysis in a legal hypothetical would not even pass the Article 6 lawful purpose test. *Id*. at 36. In either case, while such analysis may be interesting, it is, ultimately, outside the scope of this note. It is sufficient to acknowledge such a right to object exists and move on.

90. *Id.* at 46.

91. *See id*.

92. *Cf.* David Tobenkin, *HR Needs to Stay Ahead of Automation*, SOC'Y FOR HUM. RESOURCE MGMT. (Feb. 26, 2019), https://www.shrm.org/hr-today/news/hr-magazine/spring2019/pages/hr-needs-to-stay-ahead-of-automation.aspx [https://perma.cc/YRA4-3B6X] (citing to a KPMG study demonstrating the effectiveness of automation and AI in taking over a most of the lifecycle of traditional manpower activities).

artificial intelligence's decision making.[93] If the first is not satisfied, or the second is satisfied, then there is no real protection here.

An important consideration over all of these rights is the wrinkle of extraterritoriality. In the September 2019 CJEU opinion on the matter of *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)* (where the French Supervisory Authority, CNIL, sued Google for failing to de-reference data to be forgotten from all its servers), the court said, "the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights[.]"[94] That is, the right of internet users to have access to information must be balanced against the right to erasure, and those rights will vary all over the globe.[95] That balancing test is vitally important to understanding the territoriality limits on exercising these rights. The CJEU's Advocate General summarized the importance of this balancing test in a lower court opinion on the same matter, "EU regulators cannot reasonably be expected to make this balancing test for the entire world[,]" and that this obligation would be harmful by allowing "third countries eager to limit access to information[,]" to do so.[96] In practical summation, the CJEU seems to be saying that a data processor only has a responsibility to eliminate data from EU-based servers and from appearing in EU-based data searching or mining.[97]

There is one further obligation that bears special attention: the requirement to designate a Data Protection Officer (DPO).[98] DPOs have chief responsibility for ensuring compliance with the rights and responsibilities established in the GDPR.[99] They are the "belly button" of an organization for all things having to do with data privacy and data protection. Companies are free to appoint (or not) a DPO unless they fall into a category of mandatory appointment: (1) processing PII for a public authority; (2) the company's core activities "require regular and systematic monitoring of data subjects on a large scale;" or (3) the company processes data related to race, ethnicity, sexual orientation, religious belief, political opinions, health, or criminal convictions.[100] Reasons (1) and (3) are self-

---

93. *See* Regulation (EU) 2016/679, *supra* note 63, at 46. It remains unknown exactly how much of the decision making has to be done by human intervention in order to meet the standard. It may be that a human intervening simply to concur with the machine's decision is not enough to meet the statute, but, by the plain text, it appears that would be enough.

94. Case C-507/17, Google, LLC v. CNIL, 2019 INFOCURIA, ¶ 60 (Sept. 24, 2019).

95. *See id*.

96. Kristof Van Quathem, *EU Advocate General: Right to be Forgotten is Limited to EU*, INSIDE PRIV'Y (Jan. 11, 2019), https://www.insideprivacy.com/data-privacy/eu-advocate-general-right-to-be-forgotten-is-limited-to-eu/ [https://perma.cc/Y3GJ-BS7L] (Quathem provides a translation of the Advocate General from French to English).

97. *See* Kristof Van Quathem et al., *GDPR's Right to be Forgotten Limited to EU Web-Sites*, INSIDE PRIV'Y (Sept. 24, 2019), https://www.insideprivacy.com/eu-data-protection/gdprs-right-to-be-forgotten-limited-to-eu-websites/ [https://perma.cc/9L83-HKTC].

98. Regulation (EU) 2016/679, *supra* note 63, at 55.

99. *Id.* at 56.

100. *Id.* at 55.

explanatory, but reason (2) requires more careful consideration.

Determining if a private company must have a DPO under reason (2), rests on two key phrases: "core activities" and "large scale." On core activities, all (or nearly all) companies engaged in some form of Big Data analytics on their employee performance, or for process improvement, will have to conduct some form of regular and systematic monitoring to feed their predictive analytics systems the requisite data.[101] However, this does not mean that such regular and systematic monitoring is core to the company's activities, instead of being simply an ancillary activity necessary to conduct analytics, which would excuse the requirement for a DPO.[102] Yet, there is a wide gray area of what is considered "core" and what is "ancillary;" the EU's supplemental guidance DPO indicates that in such gray areas, one should err on the side of requiring a DPO, unless the activity is truly, obviously, ancillary.[103]

The second key requirement is that the core service must involve processing of PII on a "large scale."[104] This term is ambiguous, at best. As the implementing guidance for DPOs states:

> According to the recital, *'large-scale processing operations which aim to process a considerable amount of personal data at regional, national or supranational level and which could affect a large number of data subjects and which are likely to result in a high risk'* would be included, in particular. On the other hand, the recital specifically provides that *'the processing of personal data should not be considered to be on a large scale if the processing concerns personal data from patients or clients by an individual physician, other health care professional or lawyer'*. It is important to consider that while the recital provides examples at the extremes of the scale (processing by an individual physician versus

---

101. *See supra* Part I.

102. Regulation (EU) 2016/679, *supra* note 63, at 18.

103. *See* Guidelines on Data Protection Officers ('DPOs'), EUR. COMM'N WP 243, at 7 (Dec. 13, 2016). Four examples are given in section 2.1.2 ('Core Activities'). The first is hospitals, which consider health care their core activity. Health care requires service providers to track a considerable amount of PII, so even though it is ancillary, it is closely related enough to the core service to be considered core. The second example is private security companies monitoring shops and public spaces. "Surveillance is the core activity, which is inextricably linked to the processing of personal data." This also requires a DPO.

The third and fourth examples are payroll and IT services. Both would require some level of tracking personal data. Both are truly ancillary to the actual core service of the company and are only conducted because every company must conduct them. "Even though these activities are necessary or essential, they are usually considered ancillary functions rather than core activities." Thus, as truly ancillary data, they are not "core."

From these examples one can see a clear trend pushing for erring on the side of over-inclusion rather than under, and only in the case of gray areas that are well-and-truly, obviously ancillary, should the service be considered non-core.

104. Regulation (EU) 2016/679, *supra* note 63, at 55.

> processing of data of a whole country or across Europe); there is a large grey zone in between these extremes.[105]

The same guidelines further attempt to elucidate the concept by affirming that there is no precise number or metric to determine what constitutes large scale.[106] Instead, the guidelines recommend a series of factors involving the number of persons being tracked, the volume of data, the duration of data processing, and the geographical extent.[107] While the first three factors are simple enough to understand, if only in abstract terms while much less so real terms, the last factor, geographical extent, is the most nebulous in both the abstract and the real. The same guidelines provide us with only one example of processing "real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialized in providing these services[.]"[108] That single example is too attenuated to provide true insight into whether geo-location tagging on a truck would fall under the geographical extent factor.

In sum, the EU has a comprehensive set of rights—viewing, erasure, rectification, restriction, and objection—giving a person considerable control over how his or her data is used. These rights are intended to have a broad reach, but the limits of extraterritoriality must be considered when determining how to apply some of these rights, as must the balancing of other fundamental interests such as freedom of information. Further, these rights and restrictions to lawful processing apply not only to data but often to metadata as well. While some restrictions may be attenuated by the legitimacy of a need to process data in an employer-employee relationship, the same rights broadly apply. To enforce these rights, companies who have core services related to PII, as long as the relationship is stronger than being completely and obviously ancillary, have an obligation to appoint a Data Privacy Officer. What constitutes a mandatory appointment of a DPO is often unclear, but companies are allowed to appoint one even if it is not mandated. Overall, of these rights, restrictions and obligations, EU member countries can also introduce their own laws supplementing the GDPR.

ii. German Law

One year after the EU adopted the GDPR, Germany responded by updating its privacy regulation, the Bundesdatenschutzgesetz (BDSG, or the Federal Data Protection Act). The BDSG has existed since 1990 and was a replacement to one of, if not the earliest statutes on information privacy, the German Datenschutzgesetzgebung.[109] The current BDSG supplements the GDPR through

---

105. Guidelines on Data Protection Officers ('DPOs'), *supra* note 103, at n.14.

106. *Id.* at 7.

107. *Id*.

108. *Id.* at 8.

109. Tatjana Zrinski, *EU GDRP vs. German Bundesdatenschutzgesetz – Similarities and Differences*, EU GDPR ACAD., https://advisera.com/eugdpracademy/knowledgebase/eu-gdpr-vs-german-bundesdatenschutzgesetz-similarities-and-differences/ [https://perma.cc/859Z-9YUS].

the use of the GDPR's "opening clauses," and is explicitly subservient to the GDPR where the two regulations both directly apply to a situation—similar to how the Supremacy Clause works in U.S. law.[110] Accordingly, this Note only concerns those areas of the BDSG which expand, contract, or significantly differ from the GDPR.

As with the GDPR, the BDSG's scope is broad, but it is also considerably more specific as to how it applies to public bodies and private bodies (e.g., governments and companies, respectively).[111] For companies not located within Germany, or another EU member state, the BDSG relies on the GDPR's territorial scope provisions—*i.e.*, if a company not within an EU Member State would fall under the GDPR, then the BDSG also applies.[112]

The BDSG makes three alterations to the GDPR which are of concern for this Note: (1) express permission to process gathered data for purposes other than which the data were gathered, (2) specific provisions for data processing related to employment-related purposes, and (3) more specificity to the right of erasure.[113] On the first, the BDSG allows a processor to use data other than for its original purpose if such processing is either necessary to prevent threats to public safety, prosecute a criminal charge, or establish a legal defense, "[u]nless the data subject has an overriding interest in not having the data processed."[114] On the right to erasure, the BDSG introduces an explicit reasonability limit to the GDPR's right to erasure: in cases where data is non-automated (or where the erasure thereof would be non-automated) and the erasure is either impossible or involves disproportionate effort relative to the risk the PII presents, the data subject has no right to erasure.[115] Put another way, if the data is stored and used in a too inefficient manner, the subject does not have a right to have the data erased. While this would seem to incentivize having a terrible data structure, said terrible data structure would also hamper most, if not all, the risks and benefits of Big Data.[116] One important caveat: if the processor gathered the data illegally, he or she must erase it upon request regardless of the difficulty or even impossibility involved.[117]

Most important among the BDSG's alterations, for this Note's purposes, is

---

110. BUNDESDATENSCHUTZGESETZ (BDSG) [Federal Data Protection Act] § 1(5), June 30, 2017; U.S. CONST. art. VI, ¶ 2. Note, the author does not know German, any references to or quotes from the BDSG refer to the English version of the BDSG. Whatever discrepancies this may cause are unlikely to be significant for this Note's objective.

111. BDSG § 1.

112. *Id.* § 1(4)3.

113. *Id.* §§ 24, 26, 35.

There are some other specifications and minor alterations—such as a change to how the right to automated decision making is handled, but only in the context of providing insurance services which are not of concern in this note's scenario. *Id*. § 37.

114. *Id.* § 24.

115. *See id.* § 35.

116. *See supra* Part I.

117. BDSG § 35.

the right to process an employee's personal data for personnel actions (*e.g.*, hiring, firing, satisfying obligations of collective bargaining), its limitations, and how the power dynamic between the employer and the employee is an explicit factor in weighing this right.[118] The BDSG, while granting employers a right to process PII broadly in execution of its human resource related issues, gives specific protections to the employee against the processing of his or her data to detect crimes.[119] Additionally, the BDSG does not consider consent to the data usage to be, necessarily, enough to allow its processing.[120] Instead, one has to consider the employee's consent in light of his or her dependence on the employer and the total circumstances surrounding the giving of consent.[121] Regardless of how common such consent-basis may be in Germany, it ought to be of note for international employers who may be subject to the BDSG through their employees.

Many provisions within the BDSG include extra protections for when the data subject has "an overriding interest in not having the data processed."[122] To understand what an "overriding interest" means requires one to understand what the German idea of privacy as a right means. Without a clear understanding of what emphasis German society places on privacy, it would be nigh impossible for an outsider to discern if he or she has an overriding interest.

Prior to the adoption of the modern BDSG and GDPR, the Federal Constitutional Court (a specialized court in Germany focused on ensuring the German constitution is obeyed; as if the power of the Supreme Court to interpret the Constitution were its own court and limited just to the Constitution)[123] annulled the EU's Data Retention Directive for intruding into the German right of privacy and self-determination.[124] The Data Retention Directive simply required member states to retain telecommunications records for a minimum of six months, and a maximum of two years.[125] The German constitution, as many EU member state constitutions do, considers privacy to be a fundamental right of an individual, and fundamental rights are all protected with an express purpose of "prevent[ing] the holder of a fundamental right [from being] stripped of the inalienable core of her fundamental right."[126]

While the general consensus of German legal academia seems to be that what constitutes a breach of this fundamental right needs to be weighed in some sort

---

118. *Id.* § 26.

119. *Id.* § 26(1).

120. *Id.* § 26(2).

121. *Id.*

122. *See generally id.* § 35 (Sometimes also phrased as 'overriding legitimate interest,' for this note, the two are virtually interchangeable.)

123. *The Court's Duties*, BUNDESVERFASSUNGSGERICHT [Federal Constitutional Court], https://www.bundesverfassungsgericht.de/EN/Das-Gericht/Aufgaben/aufgaben_node.html [https://perma.cc/77F3-7BDH].

124. Buitelaar, *supra* note 67, at 174; Directive (EU) 2006/24, 2006 O.J. (L 105), 54-63.

125. Directive (EU) 2006/24, *supra* note 124, at 58.

126. Brkan, *supra* note 76, at 866.

of expectations, or proportionality tests, there is disagreement as to what those tests ought to be.[127] Until the EU court, the German court, or the German legislature solves these issues, there will continue to be ambiguity on how far the fundamental right of privacy extends and what that means for demonstrating an overriding interest, beyond interests otherwise proscribed (such as establishing a legal defense as described in the BDSG, Art. 24).[128]

Encapsulating the above: Germany implements all of the protections of the GDPR. Atop those protections, the BDSG grants permission to process data for other legitimate reasons than what the data was gathered for, considers the form and necessity of employment in determining whether or not an employee has validly consented to his or her data being processed, and provides a very narrow exception to the right of erasure for when the data is in a system that precludes efficient erasure, which, *de facto*, would also have to preclude its ability to be efficiently used in a Big Data engine. The BDSG further qualifies many of these rights, as well as many of the rights in the GDPR, having limitations or considerations due where either party has an overriding interest, but there is little guidance in primary or secondary sources as to what constitutes an overriding interest, creating a risk which cannot be adequately mitigated in its current state.

C. In Saudi Arabia

The Kingdom of Saudi Arabia closely resembles the United States in terms of its lack of general privacy protections, yet its legal framework is different enough to require more analysis than a simple statement that it is more like the United States than to the EU. Understanding what privacy means in Saudi Arabia is key to understanding how to apply Saudi labor laws and data protection regulations.

The Saudi legal system is a religious (Sharia) system, with the Qur'an and Sunna (the traditions) as its legal underpinnings.[129] However, because the Saudi legal system tends to only strictly apply Sharia where some portion of the Quran or Sunna sets specific rules, this leaves a great deal open to interpretation.[130]

---

127. *Compare* Brkan, *supra* note 76, at 883 (arguing that courts should determine the proportionality on a case-by-case basis, weighing rights to privacy and rights to data protection with how serious of an interference would occur) *with* Valentin Pfisterer, *The Right to Privacy—A Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy*, 20 GERMAN L. J. 722, 733 (2019) (arguing the court should set down expectations and rules for the various fundamental rights implicated in data privacy with an eye towards "certainty, reliability, and predictability . . and ultimately [to] strength the rule of law in Europe").

128. BUNDESDATENSCHUTZGESETZ (BDSG) [Federal Data Protection Act] § 24(1)2.

129. SAUDI BASIC LAW OF GOVERNMENT, No: A/90 § 1 (Mar. 1, 1992). All cites sources of law for Saudi Law in this Note are from the English versions of the respective laws. While only the Arabic versions of the law are authoritative text, the English versions approximate the law in a 'close enough' fashion to suffice for this Note's hypothetical.

130. *See* Ahmed A. Altawyan, *International Commercial Arbitration in Saudi Arabia*, *in* COUNCIL ON INTERNATIONAL LAW AND POLITICS 22-23 (1st ed. 2018) (citations omitted).

"[F]or historical reasons, the Kingdom is substantially influenced by the French legal system[,]" by way of the French influences on the modern legal system of Egypt.[131] Thus, if there is some divine law in the principles of Sharia, Saudi courts are supposed to adopt that rule; otherwise, the Saudi courts look to the laws passed by the Saudi legislature under the direct power of the King as Prime Minister of Saudi Arabia.[132] Therefore, any analysis of privacy in Saudi Arabia must begin with what Sharia says about privacy.

Several passages in the Quran speak obliquely to privacy through respect for personal autonomy, and by placing an injunction upon people from prying into other peoples' affairs.[133] From these principles, the Basic Law of Government expounds on privacy in Articles 37 and 40 by guaranteeing one's dwelling and the privacy of communications are inviolate, save where specifically sanctioned by law.[134] However, this basic law is designed to form the framework by which Saudi courts are to interpret the law (where Sharia is unclear or does not apply) and does not, itself, provide much clarity on what privacy of communications means.[135]

Turning to Saudi civil laws, there are two major legislative pieces of relevance for this Note: the Saudi Labour Law and the Credit Information Law.[136] Of these, the most obvious place to begin would be the Saudi Labour Law. Unfortunately, while the Labour Law thoroughly establishes when it applies to citizens only and when it applies to everyone, as well as how one cannot subcontract around the Saudi Labour Law, it does not provide any guidance on PII, how employers are to treat PII, or if the employee has any rights around his or her PII.[137]

The Credit Information Law is the only other source of privacy protections in the civil code of Saudi Arabia, and its application is narrowly confined to "companies, members, government and private entities maintaining credit information."[138] This law also only deals with credit information—*i.e.*,

---

131. *Id*.

132. *See generally id*. at Ch.1; No: A/90 § 48. Note, there are considerably more layers and depth to the Saudi legal system, but that is beyond the scope of this Note.

133. *Quran* 49:12 ("And do not spy or backbite each other."); *see* Vidushi Marda & Bhairav Acharya, *Identifying Aspects of Privacy in Islamic Law*, THE CTR. FOR INTERNET & SOC'Y (Dec. 14, 2014), https://cis-india.org/internet-governance/blog/identifying-aspects-of-privacy-in-islamic-law [https://perma.cc/A225-YJMH]. While Marda and Acharya are writing about Islamic law in India, with some references to Pakistan, their interpretation of certain passages of the Quran help provide context for non-Muslim readers on how to understand the basic right of privacy in the Quran.

134. No: A/90 §§ 37, 40.

135. No: A/90 Preamble.

136. *See generally* SAUDI LABOUR LAW, No: M/21 (Apr. 24, 2015); ANTI-CYBER CRIME LAW, No: M/17 (Mar. 26, 2007); CREDIT INFORMATION LAW, No: M/37 (July 8, 2008).

137. *See* No: M/21, §§ 5-7; *see generally id.*

138. No: M/37, § 3.

information solely about consumer credit, not other types of PII.[139] Thus, while this narrow set of information is protected within Saudi law, it only protects and gives rights to consumers, and only for purposes of commercial credit, not privacy protection, *per se*.[140]

Compounding the lack of protections within Saudi law, no general description of privacy data exists within Saudi law. Thus, what this Note considers PII may or may not be considered such in the Kingdom of Saudi Arabia.[141] It is simply unknown. However, many companies and government agencies within the Kingdom have privacy policies in place which look and are written similar to their U.S. or EU counterparts such that they are in every legal way modern, including their usage of the term personal information; however, in the absence of something codified, it is impossible to determine what authority these policies have.[142] Assuming that companies act in good faith, these self-offered guarantees are as good as any other modern company's.

Saudi Arabia's Communications and Information Technology Commission (CITC) recently passed a cloud computing[143] regulatory framework which entered into force on December 2, 2019.[144] This framework creates a series of sensitivity levels based on the type of data being stored, from non-sensitive data (level 1) to highly sensitive or secret government data (level 4).[145] PII data would likely fall into level 2 or 3, sensitive content not subject to sector-specific restrictions (level 2) or subject to regulation (level 3), depending on the risk involved with the type of PII.[146] This creates a split in that if the data is level 3, it cannot be transferred out of Saudi Arabia without express legal or regulatory permission, whereas level

---

139. *Id.* § 1.

140. *Id.* §§ 6, 9.

141. *See supra* Part I.

142. *Privacy Policy*, UNIFIED NAT'L PLATFORM GOV.SA; https://www.my.gov.sa/wps/portal/snp/pages/privacyPolicy/ [https://perma.cc/LAY6-PY54].

143. *See* Nabeel Zanoon et al., *Cloud Computing and Big Data is there a Relation between the Two: A Study*, 12 INT'L J. APPLIED ENGINEERING RES. 6970, 6972-6974 (2017). Cloud computing is a distributed computer system which operates over a vast network, where one can pool resources with other people on the cloud, gain access to one's own data from anywhere, adjust computing resources on demand (known as 'elasticity') and, where agreed upon, share data. This sort of distributed, networked computing is one of the major drivers of big data's ability to consume data by sharing between clients within clouds, across clouds, and aggregate data in an ever-increasingly-complex and Artificial Intelligence driven environment.

144. *See generally Cloud Computing Regulatory Framework*, COMM. & INFO. TECH. COMM'N, https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/CCRF_En.pdf [https://perma.cc/X2P5-27CK] [hereinafter CCRF]; COMMUNICATIONS AND INFORMATION TECHNOLOGY COMMISSION, CLOUD COMPUTING REGULATORY FRAMEWORK, https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Pages/CCRF.aspx [https://perma.cc/QR9C-LSWJ]. Confusing, both the regulatory framework document and website share a name. Thus, when referring to the actual framework document, this note calls it the CCRF.

145. CCRF, *supra* note 144, at 5-6.

146. *Id*.

2 data can be exfiltrated without issue.[147]

The CCRF applies only to Cloud Service Providers, meaning, "any Person providing Cloud Service to the public" including if one is merely a provider, a broker for third parties, or an aggregator who integrates multiple different cloud options.[148] Furthermore, the CCRF only applies to services offered to customers with an address in Saudi Arabia.[149] One notable exception exists in that parts of the cloud located in Saudi Arabia—which could include devices gathering data, depending on the specific cloud's setup—are subject to reporting data breaches and the provisions on unlawful content (*e.g.*, copyright-infringing material).[150] Thus, a company providing a cloud service to itself and only itself would likely not be considered a Cloud Service Provider under this regulation.[151]

D. International Framework

In addition to the national laws involved in this Note's hypothetical, a savvy data rights enthusiast needs to recognize and apply several international legal concepts. Extraterritoriality of national laws is important to understand what is or is not a cognizable legal claim in a jurisdiction, and how enforcement takes shape. This subsection lays out the most relevant international agreements—be they treaties, resolutions, generally accepted guiding principles for international labor, and other economic development agreements.

However, before diving into international agreements, it is important to operate from a common understanding of the legal concept of extraterritoriality.[152] An extraterritorial claim is a jurisdictional claim where one state or power (a jurisdiction, to confuse the word further) seeks to exert authority over the actions of a person, place, or thing outside the territory of the claimant jurisdiction.[153] This concept is critical for this Note's hypothetical because "in the context of privacy laws, it is obvious that what interests U.S. businesses is not whether the exercise of jurisdiction as such is extraterritorial, but whether the

---

147. *Id.* at 7.

148. *Id.* at 2.

149. *Id.* at 4.

150. *Id*.

151. At the time of this note's writing, the Consultative Assembly of Saudi Arabia, also called the Shura Council, is reviewing, and has been for at least a year, "a new freedom of information and protection of private data law[.]" *Data Protection Laws of the World*, DLA PIPER (Jan. 25 2019), https://www.dlapiperdataprotection.com/?t=law&c=SA [https://perma.cc/5SAR-DVLM].) Unfortunately, details are not yet available on what shape this law may take. Future readers should bear this new law in mind as it may substantially alter parts of this Note's analysis.

152. *See infra* Part III.B.

153. *See* Dan Jerker B. Svantesson, *The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on U.S. Businesses*, 50 STAN. J. INT'L L. 53, 60-61 (2014) (Svantesson uses a definition of extraterritoriality which is focused on "whether the exercise of jurisdiction . . . has any extraterritorial effect or implications.").

exercise of jurisdiction has any extraterritorial effects or implications."[154]

When extraterritorial issues arise, private international law's rules of resolving conflicts become the rules of the road in an ideal world where all sides are seeking a peaceful resolution.[155] This Note assumes the Restatement rule applies; that is, a court decides the applicable law based on which jurisdiction has the most significant relationship to the issue, following its own local rules—unless otherwise demonstrated, this means a court will most likely assume the laws of its own country are superior.[156] One way to demonstrate that the sitting court's laws ought to acquiesce to another's is through these international agreements.

i. Treaties & United Nations Assembly Resolutions

While there are no general UN resolutions or treaties deal with international data privacy, the International Court of Justice (ICJ) presents one means by which a neutral arbiter could be called upon to solve a conflict of law.[157] Therefore, this subsection section lays out two potential neutral parties to arbitrate a conflict. As all three countries in question (the United States, Germany, and the Kingdom of Saudi Arabia) are part of the UN, they are also part of the ICJ and have agreed to work towards compliance with the decisions of the court.[158]

However, using the ICJ would require the backing of the States involved, as the Court's primary purpose is to resolve disputes between States, not between citizens of those States.[159] Thus, the matter of data privacy would need to escalate to a serious economic concern such as would draw the attention of the States and not just citizens or companies within the States. While the matter may reach that point someday, it is not there yet.

Assuming the case does reach the ICJ, however, the ICJ stipulates that it considers and applies the laws found in international conventions where rules are expressly given and shall also apply "international custom."[160] For something to be a customary international law means there is "a general and consistent practice of states" following the custom.[161] According to the Restatement's comments, following the custom includes not only public measures and statutes but actions "undertaken in cooperation with other states, for example in organizations such

---

154. *Id*.

155. *See* 16 AM. JUR. 2D *Conflict of Laws* § 2 (2019).

156. *See id.* § 3.

157. U.N. Charter art. 92.

158. *Id.* art. 93, ¶ 1; *id.* art. 94. Careful readers should note the use of the word "general" here means from the United Nations General Assembly (UNGA). There are specific UN recommendations, as is shown in the next subsection. *See infra* Part II.D.ii.

159. *See How the Court Works*, INT'L COURT OF JUST., https://www.icj-cij.org/en/how-the-court-works [https://perma.cc/2SM3-TWME].

160. Statute of the International Court of Justice, June 26, 1945, art. 38, 59 Stat.1031.

161. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 102 (AM. LAW INST. 1987), § 102(2).

as the [OECD]."[162] While the UN may not have a specific guidance or custom to help in this analysis of PII rights, understanding this principle of customary law is important for other agreements and doctrines laid out in the following subsections.[163]

Another source to look at for guidance on an emerging customary law surrounding privacy is the OECD's Privacy Framework, especially as the standards body in the United States, NIST, follows OECD's fair information practices.[164] This privacy framework pushes for individual rights to access data within a reasonable time, and at a reasonable fee (if any), as well as the ability to challenge incorrect data.[165]

The OECD pushes for openness and free flow of data across international borders where members have implemented the OECD guidelines or similar safeguards.[166] To facilitate cross-border capability, the OECD recommends a twin approach: national and international. On national, member nations ought to implement a holistic approach to privacy, from laws protecting individuals, to self-regulation support, to an ability for individuals to exercise their rights of privacy.[167] For international cooperation, the privacy framework gives only a broad aspiration of developing "international arrangements that promote interoperability among privacy frameworks[.]"[168]

A third possible route to neutral arbitration from a mutual treaty between the three countries is the World Trade Organization (WTO).[169] Unfortunately, the WTO was intended to handle trading in physical goods, and the abstract nature of the logical commodity that is PII may simply be too far afield for the General Agreement on Trade and Tariffs (GATT).[170] As the sale of PII is a service, the WTO's General Agreement on Trade in Services (GATS) becomes a possible vehicle for determining how different jurisdictions could resolve differences in the law.[171] Three things are important for this analysis then: (1) the specific-

---

162. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 102 (1987), Cmt. b.

163. *See infra* Parts II.D.ii; II.D.iii.

164. *See generally The OECD Privacy Framework*, ORG. FOR ECON. CO-OPERATION AND DEV. (2013), https://www.oecd.org/internet/ieconomy/oecd_privacy_framework.pdf [https://perma.cc/5ZMY-2672]; *see supra* Part II.A.i.

165. *The OECD Privacy Framework*, *supra* note 164, at 15.

166. *Id*. at 16.

167. *Id*. at 17.

168. *Id*. at 18.

169. *Members and Observers,* WORLD TRADE ORG., https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm [https://perma.cc/VQ3C-PAK5]. The United States and Germany have been a member of the WTO since 1995. Saudi Arabia joined in 2005.

170. Mira Burri, *The Governance of Data and Data Flows in Trade Agreements: The Pitfalls of Legal Adaptation*, 51 U.C. DAVIS L. REV. 65, 129 (2017).

171. Steven Melendez & Alex Pasternack, *Here Are The Data Brokers Quietly Buying and Selling Your Personal Information*, FASTCOMPANY (Mar. 2, 2019), https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information [https://perma.cc/3L82-2RVJ] (as an aside: West Publishing is among the data brokers listed as

commitment nature of the GATS; (2) whether this is the least burdensome way of regulating the service to ensure its quality; and (3) whether the regulation at issue in this Note's hypothetical is even within the scope of the GATS.

First, the GATS operates on specific commitments that members opt-into, meaning it is not a one-size-fits-all agreement like the GATT.[172] Second, the GATS seeks to limit domestic regulation of a service to the least burdensome method "necessary to ensure the quality of the service."[173] To answer the question of whether or not regulations like the GDPR are the least burdensome required to ensure the quality of the service, you first need to know what service is being offered. The service being regulated is the privacy data brokerage service but that regulation is the incidental, though natural and probable, consequence of regulating the processing of any person's PII more broadly.[174] If this regulation were to cease to exist, the service being offered would not decline, indeed, the data brokerage service may even improve![175] Thus, the GATS may end up being used as a tool to restrict the GDPR.

However, complicating whether or not the GATS is applicable in this situation is that this Note is dealing with an employee-employer relationship. The employer may not be a data broker, as such data collection may be merely incidental to the employer's actual offerings of goods or services. Reading the GATS as applying to this sort of a situation, without other facts demonstrating that a company is actually a commercial service offering being regulated by the GDPR (and not merely a company subject to the GDPR, a broader category), would expand the GATS to cover even the sale of commercial goods so long as the company maintains basic human resources records on its employees.

ii. The International Labor Organization

A specialized agency of the UN, the International Labor Organization (ILO)

---

tracking and selling your data, specifically to the U.S. Government). *See* General Agreement on Trade in Services, May 30, 1950, 64 U.N.T.S. 187, art. I. [hereinafter GATS].

172. Burri, *supra* note 170, at 82.

173. GATS art. VI.4. This paragraph focuses on ensuring any regulations adopted around qualifying requirements for licensing of services, or applying technical standards to a service, do not become a barrier to trade. The GDPR's data processer and data handler requirements are one such technical standard that would fall within the scope of this paragraph. *See* GDPR art. 28.

174. Regulation (EU) 2016/679, *supra* note 63, at 32.

175. *See generally* Eline Chivot & Daniel Castro, *What the Evidence Shows About the Impact of the GDPR After One Year*, CTR. FOR DATA INNOVATION (June 17, 2019), https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/ [https://perma.cc/5T68-XUTT]. The article highlights the various supposed negative impacts of the GDPR with regard to the services being offered, the costs to startups, and the stifling of innovation. These effects could be seen as evidence the regulation is overly burdensome. While this Note's author does not necessarily agree with those conclusions, an objective assessment requires mentioning the evidence as a potential tool in this debate between balancing employer interests and employee rights.

provides a detailed code of practice for protecting worker's PII.[176] This code of practice provides some of the strongest evidence for the protection of PII as a growing international customary right, and one that ambiguity should be resolved in favor of doing something rather than simply stating there is no right to data protection.[177] The ILO created the code in 1997, and its regulations are intended to cover both public and private sector data.[178] Unlike Conventions, the code is not binding because the ILO sought to maximize flexibility in the face of emerging technologies.[179] Nearly twenty-five years later, the code's provisions are still relevant.

The code provides broad guidelines around the collection, storage, use, and rights (both collectively and individually) surrounding PII.[180] Of particular interest to this Note
is what rights the code grants to workers: the right to be notified of data usage, to freely and without charge access their data, to correct erroneous data, to place statements on the data, and for employers to have the ability to protect the data from the employee in the event of a security investigation.[181] Conversely, the collective rights have more to do with representation in collective bargaining; therefore, they are not relevant to this note.[182]

Most of the individual rights are self-explanatory, but two bear special attention: the right to correct, and the right to place statements on one's own data.

On the right to correct, the code asserts that workers should have the ability to correct incomplete data, and, beyond that, employers should "inform all parties who have been
previously provided with the inaccurate or incomplete personal data of the corrections made, unless the worker agrees that this is not necessary."[183] This places a burden upon the employer heretofore not seen in other privacy regulations this Note has examined.

As for placing statements on one's own PII, the code gives employees the right to place statements on records with which the employee disagrees on the accuracy thereof and the employer refuses to correct the record.[184] In a world of automated processing, where data is merely numbers on a spreadsheet or in a database, this may not be feasible. It may also be superfluous even where it is feasible, as even if an employer transfers the data to a third party, an automated process may lack the ability to acknowledge such extraneous data even exists.

---

176. *See generally Protection of Workers' Personal Data*, INT'L LABOR ORG. (1997), https://www.ilo.org/safework/info/standards-and-instruments/codes/WCMS_107797/lang--en/index.htm [https://perma.cc/SWG6-5RZX].

177. *See supra* Part II.D.i.

178. *Protection of Workers' Personal Data*, *supra* note 176, at 1.

179. *See id*. at 9.

180. *Id*. at 2.

181. *Id*. at 6-7.

182. *Id*. at 7.

183. *Id*.

184. *Id*.

Lastly, the ILO's code expresses a desire for redress.[185] That is, the ILO believes it to be critical that workers have some ability to have their complaints heard and responded to, in a manner that is "accessible to workers and simple to use."[186] This is intended not just to be an internal redressability, but some means by which employees can question and test the employer's compliance with the code itself.[187] In a common law system that has recognized a right to privacy, this could be interpreted as a customary rule intended to provide access to the courts when no other redress exists.

iii. U.S. State Department's Other International Agreements

This last subsection is a catch-all to survey other United States international agreements that will factor into the analysis, starting with the U.S.-EU Data Privacy agreement, then covering the Trade Investment Frameworks between the United States and Saudi Arabia. Because of the value of services to the U.S. economy for years and the criticality of data flow to performing those services, the United States has had a transborder data agreement known as the Privacy Shield Framework in place since 2016.[188] The Privacy Shield is an optional set of principles that private organizations may opt into, designed to facilitate both the ease of data transference between jurisdictions and protect the rights of persons covered by the GDPR.[189]

By an organization join the Privacy Shield, they are agreeing to give individuals choice, access to their data, a promise to maintain accountability for third party transfers, to limit the purposes for which gathered data can be used, and to provide a specified recourse for individuals seeking to enforce their rights.[190] Under the Privacy Shield , individual choice means that organizations must provide a means by which individuals can opt out of their information being shared with third parties or if the data may be used for purposes materially different than its intended purpose.[191] One exception exists in 'sensitive' information—*e.g.*, medical data, sex life—where an individual must explicitly opt-in.[192]

Access to one's own data under the Privacy Shield means that organizations must provide an individual access to his or her own data, unless "the burden or expense of providing access would be disproportionate to the risks to the

185. *Id*.

186. *Id*.

187. *See id*. at 24.

188. CRS R44257, *supra* note 29, at 4; Int'l Trade Admin., *Overview*, PRIV'Y SHIELD, https://www.privacyshield.gov/Program-Overview [https://perma.cc/SYP2-L6SK].

189. DEP'T OF COMM., EU-U.S. PRIVACY SHIELD FRAMEWORK PRINCIPLES 1 (2016) [hereinafter PRIVACY SHIELD].

190. *Id.* at 5-8.

191. *Id.* at 5.

192. *Id*.

individual's privacy . . . or where the rights [of another] would be violated."[193] What constitutes disproportionate burden or expense is a judgment call, but the Privacy Shield provides some guidance with examples such as grant or denial of insurance, a mortgage, or job based on the data would mean that the organization needs to disclose "even if it is relatively difficult or expensive to provide" the data.[194] Of special importance to this Note, the Privacy Shield exempts human resources data based on data that is anonymized.[195] Lastly, organizations can charge a fee for this right of access, so long as the fee is not excessive, and with the understanding that once an individual offers to pay the fee, cost ceases to be a legitimate reason to deny that individual's request.[196]

Finally, the Privacy Shield mandates that covered organizations must have mechanisms for individuals seeking recourse for non-compliance, and these mechanisms must be independent of the organization, contain organizational follow-up procedures to implement non-compliance remedies, and sanctions rigorous enough to ensure compliance by organizations.[197] Exactly what sorts of sanctions and procedures are sufficient is undefined. However, the Privacy Shield does stipulate that organizations must submit to binding arbitration should an individual invoke that right.[198] The entirety of Annex I sets forth the arbitration model to be followed and stipulates that the arbitration consists of "non-monetary equitable relief (such as access, correction, deletion, or return of the individual's data in question)" but explicitly cannot award "damages, costs, fees [including attorney's fees], or other remedies."[199]

In addition to agreements between the U.S. and the EU, the United States has two Trade and Investment Framework Agreements (TIFAs) relevant to this Note: one between the Arab States of the Gulf Coast (of which Saudi Arabia is a member), and an older one with Saudi Arabia directly.[200] The TIFAs are substantively similar and serve to reinforce the desires of both countries to

---

193. *Id.* at 7.

194. *Id.* at 17.

195. *Id.* at 20.

196. *Id.* at 19.

197. *Id.* at 8.

198. *Id.*

199. *Id.* at 33.

200. Framework Agreement for Trade, Economic, Investment and Technical Cooperation Between the Cooperation Council for the Arab States of the Gulf and the Government of the United States of America, GCC-US 1, Sept. 25, 2012, https://ustr.gov/sites/default/files/uploads/agreements/Trade%20Investment/US-GCC%20TIFA%20Final%20Text%20--%20English%209-25-12.pdf [https://perma.cc/7W5Q-MWFE] [hereinafter TIFA GCC-US]; *see generally* Agreement Between the Government of the United States of America and the Government of the Kingdom of Saudi Arabia Concerning the Development of Trade and Investment Relations, Saudi-US, July 31, 2003, https://ustr.gov/sites/default/files/uploads/agreements/tifa/asset_upload_file304_7740.pdf [https://perma.cc/DWM7-65EV] [hereinafter TIFA Saudi-US].

While the TIFA GCC-US is newer than the TIFA Saudi-US, nothing within the newer TIFA removes abrogates the older. Thus, both are listed here for completeness.

eliminate trade barriers around the sale of goods and services, as well as investments between the two countries.[201] While there is no mention, in either TIFA, of personal data or interstate data transfer at all, the dedication to eliminate trade barriers could be used as a push for a least-common denominator on enforcing privacy rights between the two nations, as any restriction to data services would be a non-tariff barrier to trade.[202]

III. CONFLICTING AND COMPLEMENTARY RIGHTS

The previous section laid out relevant law in the three nations under examination—the United States, the European Union, and the Kingdom of Saudi Arabia—as well as the relevant international frameworks for consideration. This section now turns to examine what that law means in the hypothetical set forth Part I. This analysis is done from three perspectives: what happens when the employee, Edrichtet, attempts to enforce his rights in the United States, what happens in the European Union, and what happens in the Kingdom of Saudi Arabia.

By examining how the law applies in each of these nations, with one German national being the focal point, it becomes immediately apparent how nebulous this area of the law is. There is no certainty of outcome, or even predictability of outcome, for either the company or the employee.

Our hypothetical company, Fict-Data, is owned and operated in the United States. Its principal place of business and headquarters is in Indiana. The employee, Edrichtet, is a German citizen who works for Fict-Data. Fict-Data gathered the PII that is at issue while Edrichtet was in Saudi Arabia on business for Fict-Data. It is now post-employment for Edrichtet, and he no longer wishes Fict-Data to retain or use his data. Fict-Data has, without malice, not answered Edrichtet's requests. So now what can he do?

A. Enforcement in the United States

Edrichtet is likely to meet with an inability to control his data by seeking redress in a U.S. court, and any hope he has will be highly situational because of the applicable domestic and international law. Because Fict-Data is located in the United States, Edrichtet may first seek to exert control over his data within the United States. Yet, his ability to do this will be driven almost entirely by Fict-Data's specific industry, as Edrichtet has no general federal protection for his

---

201. TIFA GCC-US, *supra* note 200, at 2-3; TIFA Saudi-US, *supra* note 200, at 2.

202. *Cf.* TIFA GCC-US, *supra* note 200, at 2 (article three's provisions to "promote an open and predictable environment for international trade and investment" could be interpreted as a tacit push to ignore proposed privacy regulations until their impacts can be ascertained); TIFA Saudi-US, *supra* note 200, at 3 (article four states an intent to develop bilateral trade and provide "for a steady increase in the exchange of products and services[,]" as well as promote "an attractive investment climate" between the United States and Saudi Arabia. Similar to the GCC-US, a push for deregulation in this area until the impact can be ascertained in other jurisdictions would meet this desire).

PII.[203]

To see where Edrichtet would be able to succeed in some form of action against a U.S. company requires adding and twisting facts around. For example, if Edrichtet shows that Fict-Data breached its own corporate-made data privacy policy, then he may have recourse within the courts through the Federal Trade Commission (FTC).[204] This seems unlikely given that the FTC has larger things to pursue and limited resources with which to do it.

Another route that may exist depends on whether or not Fict-Data is a contractor or subcontractor with the Federal Government.[205] Assuming Fict-Data is a contractor or subcontractor, it is likely that at least one of its contracts requires compliance with NIST 800-122's provisions for PII protection and for employees to challenge data collected, followed by erasure, rectification, or amendment.[206] However, even should Edrichtet win, it is unlikely he can have the data erased because Fict-Data would most certainly claim, and rightly so, that the data was gathered for a legitimate purpose. The rule is that as long as Fict-Data is protecting the PII, Edrichtet is unable to seek erasure or limitation on the company's use of it. Further complicating this, if Edrichtet was not working as a contractor or subcontractor to the Federal Government, but, instead, on another project for Fict-Data, it is possible Fict-Data would not even need to comply with the NIST guidelines, depending on the contract.

Most likely, the court would throw the case out at the pleadings in a motion for failure to state a claim upon which relief can be granted.[207] This is because the NIST guidelines do not have specific provisions granting a right of action. Thus, unless Edrichtet can somehow show a breach of Fict-Data's privacy policy or that their retaining his data would somehow constitute a breach of a contract or sub-contract, there is no right of action.

Should a court find that Fict-Data was supposed to be following the NIST 800-122 provisions, the court could say that retention of the data is no longer necessary, unless Fict-Data can anonymize the data, rendering it no longer PII by removing any identifying elements.[208] Still, should one think that Edrichtet has won the moment the court orders the anonymization of the data? Recent studies continue to demonstrate that with multiple sets of independent data, it is remarkably easy to re-identify someone.[209] Anonymization may no longer be

---

203. *See supra* Part II.A.i.

204. Rustad & Koenig, *supra* note 30, at n.312 (2019).

205. This Note is excluding the possibility that Fict-Data is running a System of Record (49 CFR 10.5.) with the assumption that Fict-Data's systems are all contractor-owned, contractor-operated systems and are not gathering data on behalf of a U.S. Government agency. While this may be an interesting conjecture, it requires another level of analysis that is beyond this Note's scope.

206. NIST 800-122, *supra* note 18, at 2-1.

207. FED. R. CIV. P. 12(b)(6).

208. NIST 800-122, *supra* note 18, at 4-4 through 4-6. Companies often have a use for anonymized data that still simulated some measure of realistic-seeming PII for statistical analysis.

209. *See generally* Dániel Kondor et al., *Towards Matching User Mobility Traces in Large-*

practically possible, but every company would claim it has anonymized one's data and be technically correct. In addition to ordering the data anonymized or removed, the court could find the contractor has materially breached its contract and allow the government contracting officer to terminate the contract.[210]

All other Federal rights of action that lead to Edrichtet winning are based on some form of a discrimination claim.[211] It is ironic that it is not a privacy claim which wins the day, but a discrimination claim. An equitable relief may be to grant deletion of Edrichtet's data, but there is no precedent to stand on for such a decision—which is not to say the court would not, merely that it would be a new relief.

Indiana law, containing no other truly relevant privacy provisions, does not substantively alter this analysis if Edrichtet were to sue in state court. If Fict-Data is a state contractor, then a similar analysis as the Federal Government analysis in the preceding three paragraphs applies.

While under domestic law, Edrichtet likely loses with a few chances for success based on very fact-sensitive setups, international law applied in the United States, provides a different story. Here, Edrichtet's strongest chance for some form of redressability is based on the EU-U.S. Privacy Shield.[212] He could also attempt to make an emerging customary law claim; but as courts are reluctant to expand local privacy laws sans a statutory relief, it seems unlikely courts would apply a customary law as yet unacknowledged.[213] Because this is unlikely to be a winning argument, it merits no further analysis beyond "Fict-Data wins," for now.

Assuming that Fict-Data is a member of the Privacy Shield, Edrichtet could seek redress under the rules set forth in forth in the Privacy Shield's Annex 1.[214] This would mean submitting to arbitration unless there is an option available within Fict-Data to handle this internally.[215] However, if Edrichtet is unhappy with the result of such arbitration, the Privacy Shield then also allows him to return to the FTC and seek action from that regulatory body, which has

---

Scale Datasets, arXiv:1709.05772[cs.SI], CORNELL UNIV. (Aug. 13, 2018), https://arxiv.org/pdf/1709.05772v4.pdf [https://perma.cc/Q76T-V2LH]. This Cornell University-published paper, authored by computer scientists, is a conclusive demonstration and thorough proof (in the mathematical and engineering sense of the word) of how pattern matching can be done on large sets of data to successfully render anonymized data personally identifiable again. The larger the data set, the closer the probability of match is to 100 percent. Section 5.2 walks the reader through the pattern matching probabilities using previously anonymized data and traffic patterns. Within one week, as data density increased, researchers could match the anonymized data to the correct persons 95.6 percent of the time.

210. 48 C.F.R. § 49. In the case of a sub-contractor, subcontractor, the contracting officer would instead issue a termination order contingent on the sub-contractor's removal.

211. *See supra* Part II.A.i.

212. *See supra* Part II.D.iii.

213. *See supra* Part II.D and II.D.ii; *see* Rustad & Koenig, *supra* note 30, at 385.

214. *See supra* Part II.D.iii.

215. PRIVACY SHIELD, *supra* note 189, at 24-25.

committed to reviewing cases like this on an expedited basis.[216] However, under the Privacy Shield, the analysis of the FTC's likely actions changes significantly. Now, the FTC would look to whether or not Fict-Data is complying with the Privacy Shield's Principles, especially on the application of the Choice principles where "employers should make reasonable efforts to accommodate employee privacy preferences."[217] At most, this would mean anonymizing the data, not outright deletion.[218] Thus, should Edrichtet seek enforcement within the United States, he is unlikely to receive satisfaction without some other legal principle or wrong-doing on Fict-Data's part. While this provides some surety of liability to Fict-Data, it is entirely based on Fict-Data (1) acting in good faith or ignorance, and (2) following the provisions of its own privacy policies. This creates a perverse incentive to not have a strong privacy policy for your employees.

While this result would seem favorable, for a company, from a risk management perspective based solely on reducing corporate liability, it is not the end of the story.

B. Enforcement in Germany

The long-arm of the GDPR introduces a regulatory hiccup and unknown level of risk for Fict-Data's ability to continue to employ EU citizens. As a German citizen and a citizen of the European Union, Edrichtet could attempt to gain satisfaction through action in the CJEU or Germans courts. Here, Edrichtet's chances for victory are much higher than in the United States, but his victory could range from substantial fines to Fict-Data down to a mere pyrrhic victory of forbidding the data to appear on an EU server.[219]

Only part of Fict-Data's activities would fall under the GDPR, which complicates Edrichtet's attempt to have the data erased. Any of the data Fict-Data collected on Edrichtet while he is within the EU fits within Article 3, but much of the PII that Fict-Data holds on Edrichtet was collected in Saudi Arabia.[220] That data which is from Saudi Arabia is not within the scope of the GDPR unless Fict-Data is maintaining some of that data on servers within the EU.[221]

The PII Fict-Data maintains under the jurisdiction of the EU would likely be subject to erasure—unless Fict-Data shows some form of legitimate scientific or

---

216. *Id.* at 25-26.

217. *Id.* at 20.

218. *See id*. (the remedies listed in example focus on anonymization and lack any reference to deletion or removal).

219. *See supra* Part II.B.i; Regulation (EU) 2016/679, *supra* note 63, at 83 (ignoring the data subject's rights can result in a fine "up to 4% of the total worldwide annual turnover of the preceding financial year," per Article 83(5)(d)).

220. Regulation (EU) 2016/679, *supra* note 63, at 32-33.

221. Depending on how Fict-Data has configured its data storage and any potential cloud computing solutions, it is possible this could be the case without Fict-Data knowing, but the facts in the hypothetical state the data is in the United States. *Id.*

historical research purpose—or Fict-Data can render the data anonymous.[222] Anonymization alone, however, may become insufficient if the CJEU's trend of treating metadata as data is logically extended—as computer systems become able to reconstruct and re-identify people from anonymized data, the ability to anonymize may become moot in practice.[223] Given the limited scope of the data under the EU's jurisdiction, this order of erasure or anonymization may end up being a pyrrhic victory for Edrichtet. However, recall that Fict-Data also did not answer Edrichtet in a timely manner. Because of this, the CJEU could issue a fine for noncompliance.[224]

Should the CJEU render a judgment against Fict-Data, Edrichtet will then have to file in an Indiana court (or Indiana federal court) for enforcement of the judgment. In either case, Indiana state law would control.[225] Enforcement would be effectuated through a process known as domestication, which the State of Indiana does following the Uniform Enforcement of Foreign Judgments Act or through the common law process of comity.[226] Here, again, Edrichtet runs into an issue depending on what type of judgment he is seeking to have enforced. As long as Edrichtet's claim is recognized as a property interest under 28 U.S.C. section 1963, he can likely have the judgment enforced in Indiana.[227] Unfortunately, the issue of one's PII in the context of the GDPR has not come up yet in any U.S. court.

Any fine the CJEU issues for non-compliance, on the other hand, cannot be recognized under the Uniform Enforcement of Foreign Judgments Act, only through comity.[228] Once it is a matter of comity a court is still unlikely to enforce such a judgment as "[t]he Courts of no country execute the penal laws of another" except as a matter of treaty is a firmly established legal principle.[229] Indeed, the CJEU seems to implicitly recognize this limitation in *Google LLC v. Commission nationale de l'informatique et des libertés Commission Nationale de l'Informatique et des Libertes (CNIL)* where the court effectively limited the right to be forgotten to EU websites and appearing in EU data searches.[230] Realistically, unless Fict-Data has assets that could be seized in the EU, there is no real penalty

---

222. *See supra* Part II.B.i, n.89; Regulation (EU) 2016/679, *supra* note 63, at 5.

223. *See supra* Part III.A, n.218; *cf.* Brkan, *supra* note 76, at 873 (if the reasoning that metadata can reveal information about an individual is sufficient to class it as data, then it surely follows that anonymized data which can be coupled with other data sets to determine with high accuracy who the anonymous data belongs to is no longer truly anonymous).

224. Regulation (EU) 2016/679, *supra* note 63, at 83.

225. *See generally* Erie R. Co. v. Tompkins, 304 U.S. 64 (1938).

226. IND. CODE §§ 34-54-11-1 to 34-54-11-7; *see* Brightpoint, Inc. v. Pedersen, 930 N.E.2d 34, 39 (Ind. App. 2010) ("Under principles of comity, Indiana courts may respect final decisions of sister courts as well as proceedings pending in those courts.").

227. IND. CODE § 34-54-11-1; 28 U.S.C. § 1963.

228. *See* Ronald Brand, *Recognition and Enforcement of Foreign Judgments*, FED. JUD. CTR. INT'L LITIG. GUIDE 12 (2012).

229. The Antelope, 23 U.S. 66 (1825).

230. *See* Case C-507/17, Google, LLC v. CNIL, 2019 INFOCURIA, ¶ 60 (Sept. 24, 2019).

the CJEU can enforce here save impairing Fict-Data's ability to do business in the EU.[231] Lastly, as a practical matter, any court which enforced a foreign court's four percent of revenue penalty on one of its own corporations would likely face swift and severe rebuke from the other branches of government as a matter of common sense.

Thus, though Edrichtet may win under the GDPR, his victory is likely to be meaningless and unenforceable in any real way. The German BDSG is substantively similar to the GDPR, including its territorial limitations on enforcement over data gathered.[232] The legal analysis of the BDSG thus ends the same way: Edrichtet is likely to achieve a limited victory which may end up being meaningless. However, recourse through the GDPR or BDSG may not be Edrichtet's only option.

In addition to the GDPR and BDSG, Edrichtet may seek enforcement under the Privacy Shield, much the same as he would in the United States.[233] Once covered by the Privacy Shield, Edrichtet could bring the matter to arbitration and the issue resembles enforcement in the United States under the Privacy Shield due to the dispute resolution mechanics working exactly the same—Fict-Data remains a U.S. company, so the analysis remains the same.[234] It is also worth noting that any foreign enforcement issues vanish under the Privacy Shield due to the mandatory arbitration clause which Fict-Data would have agreed to in order to participate.[235] However, no monetary damages may be awarded under this arbitration, so the penalties in the GDPR remain unenforceable.[236]

Should the Privacy Shield end up being largely an empty enforcement mechanism in situations of employer-employee relationships, then the Privacy Shield runs a very real possibility of being invalidated by the CJEU, similar to the

---

231. Depending on Fict-Data's size and amount of business in the EU, this may not be a problem as it is entirely possible they merely needed Edrichtet as a subject matter expert and could turn to non-EU based assets to do the same work.

This is not to say that the GDPR's protections are without worth, or even that they are not strong protections, just that they are very fact-sensitive protections. A company that derives a substantial portion of its income from the EU would certainly have much to lose for not complying with the CJEU's order and could face loss of assets in the EU to handle any fines. There is still considerable risk to defying the CJEU, depending on how much business Fict-Data does with the EU, either directly or through contracting efforts for another entity like the Department of Defense where things like the NATO Status of Forces Agreements, beyond the scope of this Note, may cause further risk to Fict-Data. A careful analysis of a company's business model, contracts, and deeper legal ramifications would need to be done as part of any comprehensive risk analysis for complying with the GDPR.

232. BUNDESDATENSCHUTZGESETZ (BDSG) [Federal Data Protection Act] § 1(4)3.

233. *See supra* Part III.A.

234. *Id*.

235. 9 U.S.C. § 201 (the convention mentioned in this statute can, for this Note's purposes, be summed up as requiring compliance with foreign arbitration).

236. PRIVACY SHIELD, *supra* note 189, at 33.

Privacy Shield's predecessor, the EU-U.S. Safe Harbor agreement.[237] When it overturned the old Safe Harbor agreement, "the CJEU highlighted the absence of 'administrative or judicial means of redress' for EU data subjects."[238] Already, "the European Parliament passed a non-binding resolution to suspend the EU-U.S. Privacy Shield[,]" because of issues similar to those of this Note's hypothetical.[239]

Invalidation of the Privacy Shield may cause Fict-Data, or other companies offering services in the human resources or statistical-analysis-over-employees markets, to call for a trigger of the GATS.[240] The Privacy Shield is intended to comply with much of the intent behind the GDPR while providing service providers the ability to transfer data back and forth across the Atlantic.[241] Thus, Fict-Data may argue to the U.S. Trade Representative (who, in turn, would argue it to the GATS Dispute Settlement Body) that the failure of the EU to recognize these provisions as sufficient would constitute a barrier to trade.[242] The EU would likely respond by claiming a general exception to maintain the fundamental liberty interest of its citizens.[243]

Who would prevail in this GATS-complaint is beyond the scope of this note, as it has more to do with trade law than with privacy law. However, Fict-Data's complaint would open up serious risk for any EU companies selling services into the United States because even a temporary order from the Dispute Settlement Body allowing for a suspension of trade concessions could result in a considerable financial impact for the EU's services industries.[244] However, as

---

237. *See* CRS R44257, *supra* note 29, at 5-7 (explaining what the Safe Harbor agreement was and how the CJEU found the Safe Harbor provisions insufficiently protected EU citizens' rights); *but see FTC Announces Settlements with Four Companies Related to Allegations they Deceived Consumers Over Participation in the EU-US Privacy Shield*, FED. TRADE COMM'N (Dec. 3, 2019), https://www.ftc.gov/news-events/press-releases/2019/12/ftc-announces-settlements-four-companies-related-allegations-they [https://perma.cc/2TAE-BDHT] (the FTC claims "21 enforcement actions related to the EU-US Privacy Shield framework[.]"). This includes at least one judgment requiring deletion of data acquired while misrepresenting adherence to the Privacy Shield. None of these actions have been in the context of an employer-employee relationship, however, meaning those provisions of the framework are, as of yet, untested.

238. Emily Linn, Note, *A Look into the Data Privacy Crystal Ball: A Survey of Possible Outcomes for the EU-US Privacy Shield Agreement*, 50 VAND. J. TRANSNAT'L L. 1311, 1326 (2017) (citations omitted).

239. *See* Rustad & Koenig, *supra* note 30, at 453.

240. *See supra* Part II.D.i.

241. *See* Linn, *supra* note 238, at 1331 (the listed improvements made in the Privacy Shield demonstrate this intent to comply).

242. *See id.*; *see* GATS art. VI.4 (Fict-Data would assert this technical regulation of their service is a barrier to trade).

243. GATS art. XIV.

244. GATS art. XXIII.2; *Cf.* EUROPEAN UNION, OFF. U.S. TRADE REP., https://ustr.gov/countries-regions/europe-middle-east/europe/european-union [https://perma.cc/XF7Y-6Z6Z] (stating services imported to the United States from the EU was $196 billion in 2018; any suspension

noted in the previous section, Fict-Data's collection of the employee data may be too incidental for them to be considered a data broker offering a service the GDPR is regulating.[245]

In summation: the avenues seeking enforcement from the EU result in an increasingly complex regulatory framework that may end up either serving as an overly burdensome barrier to trade or an ineffectual protection for employees. The risk to companies is considerable, and the protections afforded to individuals are uncertain at best.

C. Enforcement in Saudi Arabia

Since Fict-Data gathered much of its PII on Edrichtet in Saudi Arabia—a key reason why many protections of the GDPR may not apply—Edrichtet may try to seek satisfaction in the Kingdom.[246] Unfortunately, Saudi law's general lack of acknowledgment of PII means that Edrichtet is extremely unlikely to find any kind of satisfaction within the Kingdom; however, there are a few complicating wrinkles worth examining.[247]

First, because there is no specific data protection law, courts in Saudi Arabia will revert to asking, what does Sharia suggest should happen?[248] As Sharia "developed to maintain the five necessities, namely: religion, life, family, money, and mind[,]" Saudi courts would turn to legal precepts within the Sunnah to tease out a workable rule for protecting from harm caused to one's person or property through PII misuse.[249] Edrichtet would likely not have any chance of enforcing the deletion of his data, but would be able to be compensated for damages suffered "as a result of the disclosure of his personal information by another party."[250] This sort of equitable compensation could be enforced in Indiana but has the disadvantage of Edrichtet needing to suffer harm first.[251]

Second, the Saudi CCRF causes a problem for Fict-Data if Fict-Data were also offering cloud computing services to any legal person having an address in Saudi Arabia.[252] If Fict-Data were doing this, then the sensitivity level of Fict-Data's PII immediately matters.[253] Since we have no reason to believe Fict-Data is tracking "Customer Content from private sector-regulated industries" for which

---

of concessions allowing even a 5 percent increased tariff to offset the GDPR would result in an almost $10 billion charge to EU companies in total).

245. *See supra* Part II.D.i.

246. *See supra* Part III.B (stating the GDPR has no hold over the data gathered in Saudi Arabia by an American company not storing any data in the EU).

247. *See supra* Part III.C.

248. Altawyan, *supra* note 130, at 8.

249. *See id*. at 8-9.

250. Suhaib Hammad, *Doing Business in Saudi Arabia: Overview*, THOMSON REUTERS PRAC. L. (Jan. 1, 2019).

251. IND. CODE § 34-54-11-1 *et seq*.

252. *See* CCRF, *supra* note 144, at 2.

253. *Id.* at 5.

a specific law or regulatory body has created rules, there is no issue with the PII gathered on Edrichtet.[254] However, this could change once the Shura Council finalizes its new protection of private data law.[255]

If the draft Saudi data protection law resembles the GDPR, it is probable the CCRF would end up considering Fict-Data's gathered PII as level 3. This would make it illegal to exfiltrate the data gathered on Edrichtet while he was in the country and provide Edrichtet a legal claim against Fict-Data. Assuming a data protection law similar to the GDPR, Fict-Data could be on the hook for a hefty fine.[256] If Fict-Data does either regular or sufficient business in Saudi Arabia to make such a fine something the company would be concerned with, then, unlike the EU, Fict-Data would need to pay much more attention to the law, rather than simply washing their hands of one market and counting on it being unenforceable in the United States.[257]

Fict-Data could push back on any potential regulation the Shura recommends and the king signs by seeking assistance from the U.S. Trade Representative through the Trade Investment Framework Agreements (TIFAs).[258] Unlike the GATS, however, and the analysis of its potential impact on U.S.-EU relations around this matter, the two TIFAs do not contain any dispute resolution language. Instead, they rely on a Joint Committee to handle such disputes.[259] Any subsequent resolution is not a matter of law but international diplomacy.

IV. RECOMMENDATIONS

In the previous three Parts, this Note examined the current issues around privacy data and employee rights, the current state of the law in three vastly different legal systems, and the outcomes of what happens when an employee attempts to enforce privacy rights in all three of those systems. These hypothetical outcomes demonstrate two things: (1) the disparate systems of privacy regulations make it incredibly difficult for average employees to seek some form of privacy; and (2) employers are opening themselves to a vast world of regulations and risks against which they have little way of mitigating the damage other than to sheer off whole markets. This is not beneficial to either party. One cannot get satisfaction, and the other finds unexpected barriers to international commerce.

Unfortunately, employee privacy and employer ease of commerce can often find themselves at cross purposes. Reasonable individuals and corporations will

---

254. *Id*.

255. *Data Protection Laws of the World, supra* note 151.

256. Regulation (EU) 2016/679, *supra* note 63, at 83 (ignoring the data subject's rights can result in a fine "up to 4% of the total worldwide annual turnover of the preceding financial year," per Article 83(5)(d)).

257. *See supra* Part III.B (paragraph discussing the refusal to enforce another country's penal laws).

258. *See supra* Part II.D.iii.

259. *See supra* Part II.D.i; *see supra* Part III.B (the paragraphs about GATS enforcement); TIFA Saudi-US, *supra* note 200, art. 6.

thus have to make concessions to each other to build a win-win environment where both individual privacy is protected and employers stand to reduce their risk. Weighing too far for the employee will disincentivize hiring.[260] Weighing too far for the company will result in political backlash and has had historically unpleasant results.[261]

This section is split into two subsections: subsection (a) is focused on recommendations for protecting individual privacy and subsection (b) is focused on easing international commerce. Both are needed to ensure a continuing thriving international workforce that provides increasing value to the global economy, it does not make sense to simply talk of improved privacy standards without considering their costs.

A. Considerations in Furtherance of Individual Privacy

Companies gather too much data without their employees knowing, commercialize too much data without the employees knowing, and profit from their employees' data in ways the employees do not currently understand.[262] Rather than fight this commercialization on grounds like human dignity, one could help create a level playing field between employer and employee through profit sharing. As the law attempts to catch up with new technology, it is clear that companies are able to sell employee data without their knowledge or informed consent, and those employers have a growing financial incentive to do so. Mandatory transparent (meaning employees can see who employers are selling their data to) profit sharing, where employers are benefitting from their employees' personal data, would both disincentivize more questionable sales of employee data and give employees a better understanding of how their property interest in their own PII is being used. With that knowledge, employees would have an interest in making sure the company maximizes how employee data is utilized in a win-win.

In the United States, such a profit-sharing model is something that may be best tried at state levels, where the exact formulas can be tinkered with and governments are better able to react to their constituents, before implementing

---

260. *See supra* Part III.B (where the Note discusses the perverse incentive to simply never hire an EU citizen in order to avoid risk).

261. *See* Buitelaar, *supra* note 67, at 175 (section B gives a history on the EU's old Data Protection Directive, the predecessor to the GDPR, which includes how large record systems were used to facilitate genocide. While one would hope this is a few steps more extreme than what corporations are capable of today, the simple fact is it did happen in history and thus cannot be simply brushed away as comically over-the-top).

262. *See* Anne de Singh, *Some Reflections on Dignity as an Alternative Concept in Data Protection Regulation*, 19 GERMAN L. J. 1269, 1270-71 (2018). While Professor Singh is talking in a more general sense than employer-employee relationships for the value of PII, there is no reason not to extend her arguments to employment. Indeed, if one considers industries where the employee is also a consumer, such as Facebook, there is no extension: the argument is already there.

any federal rules. Attempting to have the federal government handle this one comprehensive piece of legislation would raise federalism and preemption issues.

For this kind of profit-sharing to work, companies must turn over greater control of employee data, who it is being sold to, and how it is being used by creating a transparent and profit-driven model.[263] This move to a more give-and-take model increase employee trust in what sort of data is being tracked, and even allows them to engage in self-improvement.[264]

Other scholars have recommended the United States adopt more EU-like rules through such things as a hypothetical Employee Privacy Protection Act (EPPA).[265] This act would "limit workplace surveillance to its appropriate context . . . [and] prohibit surveillance outside the workplace[,]" and could not be contracted around.[266] While this would not grant an employee the ability to see data, delete data, or other such protections that exist in the GDPR, it would, presumably, allow employees some private right of action to bring suit against an employer misusing their data—a right employees do not currently have except in cases of discrimination.[267] The goal for advocates of this approach is to help establish a more stable balance of power between the employer and employee.[268]

A third recommendation, based on the EU enforcement analysis in prior sections, is for countries to either shift from statutory penalties to statutory damages or to include statutory damages in addition to fines.[269] This would allow people an easier time enforcing their judgments in the United States and in some civil countries as it would shift the fines into accruing to an individual, and thus enforceable.[270] In considering the amount or mix of statutory damages versus fines though, countries should be cautious not to create an overly generous windfall. Doing so would create a perverse incentive to go out and find someone to sue. No one wants to see Privacy Trolling.[271]

In the United States, any legislation intended to provide a private right of action for individuals will have to be either state laws or carefully crafted to avoid

---

263. Ellyn Shook et al., *How Companies Can Use Employee Data Responsibly*, HARV. BUS. REV. (Feb. 15, 2019), https://hbr.org/2019/02/how-companies-can-use-employee-data-responsibly [https://perma.cc/FE75-YR89].

264. *See id*. A Texas company given in their examples has an employee opt-in program which resulted in more frequent, but shorter, breaks which turned out to be exactly what employees needed. This was accomplished through employees opting in and analyzing their own work habits.

265. Ajunwa et al., *supra* note 10, at 774.

266. *Id*.

267. *See supra* Part II.B.i.

268. Ajunwa et al., *supra* note 10, at 772.

269. *See supra* Part III.B.

270. *See* Brand, *supra* note 228, at 12.

271. *Cf. Patent Trolls*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/resources-patent-troll-victims [https://perma.cc/T2ME-GT9D] (a Privacy Troll would be similar to the concept of "Patent Trolling" where one uses the legal system to simply find ways to sue another without any real claim, knowing that it is often cheaper and easier to settle than it is to fight the bogus patent).

standing issues in the Federal courts. In 2016, the Supreme Court laid out that even though one may have the ability to sue for statutory damages, standing still requires some form of concrete injury.[272] Any legislation in the United States will thus need to push the intangible harms that could come from mishandled PII into something concrete, "irrespective of financial harm."[273] The Congressional Research Service presents two ways in which Congress could do this: (1) tying the harm to nuisance or another traditional harm in English law, or (2) tie the right of action to chains of causation as a new tort.[274]

Over time, many of these recommendations may cease to be an issue, as the market influence of the EU means that its GDPR's mere existence is causing companies to willingly comply.[275] However, with the U.S. legal system not yet shifting towards what appears to be an emerging global privacy standard, and with Saudi Arabia's similarly situated, one can easily see that the landscape of international commerce is still fraught with uncertainty.

B. Considerations in Furtherance of Easing International Commerce

As the global standard seems to be slowly settling on GDPR-like protections, U.S. companies seeking to conduct international trade will increasingly expose themselves to unknown levels of risk.[276] As risk management is all about defining, quantifying, and managing risks to companies through establishing what is the likelihood of a risk materializing into an issue and what is the impact of that risk,[277] it behooves companies to work with international authorities to define standards for PII risks.

Thankfully, frameworks to quantify these risks and begin actively managing them already exist.[278] Unfortunately, tools like the EU-U.S. Privacy Shield can

---

272. Spokeo Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016).

273. WILSON C. FREEMAN, CONG. RES. SERV., LSB10303, ENFORCING FEDERAL PRIVACY LAW –CONSTITUTIONAL LIMITATIONS ON PRIVATE RIGHTS OF ACTION 3 (May 31, 2019).

274. *Id*.

275. Alo, *supra* note 66, at 1134; *accord* Rustad & Koenig, *supra* note 30, at 453 ("In the past several months, major U.S. information companies have pledged to comply with the GDPR and, in some cases, extend the Resolution's protections to citizens around the world.").

276. Rustad & Koenig, *supra* note 30, at 453; *accord see generally The OECD Privacy Framework*, *supra* note 173, *and* Alo, *supra* note 67, at 1134, *and* McKay Cunningham, *Complying with International Data Protection Law*, 84 U. CIN. L. REV. 421, 450 (2016) (threat of truncation from the European Market is a huge risk for most companies, ensuring compliance which edges ever closer towards establishing a norm to be recognized in international law).

277. Gregory M. Becker, *A Practical Risk Management Approach*, PROJECT MGMT. INST. (Oct. 26, 2004), https://www.pmi.org/learning/library/practical-risk-management-approach-8248 [https://perma.cc/S48W-8QCL].

278. *See supra* Part II.B (compliance with the GDPR will, *de facto*, create a risk management framework for a given corporation); *accord see supra* Part II.D.ii (the ILO's employee privacy rights framework has been in existence for over two decades and its guidance is as helpful now as it was in the 1990s).

create an incentive not to voluntarily comply.[279] While the ability to comply with a voluntary shield can create a good marketing buzz and give one some good-will with one's market, the failure to live up to voluntary standards can create a backlash and fines.[280] The answer to this is to set international norms. This will either happen automatically through the GDPR as companies (and countries) move to comply with it,[281] or legal scholars and authorities can get ahead of the emerging norm and seek to shape it alongside legislators and international policymakers. Self-regulation is no longer an option, despite it being "less bureaucratic and costly than abiding by federal restrictions."[282]

One simple area where the United States, the EU, and the rest of the world need to reach an accord is in the treatment of metadata. The United States tends not to treat metadata the same as data, under what is known as the third-party doctrine.[283] Under the third-party doctrine, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[284] In *Smith*, the defendant had no right to privacy because he "voluntarily" gave up his information—that is, the number he dialed—to the phone company by dialing the phone. Any time one "voluntarily" gives up one's information, the expectation of privacy is gone in the United States[285]

---

279. *See supra* Part III.A (if a company volunteers to be part of the Privacy Shield, they expose themselves to risks of false advertising, whereas if a company does not, they really cannot get in trouble except for losing out on one potential marketing slogan of GDPR compliance).

280. *FTC Announces Settlements with Four Companies Related to Allegations they Deceived Consumers Over Participation in the EU-US Privacy Shield*, *supra* note 237. The FTC's enforcement can only happen to companies which volunteer to join the Privacy Shield, and the companies in trouble for it are only in trouble because they volunteered and then did not live up to the standards. A reasonable conclusion, but one which defeats the purpose of the GDPR and can make it more difficult to work with EU-based companies, is simply 'do not volunteer.'

Another answer is to structure one's data infrastructure in such a way that even if one were collecting it on EU citizens, one never collects it in the EU.

281. *See* Rustad & Koenig, *supra* note 30, at 454 ("the GDPR is rapidly evolving into the transnational gold standard of data protection.").

282. Kuempel, *supra* note 22, at 217. Ms. Kuempel's article goes on to point out, on page 218, that the U.S. Senate found companies varied privacy practices and norms cause effective self-regulation to become nearly unenforceable and highly impractical at best. *Id*. at 218.

283. *See* Smith v. Maryland, 442 U.S. 735, 743-744 (1979).

284. *Id*.

285. Louis Menand, *Why Do We Care So Much About Privacy?*, THE NEW YORKER (June 18, 2018), https://www.newyorker.com/magazine/2018/06/18/why-do-we-care-so-much-about-privacy [https://perma.cc/E6HJ-TF8X]; *but see* Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (wherein the Supreme Court held that cell phone location data is far more revealing than merely dialing another person's phone number, and thus should not fall under the third party doctrine).

While *Carpenter* means that the Court is acknowledging some forms of metadata are damaging, the case is a far cry from meaningful legislation to settle how metadata will be treated. It is, however, a case which may be signaling a change in the Court's understanding of privacy and privacy data.

Contrast the United States' position on metadata with the Kingdom of Saudi Arabia's and the EU's. In Saudi Arabia, the telecommunications act prohibits at least some metadata from being released, but it is unknown if other types of metadata would be protected under Sharia as there is no general privacy law.[286] In the EU, metadata is treated absolutely the same as regular data and is considered every bit as PII.[287] This creates possibly three different expectations of how PII-based metadata will be treated. Some companies may even certify they are GDPR compliant without considering the metadata problem and thus be found guilty of deceptive business practices if they volunteer to be under the Privacy Shield.

Even if the ultimate answer is to simply treat metadata as the EU does, this at least provides companies with a stable base from which they can conduct risk management. If U.S.-based companies wish to advocate for the exclusion of some types of metadata in future regulations and norms, now is the time to do so. Said companies would need to make a compelling case for why the metadata is not inherently as risky as the actual data.

Another area in which international organizations can assist is in crafting rules for enforcing judgments specifically around privacy data. This would help prevent situations as in our hypothetical where a company does not know with certainty whether a judgment will be enforced and must thus assume a higher level of risk.[288] If multinational companies intend to continue employing global workforces, then these sorts of conflicts are going to become commonplace. Failure to address what is or is not enforceable across transnational lines only causes unnecessary fragmentation and stress among the nations over time.

CONCLUSION

This Note demonstrated, through a fictitious scenario, how modern privacy regulations, when applied to a global workforce, are inadequate for both employer and employee. Employers have growing appetites for Big Data in order to reach ever greater efficiencies and increase economic output. Big Data feeds new and growing automated predictive and analytical systems that may demonstrate unwelcome emergent behavior—from accidental blacklisting of employees to just intruding on employees' daily lives.

In an ever-more-interconnected global workforce, the world now has a patchwork of laws, regulations, and rights, which range from patchwork, highly sector-driven (the United States), to comprehensive (the EU), to evolving from other laws without clear direction (Saudi Arabia). A minefield of international treaties, agreements, and recommendations—from the ILO to the Privacy Shield—further complicate matters between trading partners and employers who hire employees from other jurisdictions. Extraterritoriality and laws surrounding enforcements of foreign judgments create dead-ends for employees along with

---

286. TELECOM ACT, No: M/12, § 9 (June 6, 2001); *see supra* Part II.C.

287. Brkan, *supra* note 75, at 873.

288. *See supra* Part III.B.

uncertainty and risk of losing access to a market for employers.

All of these factors contribute to employees having a difficult-to-impossible road in obtaining satisfaction for their privacy concerns. Companies have near limitless risk with little ability to mitigate said risk other than to not engage and never volunteer to do better. This, in turn, creates a perverse incentive to use loopholes and exercise compliance by never improving on one's own corporate standards. In an era of increasing expectations of social responsibility on corporations, this seems odd.

The global community can and must do better for both halves of this whole economic equation. As it stands now, there is an emerging global norm around EU privacy practices. While these practices are better than nothing, they still have enforceability issues and cultural issues in interpreting such concepts as metadata which drive uncertainty. Thus, governments need to proactively take steps to provide rules of the road for both employers and employees. This can be done through a number of initiatives such as profit-sharing employee data, changes in how statutory damages are assessed (as opposed to statutory fines), and settling on international definitions for what is privacy data (*e.g.* metadata).

As technology continues to progress, artificial intelligence is going to increase stress on this global system unless governments, industries, and non-governmental organizations can forge a path forward together. A failure to act may result in the most hilariously depressing artificial intelligence driven dystopia possible: one where the machines did not rise up, but merely accidentally oppressed individuals and created a system of autonomous social judgment by incautiously making decisions based on patterns too vast and obtuse for any mortal mind to grasp all at once. This is not to say that such a scenario would be unfixable after-the-fact, but merely that the situation need never to occur to begin with.

All we have to do is act.