CREATING A 21ST CENTURY PERSONAL DATA PROTECTION REGIME IN THE UNITED STATES: CONSENT, OVERSIGHT, AND REMEDIAL REFORM; LESSONS FROM THE GERMAN MODEL

JARED MEHRE*

ABSTRACT

This paper argues that the United States' sectoral approach to personal data protection is inadequate for the twenty-first century. In order to modernize its sectoral regime, the United States should adopt some reforms used in the comprehensive data protection regime employed by The Federal Republic of Germany (Germany). These reforms include: requiring companies to obtain consent from consumers to access their data, creating an oversight committee with enforcement powers to ensure compliance with existing data protection laws, and adopting data protection laws that supersede the common law and provide data subjects with a solid foundation for suing personal data collectors when their personal data is abused or breached.

* Jared Mehre is a third year law student at the University of Wisconsin Law School. Prior to law school, he obtained his Bachelor of Arts in Political Science, Sociology, and Legal Studies with a certificate in German Language. Jared would like to thank: the Wisconsin International Law Journal Senior Board for the opportunity to publish, Taylor Nye for her years of editorial mentorship, and his parents Kelly and Roger Mehre for their unwavering support.

INTRODUCTION

In the technological era, we provide corporations and companies with an abundance of our personal data on a daily basis. When we shop on Amazon.com we provide that company with our credit card information, mailing address, and name.[1] When we purchase a product from Apple, we are required to register that product and sign an agreement, which provides that use of the product is consent to collect such information as phone numbers, birthdate, geographic location, website searches, and occupation.[2] Companies can collect personal data for a variety of purposes including: advertising targeting,[3] collecting and selling personal data[4], and medical purposes.[5] While consumers may appreciate a company's ability to tailor advertisements or provide curative products to them, most of the time people are unaware that their data is being collected and that there is very little they can do to prevent

---

1 *Amazon Privacy Notice*, https://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy?ie=UTF8&nodeId=468496#GUID-1B2BDAD4-7ACF-4D7A-8608-CBA6EA897FD3__SECTION_467C686A137847768F44B619694D3F7C (last visited May 21, 2017).

2 *Privacy Policy*, http://www.apple.com/privacy/privacy-policy/ (last visited Feb. 18, 2017).

3 *Getting to Know You*, ECONOMIST (Sept. 11, 2014), http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party.

4 *Consumers need a new legal righto control personal data*, LA TIMES (Aug. 3, 2015), http://www.latimes.com/opinion/op-ed/la-oe-rule-data-privacy-agencies-20150730-story.html.

5 Novartis, *Privacy Policy*, https://www.nibr.com/privacy-policy (last visited May 21, 2017).

a company from taking their data or to seek a remedy when the data that is held by a company is breached by or sold to a third party.[6]

The United States has chosen to abide by an ad hoc, sectoral approach for its personal data protection laws.[7] This approach has been maintained, despite other developed nations having comprehensive personal data protection, because of the United States' constitutional structure emphasizing negative liberties instead of positive liberties.[8] For this reason, companies are largely responsible for their own self-regulation, and the government only steps in to certain industries when it determines that the particular industry would benefit from oversight by the US government.[9] Examples of these types of regulations include the Health Insurance Portability and Accountability Act of 1996 (HIPPA), the Fair Credit Reporting Act (FCRA), the Children's Online Privacy Protection Act (COPPA), the Gramm-Leach-Bliley (GLB), and various state laws across many sectors.[10] However, this method of personal data protection is deficient for not informing consumers when their data is being taken, how it is being used, and whether they can receive a remedy when their data is breached.

Meanwhile, the German model of data protection is comprehensive and provides German consumers with adequate protection.[11] Germany boasts the most stringent data protection laws in the world; the laws are expansive in their coverage and strict in their punishment.[12] The Germans have strong personal data protection laws because they are required to under the Treaty on European Union (TEU), Treaty on the Functioning of the European Union (TFEU), and because they have passed their own comprehensive personal data protection laws that apply to the entire federal state.[13] While the German model of data

---

6 Tanith L. Balaban, *Comprehensive Data Privacy Legislation: Why Now is the Time?*, 1 CASE W. RES. J.L. TECH. & INTERNET 1, 18–24 (2009).

7 Patrick J. Murray, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?*, 21 FORDHAM INT'L L. J. 932, 970–71 (1998).

8 *See id.* at 970.

9 *See* Lisa J. Sotto & Aaron P. Simpson, *United States*, *in* DATA PROTECTION & PRIVACY: IN 31 JURISDICTIONS WORLDWIDE, 208, 208 (Rosemary P. Jay ed., 2015).

10 Richard J. Peltz-Steele, *The Pond Betwixt: Differences in the US-EU Data Protection/Safe Harbour Negotiation*, 19 J. INTERNET L. 1, 18 (2015).

11 *See* Anne-Marie Zell, *Data Protection in the Federal Republic of Germany and the European Union: An Unequal Playing Field*, 15 GERMAN L.J. 461, 464–72 (2014).

12 *See id.* at 462, 464–72.

13 *See* Charter of Fundamental Rights of the European Union, art. 7, 2000 O.J. (C 364) 18 [hereinafter Charter]; Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, BUNDESGESETZBLATT [BGBL] I at 66, last amended by Gesetz [G], Aug. 14, 2009 BGBL I

protection is preferable, it would not be possible for the United States to adopt all of its aspects due to constitutional obstacles as well as the fact that the United States is so far behind the model created by Germany.[14] Instead, the United States should adopt three reforms taken from the German model that would increase personal data protection awareness for the American public as well as substantially bolster the protection that companies provide to their patrons.

First, the United States should require data collectors to ask for express consent from their data subjects before they are allowed to collect their data. Under the German model, data collectors are required to give notice of data collection and obtain express consent from the data subject that the data collector may collect and use the data subject's personal data.[15] This reform is important because most people are not aware that their data is being collected or what it is being used for.[16] Most often, websites consider use of their service to be consent for data collection, and if consumers are aware that their data is being taken, they assume that the data will be used and protected in an appropriate manner.[17] However, this is not the case; companies do not use a standard agreement when it comes to personal data protection.[18] Companies create a variety of privacy agreements, which form the individual standard that the company intends to hold itself to with its patrons, and these contracts are written to favor the data collector, not the data subject.[19]

Second, the government should create an independent oversight committee to ensure that current data protection laws are followed. Under the German model, data collectors are required to hire an in-house enforcer of data protection laws, who has broad powers to investigate the

---

at 2814 (Ger.), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf [hereinafter BDSG].

[14] EUROPEAN PARLIAMENT DIRECTORATE-GEN. FOR INTERNAL POLICIES, A COMPARISON BETWEEN U.S. AND E.U. DATA PROTECTION LEGISLATION FOR LAW ENFORCEMENT 7 (2015), http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf.

[15] Zell, *supra* note 11, at 465.

[16] Paul Boutin, *The Secretive World of Selling Data About You*, NEWSWEEK (May 30, 2016), http://www.newsweek.com/secretive-world-selling-data-about-you-464789.

[17] Dennys Marcelo Antonialli, *Watch Your Virtual Steps: An Empirical Study of the Use of Online Tracking Technologies in Different Regulatory Regimes*, 8 STAN. J. C.R. & C.L. 323, 346–47 (2012).

[18] *Id.* at 347.

[19] *See* Sebastian Zimmeck, *The information Privacy Law of Web Applications and Cloud Computing*, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 451, 454–59 (2013).

data collector's operations.[20] This is in order to ensure compliance with data protection laws. The United States would benefit from a single oversight committee for two reasons. First, data protection enforcement is carried out by several bodies whose duties are not necessarily clear under the current scheme.[21] Having a single body would increase efficiency and compliance. Second, a lack of enforcement in the United States has allowed data collectors to employ lax data protection procedures, which have led to massive data protection breaches.[22] Increasing enforcement would force data collectors to monitor their processes more closely or face penalties.

Lastly, the United States should update its laws to provide data subjects with adequate routes to sue data collectors when the data collectors abuse their data subjects' data. Since German data protection laws are comprehensive, consumers have many ways to seek remedies if the government does not catch the data collector breaking the law first.[23] Since the United States lacks a right to privacy in the private arena and has a patchwork of data protection laws created by sector, most personal data protection violations must be brought under the common law.[24] The problem with seeking a remedy under tort, contract, or property law is that these common law remedies were created well before digital data existed, and our concept of data does not fit any of the common law molds.[25] This has led to data subjects being unable to attain a proper remedy or remedy at all when their data is breached by a third party and used for malicious purposes.

Part I of this paper provides background information on the three systems of personal data protection that will be analyzed in this paper. Part II argues that businesses should be required to ask for consent from data subjects before they are allowed to collect their personal data information. Part III proposes that the United States create an oversight body and give it enforcement power to ensure compliance with the current system. Part IV shows that a comprehensive personal data

---

[20] John Schinasi, *Practicing Privacy Online: Examining Data Protection Regulations Through Google's Global Expansion*, 52 COLUM. J. TRANSNAT'L L. 569, 594–95 (2014).

[21] *Id.* at 581.

[22] *See* Dave Lewis, *Notes from RSA: Accountability in Security*, FORBES (Apr. 29, 2015, 6:30 PM), http://www.forbes.com/sites/davelewis/2015/04/29/notes-from-rsa-accountability-in-security/#47e46e292163 [https://perma.cc/HV4B-D7T8].

[23] Zell, *supra* note 11, at 464–72.

[24] Balaban, *supra* note 6, at 18.

[25] *See* Candice L. Kline, *Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute*, 39 U. TOL. L. REV. 433, 460 (2008).

protection law should be implemented to replace the inadequate remedies provided to consumers by the current data protection regime.

I. PERSONAL DATA PROTECTION REGIMES OF THE EUROPEAN UNION, GERMANY, AND THE UNITED STATES

A. EUROPEAN UNION DATA PROTECTION LAW

The background section will begin by describing the personal data protection laws of the European Union (EU). Understanding the EU's laws on personal data protection is essential to understanding the German model of personal data protection because Germany is a member of the European Union and therefore must implement EU law. It is also useful for setting up the cultural differences between how Europe sees privacy and how the United States sees privacy. There are two major data protection laws in the EU: the first is found in the Charter of Fundamental Rights of the European Union (Charter) and the second is in the Data Protection Directive.

The Charter was enacted in 2000 and made binding on all EU Members States in 2007 through the Lisbon Treaty.[26] The Charter enshrines certain political, social, and economic rights for citizens of the EU.[27] The Charter itself is part of what could be considered the Constitution of the European Union and therefore is given the same authority as the US Constitution.[28] In relevant part, Article 8 of the Charter includes data protection laws for EU citizens. Article 8(1) states that, "[e]veryone has the right to the protection of personal data concerning him or her."[29] Article 8(2) requires that:

> [Personal] data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[30]

---

[26] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities, Dec. 13, 2007, O.J. (C 306) 1.

[27] Charter, *supra* note 13.

[28] Sarah Sy, *Fact Sheet on the European Union*, EUROPEAN PARLIAMENT, http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_1.1.6.html (last visited Oct. 6, 2016).

[29] Charter, *supra* note 13, art. 8(1).

[30] *Id.* art. 8(2).

Lastly, Article 8(3) states that, "[c]ompliance with these rules shall be subject to control by an independent authority."[31]

Article 8 of the Charter makes personal data protection law a right to all citizens of the European Union. The Court of Justice of the European Union, the highest court in the EU, has interpreted Article 8 to "proclaim[] the right of the protection of personal data."[32] The Charter provides EU citizens with data protection as a freedom, but it does not explicitly state what adequate data protection policies look like. The EU provided guidance on this subject before the Charter was created.

The EU's Data Protection Directive sets up the foundation for EU data privacy protection and can be broken into eight main principles: "(1) purpose limitation, (2) data quality, (3) data security, (4) special protection for sensitive data, (5) transparency, (6) data transfers, (7) independent oversight, and (8) individual redress."[33] These elements are extensive and far-reaching. It also must be noted that overall these elements are all emphasized more in European law than US law and some are unique to European law.[34]

Member States are required to implement policies consistent with the eight elements. While each Member State may implement them in its own way, the result must be consistent with the Data Protection Directive. First, information can only be collected for a specific purpose and can be stored no longer than needed.[35] Second, data must be of a high quality and updated.[36] Third, reasonable measures must be taken to secure data transmissions.[37] Fourth, governments are forbidden from collecting data with regard to "racial or ethnic origin, political opinions, religious or philosophical beliefs . . . [or] concerning health or sex life."[38] Fifth, EU citizens are required to be notified when their personal data is being collected, who it is being collected by, and for what purpose it is

---

[31] *Id.* art. 8(3).

[32] C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Judgment (Grand Chamber), ¶ 69 (May 13, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62012CJ0131&from=EN.

[33] Carolyn Hoang, *In the Middle: Creating a Middle Road Between U.S. and EU Data Protection Policies*, 32 J. NAT'L ASS'N ADMIN. L. JUDICIARY 810, 830 (2012).

[34] Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures*, 126 HARV. L. REV. 1966, 1976 (2013).

[35] Hoang, *supra* note 33, at 830.

[36] *Id.*

[37] *Id.*

[38] Council Directive 95/46/EC, art. 8 of Oct. 24, 1995, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281).

being used.[39] Sixth, a person's personal data may not be transferred to a third party without that person's consent.[40] Seventh, Member States must set up an independent body to audit data processing systems and investigate complaints.[41] Lastly, Member States can only exchange data between other Member States and non-Member States that have adequate data protection policies.[42] The United States has been deemed to have inadequate data protection policies by the EU.[43]

Additionally, the European Union has recently decided to update its data protection laws under the General Data Protection Regulation.[44] While the General Data Protection Regulation will replace the Data Protection Directive, businesses are not required to adapt to its provisions until May 25, 2018.[45] Because of this, European states are still adapting to the new changes in the European Data Protection laws and are uncertain of how the laws will be interpreted.[46] While the General Regulation will strengthen European Data Protection laws, a comparison between the General Regulation and the US data protection laws will not provide more information than a comparison between the United States and Germany. So, while Germany will have to change its data protection laws over the next two years, the laws that are currently in place are still some of the strongest data protection laws in the world.

B. GERMAN DATA PROTECTION LAWS

Germany began implementing data protection laws long before the Data Protection Directive came into force. In 1970, the German state of Hesse enacted the world's first comprehensive information privacy statute.[47] While it cannot be confirmed, many believe that Germany was motivated to pass privacy laws because of its Nazi history. The Nazi government was able to use its extensive records to single out the Jewish

---

[39] Hoang, *supra* note 33, at 830.

[40] *Id.* at 830–31.

[41] *Id.* at 831.

[42] *Id.*

[43] Peltz-Steele, *supra* note 10, at 21.

[44] W. Gregory Voss, *European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and The Right to Delisting*, 72 BUS. L. 221, 221–22 (2016).

[45] *Id.* at 222.

[46] *Merkel Call for Loosening of 'Restrictive' German Data Protection Laws*, DEUTSCHE WELLE (Nov. 17, 2016), http://www.dw.com/en/merkel-calls-for-loosening-of-restrictive-german-data-protection-laws/a-36431222.

[47] Schwartz, *supra* note 34, at 1969.

people before the Holocaust.[48] Hesse was followed by the other German states and finally by the German Federal Government.[49] German data protection laws are numerous and extensive, and this note will only be analyzing the *Bundesdatenschutzgesetz* (Federal Data Protection Act) (hereinafter BDSG) and the *Telemediengesetz* (Telemedia Act) (hereinafter TMG). Both of these laws apply only to companies that exist within the borders of Germany.

The BDSG was passed in 2003 and amended in 2009 and provides German citizens a high level of data protection, specifically with regard to the, "collection, processing and use" of personal data.[50] The BDSG can be boiled down to three notable attributes:

> (1) it requires data controllers to obtain express consent from an individual for the processing, collecting, and use of the individual's personal data; (2) it contains a 'list privilege' exception, with conditions that data controllers can fairly easily meet; and (3) it requires data controllers to notify affected individuals of data breaches, and conditions this notification requirement on a single instance of breach.[51]

The first notable attribute of expressed consent states that personal data may only be collected, processed or used if the data subject expressly consents to giving up that information.[52] The purpose of consent in this context is to make sure that the data subjects are making informed and voluntary choices about their personal data.[53] In addition to getting express consent, the data controller must also provide the data subject with the reason for "the collection, processing or use" of the data.[54] Lastly, the consent is typically required to be in writing.[55]

The second notable attribute of the BDSG is that it includes a "list privilege exception" that data controllers can easily meet when they must collect data.[56] The list privilege exception refers to an exception that allows businesses to trade and sell data that is within a specific list of characteristics.[57] The exception includes lists of data that deal with a

---

48 Hoang, *supra* note 33, at 829–30.
49 Schwartz, *supra* note 34, at 1969.
50 *See* BDSG, *supra* note 13.
51 Zell, *supra* note 11, at 465.
52 *Id.*
53 *Id.* at 465–66.
54 BDSG, *supra* note 13.
55 *Id.*
56 Zell, *supra* note 11, at 465.
57 *Id.* at 466.

specific group of information, such as: "occupation, name, title, academic degrees, address, and year of birth."[58] However, these lists can only be sold and used for advertising purposes if the data controller has obtained consent from the data subject, or if the data controller maintains records of where the data originated and was transferred from for a period of two years.[59]

Lastly, the data breach notification requires data controllers to inform data subjects if their data has been breached. This provision only applies to four categories of data: 1) special types of personal data, such as race, ethnicity, political opinions, religious or philosophical beliefs, union membership, health, or sex life; 2) personal data subject to professional secrecy; 3) personal data related to criminal or administrative offences or the suspicion thereof; and 4) bank account or credit card information.[60] A breach occurs when data stored by a data controller has been "unlawfully transferred or otherwise unlawfully revealed to third parties" and there is a "threat of serious harm to the data subject's rights or legitimate interest."[61] The threshold here is as low as it could possibly be, meaning that even if one person's personal data were threatened the data collection company would be required to notify the data subject.[62] Additionally, the notification process requires the data controller to "describe the nature of the unlawful access and include recommendations for measures to minimize possible harm." The data controller must also notify the independent supervisory authority in Germany, state the "possible harmful consequences of the unlawful access," state what they have done to ameliorate the situation at that point.[63]

The second important law in Germany is the TMG, which regulates online services such as websites and e-mail, but does not apply to telecommunication services or broadcasting.[64] The TMG places several requirements on service providers: 1) service providers must identify the sender of a message and 2) service providers must identify

---

[58] BDSG, *supra* note 13.

[59] Zell, *supra* note 11, at 466–67.

[60] BDSG, *supra* note 13.

[61] *Id.*

[62] Zell, *supra* note 11, at 467.

[63] *Id.*

[64] *Id.* at 469 (citing the Telemediengesetz [TMG] [German Telemedia Act], Feb. 26, 2007, BUNDESGESETZBLATT [BGBL] I at 179, art. 1 (Ger.), https://www.gesetze-im-internet.de/tmg/TMG.pdf).

any promotional offers or advertising.[65] This means that "a game may not serve as an advertising tool unless clearly identified as such."[66] Additionally, the service providers are still subject to the consent requirement of the BDSG and cannot include consent as a requirement of the use of the telecommunication service.[67] This means that the terms and conditions of use do not count as consent and cannot be used to force people to consent before the user is allowed access to the telecommunications service.

Additionally, the TMG endows several individual rights to users of the service. Under the TMG individuals have the rights to: "1) terminate telemedia service at any time; 2) have his or her personal data immediately deleted following termination of the telemedia service; 3) use telemedia service with no disclosure of use to third parties; and, importantly, 4) pseudonymous use of telemedia services."[68] The last right may be unfamiliar to many readers and it refers to Germany's requirement that service providers must allow people to use the service anonymously.[69] The service provider must inform the individual about this possibility and cannot create user profiles and attempt to figure out who the anonymous person is.[70] The service provider can still use the anonymous profile for market research, but they cannot refuse to create a fake profile for someone.[71]

C. DATA PROTECTION LAWS OF THE UNITED STATES

Lastly, the United States handles data protection differently from Germany and the rest of the EU. The United States does not have an "omnibus approach to the protection of personal data. Instead the United States continues to address personal data problems through ad hoc,

---

[65] Zell, *supra* note 11, at 471 (citing Telemediengesetz [TMG] [German Telemedia Act], Feb. 26, 2007, BUNDESGESETZBLATT [BGBL] I at 179, §§ 6.1.1-4 (Ger.), https://www.gesetze-im-internet.de/tmg/TMG.pdf).

[66] Zell, *supra* note 11, at 471.

[67] *Id.* (citing the Telemediengesetz [TMG] [German Telemedia Act], Feb. 26, 2007, BUNDESGESETZBLATT [BGBL] I at 179, § 12.3 (Ger.), https://www.gesetze-im-internet.de/tmg/TMG.pdf).

[68] *Id.*

[69] *Id.*

[70] *Id.* (citing the Telemediengesetz [TMG] [German Telemedia Act], Feb. 26, 2007, BUNDESGESETZBLATT [BGBL] I at 179, §§ 13.6, 13.4.6 (Ger.), https://www.gesetze-im-internet.de/tmg/TMG.pdf).

[71] Zell, *supra* note 11, at 472.

sector-by-sector solutions."[72] Privacy law has developed differently in the United States than in Germany for three reasons. First, the US Constitution does not include a guaranteed right to privacy for personal data.[73] While the US Supreme Court has stated that there is an "expectation of privacy" within the Bill of Rights, that expectation "is not preserved when an individual discloses data to a third party."[74] Second, in the US system of federalism provides the federal government with a "limited power[] to erect a nationwide level floor of statutory and regulatory privacy protection."[75] Finally, the Bill of Rights is a document that enshrines negative liberties and not positive liberties. Because of this, the Bill of Rights protects people from the actions of the government, but it does not assist in protecting people from the actions of others.[76] For the above reasons, creating data protection laws requiring private citizens and entities to be responsible for the protection of others data has been difficult to create.

The United States does not lack personal data protection laws; however, the laws are only in certain industries. Some of the personal data protection statutes passed by the federal government include: the Fair Credit Reporting Act (FCRA) (1970), the Family Educational Rights and Privacy Act (FERPA) (1974), the Privacy Act (1974), the Video Privacy Protection Act (VPPA) (1988), the Health Insurance Portability and Accountability Act (HIPAA) (1996), and the Children's Online Privacy Protection Act (COPPA) (1998).[77] Each of these statutes "defines its own scope in accordance with the problem it anticipates, and its oversight or enforcement mechanism."[78]

The United States has adopted a few regulations that exist in the German model; however, these regulations are in different subsections of the private sector, have varying degrees of enforcement, differ between the federal and state government, and vary between the different states.[79] One example of this is that forty-seven states, Washington D.C., and

---

[72] Murray, *supra* note 7, at 969–70.

[73] *See generally* U.S. CONST.

[74] Morey Elizabeth Barnes, *Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive*, 27 NW. J. INT'L L. & BUS. 171, 175 (2006).

[75] Peltz-Steele, *supra* note 10, at 17.

[76] Murray, *supra* note 7, at 970.

[77] Peltz-Steele, *supra* note 10, at 18.

[78] *Id.*

[79] Murray, *supra* note 7, at 981.

three territories have adopted data breach notification laws.[80] However, there is surely variation between these laws, and it is likely that they are not as comprehensive as the data protection laws of Germany and the EU.

Additionally, the personal data laws of the United States are not housed in constitutional law like the German model; they are housed in tort, property, or contract law.[81] For this reason, it is difficult for businesses to establish their level of responsibility for personal data protection.[82] Additionally, because the United States subscribes to an idea of self-regulation with reference to its personal data, consumers are often unable to have control over their personal data, which can lead to misuse of that data by companies.[83] Because the system is complex and unpredictable, the US personal data protection laws also do not afford much redress to data subjects from businesses if their privacy is breached.

The gap between Germany's data protection and the United States' lack thereof is significant and cannot be captured in a single note. In the following section, I have reduced my analysis to the three areas that would create meaningful protections for data subjects. The first is a requirement that data collectors must procure express consent for the collection and use of a data subject's personal data before they can collect it. Second, the United States should create an independent enforcement authority to regulate data collectors and enforce person data protections. Third, the United States should implement a comprehensive data protection law to supersede the common law in order to improve data subjects' access to relief when their rights are violated.

II. THE IMPORTANCE OF CONSENT IN PERSONAL DATA COLLECTION

Under the BDSG, all German companies are required to obtain express consent from their patrons before they are allowed to collect, process, or use any personal data.[84] Personal data under the BDSG is

---

[80] Peltz-Steele, *supra* note 10, at 18.

[81] *Id.*

[82] Thomas Davenport, Opinion, *Should the U.S. Adopt European-Style Privacy Protection*, WALL ST. J. (Mar. 10, 2013), http://www.wsj.com/articles/SB10001424127887324338604578328393797127094.

[83] *Id.*

[84] Zell, *supra* note 11, at 465.

"any information concerning the personal or material circumstances of an identified or identifiable individual."[85] This means that personal data is any data that can be used to find a specific individual. This is vastly unlike most of the data protection laws in the United States. Since the United States has a sectoral approach to its data protection law, some sectors do have consent requirements; however, most do not.[86] Additionally, the consent laws vary between states as well due to the United States' federalist structure.[87] However, the best the example of the differences is at the federal level.

Under the United States' sectoral approach, only some federal laws require consent to be obtained when a company is collecting, processing, or using personal data. One of these federal laws is the FRCA, which requires a consumer reporting agency to obtain written consent from the person before it can give that information to an employer or potential employer.[88] However, while the Fair Credit Reporting Act may have some consent requirements as to how personal data may be used, it does not have consent regulations on how the data falling under its protection is collected.[89]

Another piece of federal legislation that provides some amount of personal data protection is the HIPPA. HIPPA does have a high level of protection with regard to medical information and requires covered entities to satisfy the regulation's requirements before they may disclose or use a patient's protected health information.[90] However, this is separate from the issue of consent, which a physician is permitted, but not required to obtain.[91] Under HIPPA, a health care provider is allowed to make consenting to the privacy practices of the institution contingent upon agreeing to receive care.[92] This is a second federal regulation of the United States that would not pass under Germany's BDSG.

---

[85] BDSG, *supra* note 13.

[86] Murray, *supra* note 7, at 981.

[87] *Id.*

[88] First Advantage, *Fair Credit Reporting Act*, THREE RIVERS MFRS.' ASS'N, http://www.trma.org/pdf/fcra_procedures_&_consent_form.pdf (last visited Oct. 7, 2017).

[89] Hoang, *supra* note 33, at 821.

[90] Uses and Disclosures for Which an Authorization is Required, 45 C.F.R. § 164.508 (2016).

[91] *Consent vs. Authorization Under HIPPA*, TEX. MED. ASS'N., https://www.texmed.org/Template.aspx?id=1611 (last visited Nov. 4, 2016).

[92] *See Health Information Privacy*, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html (last visited Nov. 4, 2016).

However, the most telling comparison comes from the various guidelines made by the Federal Trade Commission (FTC). The FTC is one of the main bodies tasked with enforcing the United States' data protection laws.[93] Enforcement of data protection will be discussed in Section III; however, as one of the main personal data protection enforcement bodies the FTC has created a series of Guidelines on how businesses should conduct themselves in attaining consent for collecting, processing, and using personal data. The FTC is a good place to look for further analysis on the issue of consent because section 5 of the FTC Act is used as a way to cover any businesses that are not regulated in their use of personal data by a federal regulation.[94] The FTC has created a set of data protection guidelines and it is tasked with regulating all business sectors that collect data; its guidelines are recommended to all sectors.

A. THE UNITED STATES HAS SIGNALED THAT IT BELIEVES IN CONSENT, BUT HAS NOT CODIFIED CONSENT IN THE PRIVATE SECTOR

The first set of guidelines is the FTC Fair Information Practice Principles. These principles got their start within a study group of the Department of Health, Education and Welfare.[95] The goal of the study was to discover businesses' generally held online privacy practices and then to codify those principles into a series of recommendations.[96] The study group produced their findings in a 1973 report named *Records, Computers and the Rights of Citizens*, which identified "five key principles to be respected in any information-keeping system."[97] Two decades later, the FTC broke up the report into five different core principles each recommending a different set of rules for privacy rights in an online setting: Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, and Enforcement/Redress.[98]

---

[93] Hoang, *supra* note 33, at 826.

[94] *Id.* at 822–23.

[95] Sarah Andrews, *Protecting Privacy through Government Regulation*, 2 SEDONA CONF. J. 1, 3 (2001).

[96] FED. TRADE COMM'N, FAIR INFORMATION PRACTICE PRINCIPLES 26–27 (2007), https://web.archive.org/web/20100309105100/http://www.ftc.gov/reports/privacy3/fairinfo.shtm#Notice/Awareness.

[97] Andrews, *supra* note 95, at 3.

[98] FED. TRADE COMM'N, *supra* note 96, at 28.

The first two core principles directly address the issues surrounding consent. The Notice/Awareness Principle states that "consumers should be given notice of an entity's information practices before any personal information is collected from them."[99] The principle does not require that people must consent to having their data collected; it only recommends that they should be made aware of the data practices of the business that is collecting their data.[100] The principle here is not as broad as the BDSG. The BDSG requires that companies obtain consent for collecting, processing, and using personal data as well as inform the individual of the purpose of the collection, processing, and usage of the data.[101] The Awareness/Notice principle is significantly narrower than the consent requirement of the BDSG because notice is only available at the collection phase and not after.[102] The principle does not recommend that express consent be given, only that the data subject could find out what the privacy practices are.[103]

The second principle, Choice/Consent, refers to the way that information that has already been collected is used.[104] Specifically, this principle addresses the secondary uses of information.[105] Secondary uses refer to instances beyond the contemplated transaction that can be internal or external.[106] An internal purpose would be when a data collector uses the data in a way that wasn't part of the original agreement, such as, "placing the consumer on the collecting company's mailing list."[107] An external purpose is a process that takes place when the personal data is transferred to an entity other than the collecting company that was not part of the original agreement.[108] The principle recommends that companies provide an opt-in or opt-out scheme whereby patrons must take affirmative steps to either allow or prevent a

---

[99] *Id.*

[100] *Id.* at 30–36.

[101] Zell, *supra* note 11, at 465–66.

[102] FED. TRADE COMM'N, *supra* note 96, at 30–36.

[103] *Compare* Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, BUNDESGESETZBLATT [BGBL] I at 66, last amended by Gesetz [G], Aug. 14, 2009 BGBL I at 2814, § 4(a).1 (Ger.), https://www.gesetze-im-internet.de/englisch_bdsg/englisch_bdsg.pdf *with* FED. TRADE COMM'N, *supra* note 96, at 30–36.

[104] FED. TRADE COMM'N, *supra* note 96, at 41–43.

[105] *Id.* at 42.

[106] *Id.*

[107] *Id.*

[108] *Id.*

data-collecting company from collecting or using their personal data.[109] Distinction between the principles and the BDSG does not lie in whether a company has an opt-in or opt-out system, but rather in the fact that the data subject must take affirmative steps in order to express their consent. Under the BDSG, it is the company that must take affirmative steps in order to secure the data subject's express consent to collect, process, or use the data.[110] Under the principles, the onus falls on the data subject to show how they would like data collecting companies to use their personal data.[111]

However, while these recommendations do provide guidelines similar to some of the protections in Germany's BDSG, they are not codified in laws that apply to the private sector and therefore are not enforced as law by the federal government. The Fair Information and Practice Principles were codified in the Privacy Act of 1974; but, the privacy act only applies to the public sector.[112] As the FTC itself noted, "the Commission lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principles on their web sites."[113] Thus, the data collecting company has the ability to employ its own practices as it sees fit, and consumers must bear the burden of discovering what the company is able to collect, process, and use.[114]

As a result of the lack of enforcement and lack of detail with regard to what constitutes consent, data subjects are at a distinct disadvantage when it comes to knowing what data they have consented to collection by data collectors. Most companies have implemented privacy policies on their websites detailing in lengthy descriptions the terms and conditions of using their website services.[115] However, companies do not make their privacy policies easy for consumers to find. They are most often in fine print on the bottom of the website, or typically the websites do not contain enough information to convincingly state where the privacy policy can be found.[116] For example, a study found that on Adobe's website the privacy policy was on the bottom of

---

[109] *Id.* at 43–44

[110] Zell, *supra* note 11, at 465–66.

[111] FED. TRADE COMM'N, *supra* note 96, at 43.

[112] Andrews, *supra* note 95, at 5.

[113] *Id.* at 8.

[114] *See id.* at 6.

[115] *See* Antonialli, *supra* note 17, at 341.

[116] *Id.*

the website linked within the sentence: "Use of this website signifies your agreement to the Terms of Use and Online Privacy Policy (updated 07-14-2009)."[117] The limited notifications used by most websites in the United States would not be allowed under the BDSG.

Additionally, the BDSG would not allow some websites that do get consent to get it in the manner that they typically do. The BDSG typically requires data collectors to get express consent from their data subjects before they can collect, process, or use the data subjects' data.[118] The Fair Information Practice Principles do not contain "any sort of collection limitation principle prohibiting the collection of excessive data or its storage for a time longer than necessary."[119] This becomes an issue especially with websites that make visiting the website a condition of using their services. For example, Amazon.com states that "[b]y visiting Amazon.com, you are accepting the practices described in this Privacy Notice."[120] Under Amazon's scheme, a person must access the website to find out what the privacy policy is; however, once they read the privacy policy, they will only know what they have already agreed to by accessing the website.

B. A COMPARATIVE CASE STUDY IN DATENSCHUTZRICHTLINIE V. APPLE

Privacy policies that are employed in the United States have failed in German Court.[121] In a case against Apple, the *Landgericht Berlin* (District Court of Berlin) found that Apple's privacy policies violated Germany's data protection laws.[122] The privacy policy used in Germany by Apple was slightly different, but similar to the one used in the United States.[123] The Berlin District Court found that Apple's privacy policy violated Germany's data protection laws in several ways: the company asked for consent in too general a manner, the company shared

---

[117] *Id.*

[118] Zell, *supra* note 11, at 465–66.

[119] Andrews, *supra* note 95, at 7.

[120] Antonialli, *supra* note 17, at 349.

[121] *See* Landgericht Berlin [LG Berlin], Apr. 30, 2013, NEUE JURISTICHE WOCHENSCHRIFT [NJW] 2013, 2605 (Ger.).

[122] Zell, *supra* note 11, at 482–83.

[123] Loek Essers, *Apple's privacy policy violates German data protection law, Berlin court rules*, COMPUTERWORLD (May 7, 2013, 12:10 PM), https://www.computerworld.com/article/2497084/data-center/apple-s-privacy-policy-violates-german-data-protection-law—berlin-court-rules.html.

personal information too broadly, consumers were unaware of what data was being collected and how it was being used, and the company collected data from users about third parties who had not consented to giving up their personal data.[124]

It was not only the way that the data was collected that the court had a problem with, but also the type of data that Apple could ask for under its privacy policy. The BDSG protects any data that could be used to identify a single person. The court found that Apple's privacy policy violated Germany's privacy law because it allowed Apple to collect data of friends and family of the initial data subject.[125] This data could include names, addresses, email addresses, and phone numbers of people who had not personally consented to the collection of their personal data. Additionally, Apple could anonymously collect, use, and share a person's precise location data, "including the real-time geographic location of a user's Apple computer or device, in order to provide location based services like advertising on Apple products."[126] The BDSG prevented Apple's privacy policy from being used in Germany, but it would have been allowed in the United States and it would have been broader in its data collection and usage terms.

The issue of consent is not reduced only to whether it is asked for, but instead in the way it is asked. Under the BDSG, companies must ask for express consent and typically that consent must be in writing.[127] In Apple's case, the German District Court stated that Apple needed to make its consent requests specific and ask for users' explicit consent in order to collect their data.[128] A high consent requirement is necessary in the United States because people assume that all privacy policies provide the same baseline of privacy, but this is not the case.[129] Studies have shown that privacy policies come in "all different flavors."[130] Additionally, people most often do not read the privacy policy on every data-collecting website or device they use. With a higher and more detailed consent requirement, people will be more aware of what data is being taken from them and how it is being used. Furthermore, data collectors will be required to provide a higher level of protection.

---

[124] *Id.*
[125] *Id.*
[126] *Id.*
[127] Zell, *supra* note 11, at 465–66.
[128] *Id.* at 482–83.
[129] *See* Antonialli, *supra* note 17, at 346–47.
[130] *Id.* at 346

III. THE IMPORTANCE OF OVERSIGHT IN THE ENFORCEMENT OF PERSONAL DATA PROTECTION LAW

A. DATA PROTECTION AND OVERSIGHT IN GERMANY AND THE EUROPEAN UNION

Under Europe's Data Protection Directive each Member State is required to "set up an independent supervisory authority to monitor state protection compliance in that state."[131] Although all EU Member States are required to have an independent authority to supervise compliance with the respective state's data protection laws, Germany is still the best example to look at for two reasons.

First, despite having one of the strongest data protection frameworks in the world, the independent authority can only exercise its authority over data collection companies that are headquartered in Germany or have substantial ties to Germany.[132] However, the EU has recently passed a new Data Protection Regulation, which attempts to make the data protection laws of Europe more uniform.[133] The regulation entered into force on May 24, 2016, but member states are given a two-year transition period to meet its requirements.[134] The regulation will supersede member state law if the regulation interferes with member state law; this includes German data protection laws.[135] Since member states will spend the next two years implementing the regulation into their national laws, it is not possible to predict how Germany will implement the provisions of the regulation with its national code, but since Germany's data protection laws are the strongest in the world the regulation will likely mirror Germany's data protection framework.[136]

Second, while EU law is being updated, it is still useful to use German law as a comparison tool because Germany is the largest member of the European Union and holds the most seats in the European

---

[131] Council Directive 95/46, art. 28.1, 1995 O.J. (L 281) 31, 34 (EC).

[132] Zell, *supra* note 11, at 462.

[133] *See* Council Regulation 2016/679, 2016 O.J. (L191) 1 (EU).

[134] Francoise Gilbert, *EU General Data Protection: What Impact for Businesses Establish Outside the European Union*, J. INTERNET L., May 2016, at 3, 3.

[135] Zell, *supra* note 11, at 462–63.

[136] *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (*General Data Protection Regulation*), COM (2012) 11 final (Jan. 25 2012) art. 91.

Parliament.[137] Additionally, "Germany contains the single biggest market in the European Union, as well as influence over other European data protection agencies and EU policy decisions."[138] For this reason, it is reasonable to believe that the European Union has adopted policies similar to the BDSG and will mirror several of the structures created in Germany's data protection framework. For example, under the Directive, the EU allowed for implied consent where Germany required express consent.[139] The new data regulation has eliminated implied consent and requires consent to be given "freely, specific, informed, and unambiguous."[140] Thus, although the data protection laws of Europe will be changing over the next two years, the German model provides the direction the rest of Europe is likely to take.

Under the German model of data protection enforcement, the power to supervise the data collection process is split between many authorities.[141] The first split is between the public and private sector. In the public sector, supervisory power is given to Data Protection Commissioners.[142] There are two types of commissioners: a federal data commissioner for the federal government and many state data commissioners for each state of Germany.[143] These authorities are only responsible for public data collectors, operate outside of the BDSG, and operate under Germany's Federal Freedom of Information Act.[144] These authorities have limited enforcement power but do have a substantial influence on policy and practice.[145]

---

[137] *Commerce in the EU by population (2016)*, WORLDOMETERS, http://www.worldometers.info/population/countries-in-the-eu-by-population/ (last visited Dec. 19, 2016).

[138] Schinasi, *supra* note 20, at 594.

[139] *Compare* Council Directive 95/46 *supra* note 130, art. 8.2, at 40–41*with* Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, Bundesgesetzblatt, [BGBL] at § 4(a)(1) (Ger.).

[140] Gilbert, *supra* note 134, at 6.

[141] *Commission Comparative Study on Different Approaches to New Privacy Challenges, in Particular in the Light of Technological Developments: Final Report*, at 48, COM (2008) 011 final (May 2010), http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A4_germany.pdf [hereinafter *Data Protection Study*].

[142] *Id.*

[143] *Id.*

[144] *Data protection in Germany: overview*, PRACTICAL LAW, http://us.practicallaw.com/3-502-4080#a189243 (last visited Dec. 19, 2016).

[145] *Data Protection Study*, *supra* note 141, at 52.

The private sector does operate under the BDSG, and the government does have substantial enforcement powers in this sector.[146] Under the BDSG, "every company that processes data [must] employ a data protection official to monitor the company's data processing to ensure proper privacy considerations are met."[147] The in-house "official reports directly to the CEO of the company, must be allowed to carry out his or her function free of interference, may not be penalized for his or her actions, and can only be fired in exceptional circumstances," such as lacking the proper technical knowledge to perform the job.[148] In addition to being given extensive security to supervise the company, the in-house official is also given extensive authority to enforce data protection laws.

Since the "main task of the in-house official is to ensure compliance with the law," he or she is given significant access to a company's process information.[149] The in-house official has the right to demand, without cause, "any information which the supervisory authority needs for the fulfillment of its task."[150] The data collector is required to respond to any requests for information "without delay" and in most cases the data collector has no right to object to such inquires.[151] The request for information extends to: demanding access to any business premises and offices, carrying out inspection in the office during office hours, inspecting business documents, inspecting personal data files and computers, accessing business mail, and accessing private homes, files, and computers if a warrant is requested.[152]

If the supervisory authority were to find a violation of the federal data protection law, the supervising authority is empowered to make its own changes to ensure that a minimum level of security and confidentiality is being practiced.[153] However, if the company is not violating these aspects of the law, the supervisory authority still has several options to enforce compliance with the law.[154] A few options available would be: report the controller to prosecuting authorities, inform data subjects of the data controller's illegitimate process, or

---

[146] *Id.* at 48.
[147] Schinasi, *supra* note 20, at 594–95.
[148] *Data Protection Study*, *supra* note 141, at 49.
[149] *Id.* at 54.
[150] *Id.* at 52.
[151] *Id.* at 52–53.
[152] *Id.*
[153] *Id.* at 53.
[154] *Id.*

report the violation to the office of fair trading.[155] The sanctions for violating the BDSG vary greatly from case to case, but authorities are allowed to impose an unlimited fine and up to two years imprisonment depending on the severity of the violation.[156]

Lastly, when the new European Data Protection Regulation goes into effect, the German process will not change significantly. Under the Data Protection Regulation, the EU has aimed to create a "one-stop-shop" for data processing companies.[157] Essentially, the Member State in which the company does most of its business will be in charge of enforcing the Data Protection Laws of the affected state.[158] The lead authority may make binding decisions, but it must work with supervising authorities in other member states and it is expected to "take 'utmost account' of the suggestions made by the other supervisory authorities."[159]

B. DATA PROTECTION AND OVERSIGHT IN THE UNITED STATES

By contrast, under the US sectoral approach, there is no single enforcement authority for data processing companies.[160] The primary agencies relied on for personal data protection enforcement are the Federal Trade Commission and the Department of Commerce.[161] However, the FTC has limited its own power in regulating online privacy stating that it "lacks authority to require firms to adopt information practice policies or to abide by the fair information practice principle on their Web sites, or portions of the Web sites, not directed to children."[162] The Department of Commerce focuses even less on personal data protection than the Federal Trade Commission does.[163] Instead, the American personal data protection framework is a patchwork of, "legislation, administrative oversight, and, predominantly, self-regulation."[164]

---

[155] *Id.*

[156] *Id.* at 54.

[157] *See* Gilbert, *supra* note 134, at 4–5.

[158] *Id.* at 5.

[159] *Id.*

[160] Schinasi, *supra* note 20, at 579.

[161] *Id.*

[162] Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305, 1324 (2001).

[163] Schinasi, *supra* note 20, at 583.

[164] *Id.* at 581.

The concept of self-regulation for personal data protection has been the predominant method of protecting personal data and is based on the idea that the "market itself, and a need to maintain consumer trust, would compel corporations to promulgate sufficient safeguards to internet users' personal data."[165] However, the lack of a central authority to enforce personal data protection laws has promoted a "weak approach to privacy all in favor of business interests."[166] Although there are data protection laws in the United States, the punishment for violating those laws is typically civil penalties, and those affected are usually at a disadvantage to bring suit against a company, if they are allowed to bring suit at all.[167]

Since there is little chance of penalty for misusing or inadequately protecting personal data, breaches of data collecting companies are frequent in the United States. In 2012, Forbes magazine titled its summer 2012 issue "The Summer of the Data Breach."[168] In 2014, a breach of Home Depot resulted in the loss of "'56 million credit cards accounts, 53 million email addresses' and an estimated 63 million dollars in damage."[169] Additionally, the loss associated with data breaches is not always financial; it can be personal as well, as many learned from the Ashley Madison breach of 2015, "shaming not only the subscribers to Ashley Madison's service, but also innocent bystanders such as their family members."[170]

If a breach or other violation of personal data protection laws does occur, the victim of the company is unlikely to recover damages or penalize the company's behavior.[171] Victims of data breaches are entitled to some common law and statutory regulation; however, these remedies are significantly curtailed by a lack of strong regulation and enforcement on behalf of the federal government.[172] First, some breaches of online privacy are covered under tort law; if a person lives in an "economic loss doctrine" jurisdiction, they cannot make a claim without personal or

---

[165] *Id.* at 585.

[166] Shara Monteleone, *Addressing the 'Failure' of Informed Consent in Online Data Protection: Learning the Lessons from Behavior-Aware Regulation*, 43 SYRACAUSE J. INT'L L. & COM. 69, 79 (2015).

[167] Sotto & Simpson, *supra* note 9, at 208.

[168] *See* Lewis, *supra* note 22.

[169] Hilary G. Buttrick, Jason Davidson, & Richard J. McGowan, *The Skeleton of a Data Breach: The Ethical and Legal Concerns*, 23 RICH. J.L. & TECH. 2, ¶ 1 (Dec. 2016).

[170] *Id.*

[171] *Id.* ¶ 13.

[172] Sotto & Simpson, *supra* note 9, at 213.

physical property damage, which is rare in online privacy breaches.[173] Second, victims are unable to prove that they have standing because an online privacy injury may be seen as speculative or hypothetical and not real.[174] Finally, the plaintiff will have difficulty establishing that the defendant caused the plaintiff's injuries because the personal information may have been compromised in a separate breach.[175]

Lastly, the self-regulation model is flawed because consumers are at a distinct disadvantage to corporations. Corporations are not required to be transparent about their privacy agreements under US law and this has led to the market becoming uninformed.[176] Additionally, most users are unable to protect themselves from privacy violations because the privacy terms have been given to them through "long and convoluted privacy policies."[177] This method has led to a practice of companies convincing consumers of "an appearance of privacy rather than a reality."[178] As a result, the "lax regulatory framework in the United States has allowed corporations in America to gather more information about domestic consumers than anywhere else in the world."[179]

By adopting a uniform central authority like Germany has done, the United States can level the playing field between corporations and their consumers. Central oversight would eliminate the belief that companies follow their private policy claims and turn it into a reality. Companies would be subject to harsher penalties for negligent breaches or misuse of personal data. Consumers would be in a better position to sue companies for breaches of their personal data, and the regulations would allow consumer to properly self-regulate the free market. Finally, a central authority would increase transparency of corporations' data collection processes, uses, and breaches.

IV. THE IMPORTANCE OF INCREASING REMEDIES FOR PERSONAL DATA PROTECTION VIOLATIONS

Germany is in the fortunate position to have its personal data protection laws rooted in both international and national constitutional

---

[173] Buttrick, Davidson, & McGowan, *supra* note 169, ¶ 20.
[174] *Id.* ¶ 21.
[175] *Id.* ¶ 22.
[176] Schinasi, *supra* note 20, at 585.
[177] *Id.*
[178] Monteleone, *supra* note 166, at 79.
[179] Schinasi, *supra* note 20, at 587.

law. The right to privacy in Germany extends to actions against both public and private data-collecting actors. The right to privacy of personal data protection is included in the Charter stating that "[e]veryone has the right to the protection of personal data concerning him or her."[180] Germany is also covered by the Personal Data Directive, which is to be replaced by the even stronger Personal Data Regulation in May 2018.[181] Additionally, like the US Constitution, the German constitution does not include a general right to privacy; instead, the right is found by cobbling together several rights under the German Constitution.[182] However, unlike the United States, Germany has enacted numerous data protection laws that have resulted in a comprehensive framework of data protection for its citizens including the BDSG and TMG.[183] The result of this extensive coverage in Germany is a universal understanding of what personal data is and how it should be handled.

The United States does not have a constitutional right to the protection of personal data. While the United States does have a general right to privacy by cobbling together several other rights, this general right applies with respect to the government and not to private entities.[184] Additionally, the United States has the Fourth Amendment, which provides additional privacy rights, but this amendment only applies to government actions.[185] As stated in the previous section, the United States does have some regulations and enforcement of personal data protection; however, the majority of the enforcement is self-regulating.[186] The patchwork of protection does not regulate all types of data equally between statutes, states, or sectors.[187] The regulations are not even uniform in determining the definition of personal data.[188] Based on the disunity of data protection laws in the United States, it is not surprising that the remedies available to citizens for violations of their privacy rights by data collectors is also sectoral and inadequate. The best

---

[180] Charter, *supra* note 13, art. 8(1).

[181] Gilbert, *supra* note 134, at 3.

[182] Nicole Jacoby, *Redefining the Right to be let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States*, 35 GA. J. INT'L & COMP. L. 433, 453 (2007).

[183] Zell, *supra* note 11, at 464–72.

[184] Jacoby, *supra* note 182, at 436.

[185] U.S. CONST. amend. IV.

[186] Schinasi, *supra* note 20, at 581.

[187] McKay Cunningham, *Complying with International Data Protection Law*, 84 U. CIN. L. REV. 421, 423–24 (2016).

[188] *Id.* at 424.

examples of this are the remedies available to consumers under tort, contract, and property law.[189]

While citizens may have the ability to bring a few claims against personal data collectors through state or federal laws, the majority of claims must be brought under the common law of torts, contracts, or property.[190] However, each of these areas is deficient for one of several possible reasons: people do not know that their data has been breached until it is too late, it is too difficult to show that there has been an individualized harm, or any claim is swallowed by the third party exception to the Fourth Amendment.[191]

A. INSUFFICIENCY OF TORT LAW REMEDY

Tort law has been suggested as a way to protect people's informational privacy; however, the tort regime falls short of protection for several reasons.[192] "[C]ourts have long rejected assertions that torts such as intrusion upon seclusion, public disclosure of embarrassing facts, and appropriation of name and likeness ought to be extended to the consumer information privacy context."[193] The main goal of privacy torts is to protect individuals from reputational harm and not to encourage a sense of autonomy or prevent loss or misuse of personal data.[194] Due to this unfortunate distinction tort law is often inadequate to give people relief when their personal data is misused.[195]

Most often, tort law fails because people voluntarily give up their information rather than having it taken from them.[196] For much of people's personal data is already made available to the public and will not be protected by tort law. While phonebooks are a bit outdated, they do provide an excellent example of a document that contained a person's name, address, and phone number. Information that is contained in similar format, but made available to anyone who wishes to view it,

---

[189] Balaban, *supra* note 6, at 18.
[190] *Id.* at 18.
[191] *Id.* at 18–19; Kline, *supra* note 25, at 462–65.
[192] Balaban, *supra* note 6, at 22.
[193] *Id.*
[194] *Id.*
[195] *Id.*
[196] Kline, *supra* note 25, at 462–63.

would be unprotected by tort law.[197] This could be analogized to information that people put on their Facebook, Instagram, Snapchat, or other social medium. If the information is made available to the public it cannot be protected by tort law. It is unlikely that many people will have a problem with tort law being inadequate for such information. Many people put personal data onto social media for the exact purpose of garnishing attention; if that personal data ends up adversely affecting the poster, it can only be blamed on the poster's poor judgment. More controversial, however, is tort law's inability to protect consumers from misuse of their data by companies.

When information is voluntarily given to a third party that third party "enjoy[s] an almost unfettered right to access, use, and distribute public record information."[198] This lack of protection under tort law could be referred to as the third-party gap.[199] For example, in *Dwyer v. American Express Co.*, an Illinois appellate court allowed American Express to use its customer data to create lifestyle profiles and target customer lists for use by third parties because the data was collected from American Express credit cards, which the cardholders used voluntarily.[200] While the idea that simply using a credit card gives companies the right to collect and distribute buying practices to third parties may make people uncomfortable, the plaintiffs in *Dwyer* at least had the benefit of knowing what information had been shared with third parties.[201]

The implications for a lack of appropriate remedies in tort law can be much more severe than simply giving third parties the buying habits of their customers. In 2005, three major data breaches occurred due to inadequate data security measures being taken by LexisNexis and Choicepoint.[202] In the case of LexisNexis, the company announced that criminals had accessed the personal information of 310,000 people on fifty-nine separate occasions.[203] The data stolen in this instance included:

---

[197] *See* Cox Broad. Corp. v. Cohn, 420 U.S. 469, 498–99 (1975) (finding that information that was in a public record was not protected by tort law).

[198] Kline, *supra* note 25, at 463–64 (citing Busse v. Motorola, Inc., 813 N.E.2d 1013, 1015 (Ill. App. 2004) (finding that when a company gave private information for a research study and that study was published, the private information became public and lost all protections under tort law)).

[199] Kline *supra* note 25, at 474.

[200] Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1353–54 (Ill. App. Ct. 1995).

[201] *Id.*

[202] Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV 140, 140 (2006).

[203] *Id.* at 155.

names, addresses, driver's license numbers, and social security numbers.[204] In the case of ChoicePoint, the company was tricked into selling individuals' personal data to fake companies that had been set up to steal people's names, addresses, social security numbers, and credit card reports.[205] ChoicePoint lost more than 163,000 people's personal information and refused to tell its consumers what data it had sold to the identity thieves.[206] While attempts were made to provide tort remedies to the affected consumers, there were few legislative successes.[207] For a consumer who has been harmed by a company's insufficient personal data protection, there are still very few options to exact a remedy under tort law.

B. INSUFFICIENCY OF CONTRACT LAW REMEDY

Contract law has also been used for some privacy claims. However, contracts claims often fail for two reasons: 1) contracts do not carry a default contractual right to privacy; and 2) there is an imbalance of power between businesses and individuals.[208] First, having meaningful privacy protections through contract would require an "implied-contract-of-confidentiality default rule," which would likely prove as difficult to implement as comprehensive data protection.[209] Second, individuals typically lack negotiating power when using an online service since use of the service constitutes acceptance to the contract.[210] Additionally, federal law contains many loopholes that give businesses more control than data subjects over personal data once the data has been collected.[211] For example, the plaintiffs in one particular case also tried to make a claim under a theory of contract law but were denied because the Federal Telecommunications Act allowed the company to disclose information to protect its own interests, provide information to other carriers upon reasonable request, and permit access to organizations conducting research on the health effects of wireless phone use.[212]

---

[204] *Id.*
[205] *Id.* at 154–55.
[206] *Id.* at 155.
[207] *Id.* at 155–56.
[208] *See* Balaban, *supra* note 6, at 23–24.
[209] *Id.* at 22–23.
[210] *Id.* at 24.
[211] Kline *supra* note 25, at 464.
[212] *Id.* (citing Busse v. Motorola, Inc., 813 N.E.2d 1013, 1016 (Ill. App. 2004)).

C. INSUFFICIENCY OF PROPERTY LAW REMEDY

Lastly, data subjects may make claims for a violation of their privacy rights under property law. However, claimants typically have limited success in this area because they must convince the court that personal data is property, and that they have ownership of that data.[213] Claims under property law typically fail when data collectors trade the data to a third party.[214] Additionally, claimants may face cross-claims by the data collector claiming that the personal data is not the data subject's property.[215] In order to have a property right in personal data, the court or legislature would need to create a reliable system to show when a person's personal data is being collected, and where the personal data goes once it is collected.[216] This would be problematic for at least two reasons. First, the theory of a claim under property law assumes that the data subjects are aware that their data is being collected in the first place, which often they are not.[217] Second, if a person has a property right in his or her personal data, then a system must be created to make that property alienable.[218] Personal data lacks many of the attributes that real property items have, such as cars or land.[219] The main problem in viewing personal data as real property is alienability.[220] A key characteristic of property is the ability of the buyer of the property to give those property rights away to a third party.[221] However, this does not transfer easily to personal data because data collectors would receive data from potentially millions of data subjects. If each data subject created a different set of property rights to sell to the data collector, the data collector would find it too difficult to manage the millions of individual accounts.[222] Additionally, while there may be a privacy element to current property regimes, most are created primarily for an economic purpose and not for a privacy purpose.[223]

---

[213] *Id.* at 464–65.
[214] *Id.* at 465.
[215] *Id.*
[216] Balaban, *supra* note 6, at 21.
[217] *See id.* at 21–22.
[218] Pamela Samuelson, *Privacy as Intellectual Property*, 52 STAN. L. REV. 1125, 1137–38 (2000).
[219] *Id.* at 1138.
[220] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2090–91 (2004).
[221] *Id.* at 2090.
[222] *See id.* at 2091.
[223] Samuleson, *supra* note 218, at 1138.

The United States should implement a comprehensive federal law to supersede common law claims when data subjects' personal data is misused or negligently breached. A statutory proposal would be superior to the common law because the common law was created before the digital technologies we have today existed. Without leveling the playing field in litigation, data collectors have no incentive to improve their data protection systems nor vet third parties to whom they may transfer extensive amounts of personal data information.

V. CONCLUSION

Germany has created extensive personal data protection laws that go beyond the comprehensive personal data protection laws enforced in the European Union. Contrary to this, the United States lags far behind the two entities. The United States must increase the personal data protection given to its citizens' and consumers' personal data information in order to maintain online security. With the current system, there is little oversight of what third parties can do with a person's personal data. People in the United States are rarely aware when their personal data is being collected and are equally unaware of where their personal data is being sent once it has been collected. In order to fix the problems created by a lack of personal data protection, the United States should look to the German model and adopt components of their comprehensive personal data protection laws. Three of these reforms should include: asking for written consent from data subjects in order to make them aware that their data is being collected, creating an oversight body to ensure greater compliance with data protection law to reduce the chance for data breaches, and replacing the common law avenues for suing data collectors with substantive data privacy laws that will provide data subjects with adequate remedies to breaches of their data. The United States must increase its acceptable standard for personal data protection to ensure online security for its citizens.