PRE-PAID PAYMENT CARDS IN A POST-*SCHREMS* WORLD: A CASE STUDY ON THE EFFECTS OF THE PRIVACY SHIELD PRINCIPLES

KATHERINE E. RUIZ DÍAZ*

INTRODUCTION

On October 2015, the Court of Justice of the European Union (CJEU or the Court) in *Schrems v. Data Commissioner*[1] completely changed how U.S. companies do business in the European Union (E.U.). The star of this case was Maximillian Schrems, a lawyer, Austrian citizen, and — more importantly — a Facebook user circa 2008. As is the case with other subscribers residing in the E.U., some or all the data provided by Schrems to Facebook was transferred from Facebook's Irish subsidiary to servers located in the United States, where it was processed. In light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the U.S. National Security Agency or N.S.A.), Schrems presented a complaint before the Irish Data Protection Commissioner, arguing that the law and practice of the United States did not offer sufficient protection against surveillance by the public authorities of the data transferred to that country.[2] The Data Commissioner rejected the complaint, on grounds that in the so-called *Safe*

* Katherine E. Ruiz Díaz, Esq. is a practicing attorney in private practice, working on Commercial and Securities Law. She received her B.A. from Boston University in 2014, and her J.D. from the University of Puerto Rico School of Law in 2017. This article was originally written for a seminar on International Business Transactions at the University of Puerto Rico School of Law, under the supervision of Prof. Luis A. Aviles, to whom she gives her thanks for his guidance.

[1] C-362/14, Schrems v. Data Protection Commissioner, 2015 E.C.R. 650 [hereinafter, *Schrems*].

[2] *Id.* ¶ 28.

Harbor Decision,[3] the Commission considered that under the *safe harbour scheme* the United States ensured an adequate level of protection of the personal data transferred.[4]

Economic relations between the E.U. and the United States predate the European Economic Community, and their governmental institutions constantly encourage trade through bilateral trade agreements and government incentives.[5] As technology progressed and inevitably made its way into transnational and international business, customer data as an exchangeable commodity quickly emerged as key in the development of the industry. These developments brought implications on fundamental rights protected by the E.U. & U.S. laws, namely, the rights to privacy. This, along with the parallel experimental rise of modern terrorism and cybercrimes, it became imminent that such market should be regulated.

When elaborating its decision in the *Schrems* case, the CJEU stated that no provision of the Directive[6] prevents oversight by the national supervisory authorities of transfers of personal data to third countries which have been the subject of a Commission decision; the Court alone has jurisdiction to determine the validity of a directive. The Court added that legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to privacy. Thus, the Court declared the *Safe Harbor Decision* — and consequently, the Safe Harbor Privacy Principles — invalid.

The *Schrems* decision was praised by many as a milestone towards data protection reform and the human right to privacy. But human rights are not the only area of law that *Schrems* has directly affected. Data protection is an issue that goes beyond the arena of human rights, and spills over into, for example, the scope of international and transactional law. This decision has also had very specific consequences for many industries. The CJEU's ruling in *Schrems* seriously complicated operations for U.S. companies that had relied on Safe Harbor Privacy Principles to do business. Compliance with Safe Harbor Principles was relatively easy, and provided a way for U.S. companies to transfer personal data between the United States and the E.U.[7] By finding the Safe Harbor Principles inadequate to protect the privacy of E.U. citizens, the Court's decision stripped U.S. companies from the ability to transfer E.U. citizens' personal data among E.U. Member States and the United States for commercial purposes. One

---

[3] Commission Decision 2000/520, 2000 O.J. (L 215).
[4] *Id.* ¶ 29.
[5] *See, e.g.*, European Commission, *Countries and regions: United States*, (last updated Apr. 29, 2016) (http://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/ (last visited Jun. 16, 2018); United States Mission to the European Union, *Doing Business in the European Union*, https://useu.usmission.gov/doing-business-local.html (last visited Jun. 16, 2018).
[6] Council Directive 95/46/EC, 1995 O.J. (L 281).
[7] *See* Sharon G. Lin, *A new, "safer" harbor for personal data transfer?*, N.C. J. INT'L L. (March 10, 2016 11:47 AM), http://blogs.law.unc.edu/ncilj/2016/03/10/a-new-safer-harbor-for-personal-data-transfer/ (last visited on Jun. 1, 2018).

industry that was particularly affected was that of pre-paid financial instruments and payment cards. Having gained prominence for its anonymous card products and for presenting an alternative to traditional banking for the unbanked and underbanked, the pre-paid payment card industry presents an interesting case study of the effects of this new legislation. Until recently, pre-paid cards and online wallets constituted a laxly regulated and poorly-understood area of law. By its nature, the pre-paid payment card industry is one that is relegated to the grey areas of domestic and international regulation. Decisions like *Schrems*, along with a general push for stronger anti money laundering (A.M.L.) measures and greater transparency are now inviting higher scrutiny.

The *Schrems* ruling shows how interconnected the E.U. and U.S. markets have become throughout the years. The purpose of this paper is to study the effects of the *Schrems* case and the new E.U.-U.S. Privacy Shield Framework on the pre-paid card business. This paper will also analyze how the government policy changes derived from *Schrems* impact transnational and international commercial transactions in today's globalized world. Part II of this paper will particularly focus on the *Schrems* case and the E.U.-U.S. Privacy Shield Framework. Part III will expand on the pre-paid card industry, along with regulations that E.U. and U.S. businesses — dedicated to the payment system industry — must now comply with. Part IV will further focus on the implications of the implementation of Privacy Shield within the pre-paid payment card industry. Finally, Part V will comment on how such changes influence the dynamic between institutions and consumers, including corporations' responsibility regarding criminal activity performed by their own consumers.

I. *SCHREMS* AND THE E.U.-U.S. PRIVACY SHIELD FRAMEWORK

Designed around 1998 and 2000, the Safe Harbor Privacy Principles were implemented by both the United States and the E.U. Under this so-called *safe harbor scheme*, U.S. companies complying with the principles and certifying that they met the E.U. requirements could transfer data from the E.U. to the United States. The resulting *Safe Harbor Decision*, which will be discussed below, was one of the main issues the Court attacked in *Schrems*.

A. E.U.-U.S. Safe Harbor Privacy Principles and the Safe Harbor Decision

In the 1980s, the Organization for Economic Cooperation and Development (OECD) issued its Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data (the OECD Guidelines),[8] with the purpose of creating a

[8] ORG. FOR ECON. COOPERATION & DEV., GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980) http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (These guidelines were updated in 2013) (last visited Jun. 16, 2018).

comprehensive data protection system throughout Europe. The OECD Guidelines established seven principles for protection of personal data: (1) data subjects should be given notice when their data was being collected; (2) data should only be used for the intended purpose and not for any other purposes outside of those the data was originally required for; (3) data should not be disclosed without the data subject's consent; (4) data should be kept secure from any potential abuses; (5) data subjects should be informed as to who is collecting their data (disclosure); (6) data subjects should be allowed to access their data and make corrections to any inaccurate data; and (7) data subjects should have a method available to them to hold data collectors accountable for not following the above principles.[9] However, the OECD Guidelines were nonbinding, and data privacy and security legislation still varied across Europe.[10]

After experimenting with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data,[11] the European Commission realized that bifurcating data protection legislation amongst E.U. Member States hindered the free transfer of data within the E.U., and thus proposed the Data Protection Directive in 1995.[12] All seven principles of the OECD Guidelines were incorporated into this Directive.[13] The Data Protection Directive established that the transfer of personal data to a third country may, in principle, take place only if that third country ensures an adequate level of protection of the data.[14] The Directive also established the European Commission could find that a third country ensured an adequate level of protection due to its domestic law or its international commitments.[15] Finally, the Directive required each Member State to designate one or more public authorities responsible for monitoring the application within its territory of the national provisions adopted based on the Directive (also known as national supervisory authorities).[16] Articles 25 and 26 of the Data Protection Directive set forth the legal framework for transfers of personal data from the E.U. to third countries outside the European Economic Area (E.E.A.).[17]

---

[9] GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, *supra* note 8.

[10] Anna E. Shimanek, *Do you Want Milk with those Cookies?: Complying with Safe Harbor Privacy Principles*. 26 IOWA J. CORP. L. 455, 462–63 (2001).

[11] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108 (1981); Shimanek, *supra* note 9 (This Convention's signatories were obligated to enact domestic legislation concerning the automatic processing of personal data, which many Member States duly did. The Convention for the Protection of Individuals regarding Automatic Processing of Personal Data was signed and ratified by all E.U. Member States, and Mauritius, Senegal and Uruguay have acceded to it.).

[12] Council Directive 95/46, 1995 O.J. (L 281) 38, 31 (EC).

[13] *Id.*

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] Council Directive 95/46, art. 25-26, 1995 O.J. (L 281), 38, 45–46 (EC).

During the 1990s, and under the Data Protection Directive, European countries developed comprehensive rules governing the collection and processing of personal information, overseen by independent regulatory agencies called "data protection authorities." This approach to privacy was elevated to a fundamental constitutional right when the E.U. adopted its Charter of Fundamental Rights in 2009.[18] In contrast, as some have put it, the United States "lacks [to this day] a comprehensive approach to privacy, relying instead on an idiosyncratic patchwork of specific — and, in some cases, dated — rules governing sectors as diverse as health care and video rentals."[19] This presents a problem for the United States, given that European regulations have long prohibited the transfer of data to countries that the E.U. considers to have weak privacy protections, among them the United States.[20] Meanwhile, while the United States endorsed the OECD Guidelines, there was much inaction on the government's part to implement said recommendations.[21]

The E.U.-U.S. Safe Harbor Privacy Principles were designed to prevent private organizations within the E.U. and the United States that store customer data, from accidentally disclosing or misplacing personal information. Under the safe harbor scheme, U.S. companies could opt into a voluntary program and be certified if they adhered to the seven principles and fifteen frequently asked questions and answers per the Directive. The seven principles are: (1) notice; (2) choice; (3) onward transfer; (4) security; (5) data integrity; (6) access; and (7) enforcement.[22]

The first principle — notice — establishes that individuals must be informed that their data is being collected and how it will be used; that is, the

---

[18] *See* Charter of Fundamental Rights, Commission Regulation 326/2, 2012, 2012, O.J. (391) 02.

[19] Henry Farrell & Abraham Newman, *The Transatlantic Data War: Europe Fights Back Against the NSA*, FOREIGN AFFAIRS (Jan./Feb. 2016), https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war.

[20] *Id.*

[21] Shimanek, *supra* note 8. *See also* Thomas A. Hemphill, *Electronic Commerce and Consumer Privacy: Establishing Online Trust in the U.S. Digital Economy*, 107 BUS. & SOC. REV. 221, 222–23 (2002). Almost at the end of the 1990s, then U.S. President Bill Clinton announced his administration's policy on the "commercialization of the Internet." The administration report included a set of "Privacy Principles" developed back in 1995 by the Privacy Working Group of the U.S. Information Infrastructure Task Force. Building on the OECD Guidelines, and incorporating "fair information practice principles," these recommended privacy principles identified three principles to govern the collection, processing, storage, and re-use of personal data: (1) information privacy; (2) information integrity; and (3) information quality. Accordingly, these privacy principles recommended that online businesses gathering data should inform consumers of: (1) what information they are collecting and how they intend to use such data; (2) whether or not personal information is collected from children; (3) the consequences of providing or withholding information; (4) what steps will be taken to protect the information; (5) a meaningful way to limit use and re-use of personal information and; (6) any rights of redress for harmful or improper disclosure of personal information or if decisions are based on inaccurate, outdated, incomplete, or irrelevant personal information.

[22] EUROPEAN COMMISSION, PRIVACY SHIELD ADEQUACY DECISION, *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf.

organization must provide information about how individuals can contact the organization with any inquiries or complaints. With the second principle — choice — individuals must have the option to opt out of the collection and forward transfer of the data to third parties. The third principle establishes transfers of data to third parties may only occur to other organizations that follow adequate data protection principles. The fourth principle requires reasonable efforts be made to prevent loss of collected information. Regarding data integrity, this principle establishes that data must be relevant and reliable for the purpose it was collected. The Safe Harbor Principles also establish that individuals must be able to have access to their information (or information on them), including access to correct or delete it, in cases where this information may be inaccurate. Finally, the seventh and last principle establishes that there must be effective means of enforcing these rules, which usually translates into domestic legislation.[23]

Since the 2000s and the adoption of the Safe Harbour Scheme, the legal and factual frameworks have been substantially altered,[24] particularly in the E.U. For instance, Article 8 of the E.U. Charter of Fundamental Rights states that everyone has the right to the protection of personal data concerning themselves.[25] The right to protection of data contributed to the exponential evolution of the information and communications technology (I.C.T.) sector, providing products that gather, transfer and process personal data.[26] Despite seemingly providing a solution for data security in commercial activity, the Safe Harbor Principles did not exist without their problems, and the program seemed to be lacking the strength needed to enforce it, since its inception. For example, in 2002, the antecessor of the European Commission, the Commission of the European Communities, issued a report on the application of the Safe Harbor Decision, and the Data Protection Directive found that "a substantial number of organizations that have self-certified adherence to the Safe Harbour do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies" and that "not all dispute resolution mechanisms have indicated publicly their intention to enforce Safe Harbour rules and not all have in place privacy practices applicable to themselves."[27]

---

[23] PRIVACY SHIELD ADEQUACY DECISION, *supra* note 22.

[24] Alessandro El Khoury, *Case Notes: The Safe Harbour is not a Legitimate Tool Anymore. What Lies in the Future of EU-USA Data Transfers?*, 6 EUR. J. RISK. REG. 659, 659 (2015).

[25] *See Charter of Fundamental Rights*, *supra* note 18.

[26] *Id.*

[27] Commission of the European Communities, *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce* 2, 4–5, (2002), http://web.archive.org/web/20060724174359/http://www.ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf.

Moreover, in 2004, the European Commission again expressed unease with self-certified organizations that had not published a privacy policy or had published a policy that is not compliant with the Safe Harbor Principles. The Commission understood this as a problem, "not only because under the Safe Harbour having a publicly available privacy policy is mandatory, but also, because the absence of a privacy policy or of one fully consistent with the Principles means that the [U.S. Federal Trade Commission] ha[d] no jurisdiction to enforce the missing Principles upon the organizations that failed to publish them."[28]

While the European Commission seemed to maintain an optimistic view of U.S. businesses patently lacking compliance with the Safe Harbor Principles, others were less naïve. For instance, in 2008, the Australian consulting company Galexia issued a blistering review, concluding that "[t]he ability of the U.S. to protect privacy through self-regulation, backed by claimed regulator[y] oversight [was] questionable."[29] In its review, Galexia recommended the E.U. renegotiate the Safe Harbor arrangement, provide warnings to E.U. consumers, and consider to comprehensively review all list entries,[30] while at the same time recommending the United States, inter alia, to investigate the hundreds of organizations making false claims and to revise their statements about the number of participants.[31]

In light of criticisms of this nature, the Commission Decision 2000/520,[32] known as the Safe Harbor Decision, was released by the European Commission in

---

[28] COMMISSION OF THE EUROPEAN COMMUNITIES, *The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce* 13, http://web.archive.org/web/20060724173657/http://www.ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf.

[29] Chris Connolly, *The US Safe Harbor-Fact or Fiction?* 18, (2008), http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (emphasis added). Galaxia documented basic claims as incorrect, where only 1109 out of 1597 recorded organizations listed by the U.S. Department of Commerce on 2008 remained in the database after doubles, triples and 'not current' organizations were removed. Only 348 organizations met even the most basic requirements for compliance. Of these, only 54 extended their Safe Harbor membership to all data categories (manual, offline, online, human resources). Other 206 organizations falsely claimed to be members for years, yet there was no indication that they were subject of any U.S. enforcement. Connolly also criticized the Department of Commerce's *Safe Harbor Certification Mark* offered to companies to use as a "visual manifestation of the organization when it self-certifies that it will comply" as misleading, because it does not carry the words "self-certify" on it. Only 900 organizations provided a link to their privacy policies, for 421 it was unavailable. Numerous policies were only one to three sentences long, containing "virtually no information." Many entries appeared to confuse privacy compliance with security compliance and showed a "lack of understanding about the Safe Harbor program." The companies' listing of their dispute resolution providers was confusing, and problems regarding independence and affordability were noted. Many organizations did not spell out that they would cooperate with or explain to their customers that they could choose the dispute resolution panel established by the E.U. Data Protection Authorities.

[30] *Id.*

[31] *Id.*

[32] Commission Decision 2000/520, 2000 O.J. (L 215) 43, 7 (EC).

response to requests for clarification of U.S. law with respect to damages claims for breaches of privacy, "explicit authorizations" in U.S. law for the use of personal information in a manner inconsistent with the Safe Harbor Principles, and the effect of mergers and takeovers on obligations undertaken pursuant to the Safe Harbor Principles. The European Commission, inter alia, declared that the United States was in fact complying with the Safe Harbor Principles, thus solidifying the validity of the safe harbor scheme that was being practiced at the time.

It was not until 2013 that the issue on privacy principles was brought again to the European Commission's attention. On November 27th, 2013, the Commission adopted the communication to the European Parliament and the Council entitled Rebuilding Trust in E.U.-U.S. Data Flows.[33] This communication was accompanied by the Report on the Findings by the E.U. Co-chairs of the ad hoc E.U.-U.S. Working Group on Data Protection,[34] which contained, among other things, a detailed analysis of U.S. laws authorizing the existence of surveillance programs and the collection and processing of personal data by United States authorities.[35] The Commission stated that "[c]ommercial exchanges are addressed by Decision [2000/520]," adding that the Safe Harbor Decision provided a legal basis for transfers of personal data from the E.U. to companies established in the United States which have adhered to the Safe Harbor Privacy Principles. Moreover, the European Commission observed that concerns about the level of protection of personal data of E.U. citizens transferred to the United States under the safe harbor scheme had grown, but that "[t]he voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement." However, the Commission noted a number of weaknesses in the application of Decision 2000/520, like noncompliance of certain U.S. certified businesses with the Safe Harbor Principles, and that improvements had to be made to that decision regarding "structural shortcomings related to transparency and enforcement, the substantive Safe Harbor Principles and the operation of the national security exception."[36] It also observed that Safe Harbor acted as a conduit for the transfer of the personal data of citizens from the E.U. to the United States by companies required to surrender data to U.S. intelligence agencies under the U.S. intelligence collection programs.[37]

Nevertheless, the European Commission concluded that, in light of the weaknesses identified and despite the fact that the current implementation of Safe Harbor could not be maintained, its revocation would have adversely

---

[33] *Rebuilding Trust in EU-US Data Flows*, COM (2013) 846 final (Nov. 27, 2013).

[34] This report was drawn up, in cooperation with the United States after the existence in that country of a number of surveillance programs involving the large-scale collection and processing of personal data had been revealed.

[35] *Schrems*, at ¶11.

[36] *Rebuilding Trust in EU-US Data Flows*, *supra* note 33.

[37] *Id.*

affected the interests of member companies in the E.U. and in the United States.[38] Little was the Commission aware that around the same time, Schrems was filing his complaint before the Data Protection Commissioner of Ireland for lack of protection of his personal data and of the data of many E.U. citizens like him, whose data was being handled by U.S. companies that were not strictly complying with Safe Harbor Principles of data protection, hindering their fundamental rights in the process. The Court in Schrems interpreted the Safe Harbor Decision as placing "national security, public interest, or law enforcement requirements" of, in this case, the United States, above Safe Harbor Principles. This basically permitted self-certified U.S. organizations receiving personal data from the E.U. to disregard those principles "without limitation where they conflict with those requirements and therefore prove incompatible with them."[39] Thus, the Safe Harbor Decision, and consequently the U.S. safe harbor scheme at the time, "enable[d] interference, founded on national security and public interest requirements or on domestic legislation of the United States, with the fundamental rights of the persons whose personal data is or could be transferred from the [E.U.] to the United States."[40] Moreover, as the Advocate General so poignantly observed, "the United States rules on the protection of privacy may be applied differently to United States citizens and to foreign citizens."[41]

B. Post *Schrems* and the New E.U.-U.S. Privacy Shield Framework

At the foundation of any regulatory framework to ensure consumer online privacy and confidentiality are the "fair information practice principles," which include, (1) "notice/awareness," (2) "choice/consent," (3) "access/participation," (4) "integrity/security," and (5) "enforcement/redress."[42] Soon after *Schrems*, the European Commission and the U.S. government started talks about a new framework, and on February 2nd, 2016 they reached an agreement.[43] On July 8th 2016, E.U. Member States representatives approved the final version of the E.U.-

[38] *Rebuilding Trust in EU-US Data Flows*, *supra* note 33.
[39] *Schrems*, at ¶ 86.
[40] *Schrems*, at ¶ 87.
[41] C-362/14, Schrems v. Data Protection Commissioner, Advocate General Opinion, ¶ 213. For a discussion on the principle of proportionality in light of Arts. 7, 8, and 52(1) of the Charter, refer to ¶¶ 214–215. *See also* Alessandro El Khoury, *Case Notes: The Safe Harbour is not a Legitimate Tool Anymore. What Lies in the Future of EU-USA Data Transfers?*, 6 EUR. J. RISK. REG. 659, 660 (2015).
[42] Thomas A. Hemphill, *Electronic Commerce and Consumer Privacy: Establishing Online Trust in the U.S. Digital Economy*, 107 BUS. & SOC. REV. 221, 222–23 (2002); F.T.C., "Privacy Online: A Report to Congress," Section III. Fair Information Practice Principles (June 1998).
[43] Press Release, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, (Feb. 2, 2016) http://europa.eu/rapid/press-release_IP-16-216_en.htm (last visited Jun. 16, 2018).

U.S. Privacy Shield.[44] The European Commission adopted the framework on July 12th, 2016 and it went into effect the same day.[45]

This new framework protects the fundamental rights of anyone in the E.U. whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers. The new arrangement includes: (1) strong data protection obligations on companies receiving personal data from the E.U. safeguards on U.S. government access to data; (2) effective protection and redress for individuals; (3) annual joint review to monitor the implementation. "The new arrangement lives up to the requirements of the European Court of Justice."[46]

To transfer personal data from the E.U. to the U.S., different tools are available such as contractual clauses, binding corporate rules and the Privacy Shield. If the Privacy Shield is used, U.S. companies must first sign up to the framework, subscribed to the U.S. Department of Commerce.[47]

> The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles." . . . In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles. They must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use personal data from the E.U. under that framework.[48]

While Privacy Shield offers major improvements compared to the Safe Harbor Privacy Principles, concerns still remain relating to deletion of data, collection of massive amounts of data, and need for clarification on the new Ombudsperson mechanism.[49] The new Privacy Shield Principles continue to encompass all seven principles of the old safe harbor scheme: (1) notice; (2) choice; (3) accountability for onward transfer; (4) security; (5) data integrity and

---

[44] Press Release, *Statement by Vice-President Ansip and Commissioner Jourová on the Occasion of the Adoption by Member States of the EU-U.S. Privacy Shield*, http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm.

[45] European Commission Decision, C(2016) 4176, http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.

[46] *The EU-U.S. Privacy Shield*, EUROPEAN COMMISSION, http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605819.

[47] This Department is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments.

[48] EUROPEAN COMMISSION, DIRECTORATE-GENERAL FOR JUSTICE AND CONSUMERS, GUIDE TO THE EU-U.S. PRIVACY SHIELD (2016).

[49] *See* Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion recommendation /files/2016/wp238_en.pdf. The European Data Protection Supervisor issued an opinion on 30 May 2016 in which he stated that "the Privacy Shield, as is stands, is not robust enough to withstand future legal scrutiny before the [European] Court." Press Release, *Privacy Shield: More Robust and Sustainable Solution Needed*, https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite /shared/Documents/EDPS/PressNews/Press/2016/EDPS-2016-11-PrivacyShield_EN.pdf.

purpose limitation; (6) access; and (7) recourse, enforcement, and liability, plus additional supplementary principles.[50]

Along with creating a new data protection framework between the E.U. and the United States, the *Schrems* decision also brought reform within the E.U. On April 27th, 2016, the European Commission adopted the General Data Protection Regulation.[51] With the purpose of replacing the long-lasting but weakened Data Protection Directive, this Regulation's purpose is to strengthen and unify data protection across the E.U.[52]

II. THE REGULATED WORLD OF THE PRE-PAID PAYMENT CARD

Payment cards are the result of an economic system that has been developing for centuries.[53] The modern payment card issued by major banks took flight after the second half of the twentieth century, particularly in the 1960s, after an unsuccessful launch in the 1950s due to lack of solvent clients and credit card fraud.[54] The United States was the pioneer in the payment card market, and continues to lead the market today in its number of non-cash transactions, per statistics of 2013-2014.[55] On the other hand, in Europe credit cards were originally introduced to render service to U.S. citizens during their trips to Europe.[56] Thus, a market for payment cards was created among luxury-goods sellers and other European establishments that quickly became acquainted with American cards with the purpose of increasing sales.[57] An issue that does not present problems in the United States — beyond those that fall into interstate commerce domain — is the European Community's goal to cooperate and maintain reciprocity between the different Member States to facilitate business

---

[50] International Trade Administration, PRIVACY SHIELD FRAMEWORK: OVERVIEW, https://www.privacyshield.gov/article?id=OVERVIEW (last visited Jun. 16, 2018).

[51] General Data Protection Regulation, Council Regulation 2016/679, 2016 O.J. (L 119) 59, 1 (EU).

[52] Regulations, unlike directives, can be adopted by means of a variety of legislative procedures depending on their subject matter. Directives, on the other hand, need to be transposed into national law. Consolidated Version of the Treaty of the Functioning of the European Union, art. 288, May 9, 2008, 2008 O.J. (C 115) 47 [hereinafter TFEU].

[53] JOSÉ CARLOS CARBONEL PINTANEL, LA PROTECCIÓN DEL CONSUMIDOR TITULAR DE TARJETAS DE PAGO EN LA COMUNIDAD EUROPEA 28 (1994). As Carbonel Pintanel points out, the correct term is *payment cards* rather than *credit cards* or *debit cards*. Both debit cards and credit cards are part of the larger group of payment cards. Credit cards are those that offer a line of credit without having to liquidate the entire balance due by a certain date, charging an interest over said balance due (also known as credit instruments). Debit cards, on the other hand, are those linked to a bank account, and payments done with said card are deducted from the user's bank account, either automatically or by a pre-established date. Nevertheless, under common law, the term *credit card* is used indistinctly to refer to any type of card. *See id.* at 28 n.1.

[54] *Id.* at 29–30.

[55] *Transaction Volumes: Top Ten Markets*, https://www.worldpaymentsreport.com/Top-10-Non-Cash-Payments-Markets.

[56] CARBONEL PINTANEL, *supra* note 53, at 37.

[57] *Id.*

transactions between European users.[58] Thus, this *interoperability* involves interconnectivity, compatibility, and standardization of the payment instruments used.[59]

Pre-paid payment cards, or stored-value cards,[60] are a comparatively new yet growing sector of the payment card industry, due to the accessibility benefits to their consumers. In the United States, "the use of pre-paid cards has exploded in the past several years, especially in the retail industry."[61] The use of pre-paid payment cards in the retail industry is very limited, and pales in comparison with its contemporary use in Europe. Pre-paid payment cards have emerged in recent years into the mainstream of the U.S. financial system. As consumers embrace the convenience and security of being able to transact many daily commercial activities electronically, more and more areas of U.S. commerce explore ways to reap the advantages of electronic payment delivery. Yet this accelerated growth might not necessarily be due to the same reason its European counterpart has been as successful.

Despite the uses given in different markets, what remains clear is that the payment card industry, stored-value cards included, depends on the storage and exchange of customer data for its day-to-day operations to run properly. As we will see below, both the United States and Europe regulate the handling and usage of customer data.

A. K.Y.B./K.Y.C. Regulations in the United States: Moving Towards Transparency

The objective of K.Y.B./K.Y.C. regulations is to prevent banks from being used, intentionally or unintentionally, by criminals for money laundering activities or terrorist financing. Related procedures also enable banks and other financial institutions to better understand their customers and their financial dealings, helping them manage their risks prudently. Banks usually frame their K.Y.C. policies incorporating the following four key elements: (1) customer policy; (2) customer identification procedures; (3) monitoring of transactions; and (4) risk management. The approaches to K.Y.B./K.Y.C. regulations vary between the United States and the different Member States within the European Union. As this paper will later discuss, both systems vary in that the United States takes a stronger stance in the security of their citizens, while the European

---

[58] CARBONEL PINTANEL, *supra* note 53, at 38.
[59] *Id.*
[60] Stored-value cards can be defined as a payment card with a monetary value stored on the card itself, not in an external account maintained by a financial institution. They include a wide variety of financial products, including gift cards, phone cards, teen cards, government benefit cards, travel cards, flexible spending account cards, subway system cards, employee incentive cards and payroll cards. Christopher B. Woods, *Stored Value Cards*, 77 OKLAHOMA BAR J. 2253, 2253 (2006).
[61] Phillip W. Bohl et al., *Prepaid Cards and State Unclaimed Property Laws*, 27 FRANCHISE L.J. 23, 23 (2008); *see generally* J. CHENIE & S. RHINE, PREPAID CARDS: AN IMPORTANT INNOVATION IN FINANCIAL SERVICES (2006).

Union, under fundamental human rights arguments, focuses on their citizens' right to privacy.

Pre-paid payment cards, like any other new payment method, were subject to abuse back when regulators, legislators, and payment providers were beginning to not only understand the system, but to also observe the different ways criminal activity could manifest in this field.[62] Nonetheless, the fact that pre-paid cards are subject to abuse and criminal activity should not come as a surprise due to their nature — at least in the early days of the industry. Various characteristics provided — and still provide — fodder for its abuse: (1) its high degree of anonymity; (2) the participation of additional nonbank and unregulated parties in the process; and (3) its ease of acquisition and *reloadability*.[63] However, once the industry and government agencies came to better understand these risks, regulation over this particular payment method began.

After the September 11 attacks, the U.S. Congress rushed to pass legislation to strengthen security controls. Thus, the USA PATRIOT Act was signed into law.[64] This act touches various areas of national security, ranging from border security and public surveillance to anti-money laundering measures related to terrorism. Pursuant to Title III of the USA PATRIOT Act,[65] the Secretary of the Treasury was required, *inter alia*,[66] to finalize regulations before October 26th, 2002 making the implementation of K.Y.C. guidelines mandatory for all U.S. banks.[67] The related processes are required to conform to a customer identification program (CIP). A CIP is a requirement in the United States, where financial institutions need to verify the identity of individuals wishing to conduct financial transactions with them. Moreover, section 326 of the USA PATRIOT

---

[62] Stanley J. Sienkiewicz, *Prepaid Cards: Vulnerable to Money Laundering?*, FEDERAL RESERVE BANK OF PHILADELPHIA PAYMENT CARDS CENTER DISCUSSION PAPER, at 20 (2007), https://www.philadelphiafed.org/-/media/consumer-finance-institute/payment-cards-center/publications/discussion-papers/2007/d2007febprepaidcardsandmoneylaundering.pdf?la=en

[63] *Id.*

[64] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstructing Terrorism Act of 2011, Pub. Law 107-56, 115 Stat. 272 (2006) [hereinafter, USA PATRIOT Act].

[65] *Id.* (Codified as amended in scattered sections of 31 U.S.C.).

[66] 31 U.S.C. § 5318A (Under Section 311 of the USA PATRIOT Act, the U.S. Treasury Department can classify a foreign financial institution as a "primary money laundering concern.").

[67] 31 U.S.C. §§ 311, 314. Section 311 requires the maintenance of records of the aggregate amount of all transactions that are made outside the United States in areas where money-laundering has been identified as a concern. It also requires that reasonable steps be undertaken by a financial institution to obtain and retain information on foreigners who gain a benefit of ownership of an account which is opened and maintained in the United States, and yet who do not own the account itself (also known as beneficial ownership). Section 311 also requires that the financial institution identify any foreign customers who are authorized to use or route transactions through a payable-through account in the United States. Section 314 adds regulations that attempt to foster cooperative efforts to deter money laundering. This was mainly done by ordering the U.S. Treasury and other agencies to create regulations that set out how information was to be shared, and by allowing financial institutions to share information with other financial institutions when so allowed by the Secretary of Treasury.

ACT requires financial institutions to implement "reasonable procedures" for "verifying the identity" of accountholders.[68] Thus, this requirement compels all U.S. financial institutions to develop a CIP appropriate to its size and type of business.[69] The CIP must be incorporated into the bank's AML compliance program, which is subject to approval by the financial institution's board of directors.[70]

The CIP is intended to enable banks to form a reasonable belief of the identity of each customer.[71] As financial institutions, pre-paid payment card issuers that operate in the United States must also comply with CIP requirements. The program must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer. Furthermore, this requirement compels financial institutions to conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider: (1) the types of accounts offered; (2) the methods of opening accounts; (3) the types of identifying information available; and (4) the institution's size, location, and customer base.[72] It is also important to point out that under Title III of the USA PATRIOT ACT, "[t]he Secretary of the Treasury may require *any domestic financial institution or domestic financial agency* to maintain records, file reports, or both, concerning the aggregate amount of transactions, or concerning each transaction, *with respect to a jurisdiction outside of the United States*,"[73] including one or more financial institutions operating outside of the United States, one or more classes of transactions within, or involving, a jurisdiction outside of the United States, or one or more types of accounts "if the Secretary finds any such jurisdiction, institution, class of transactions, or type of account to be of primary money laundering concern."[74]

B. K.Y.C. and Payment Services Regulation in the European Union

In the E.U., various pieces of Union-wide legislation govern and regulate the usage of payment services. There are varying levels of K.Y.C. requirements depending on the product and its level of risk/load limits.[75] The two main types of e-money products available are those that require Simplified Due Diligence

---

[68] USA PATRIOT Act § 326, Pub. L No. 107–56, § 326, 115 Stat. 272, 317 (2011).
[69] 31 C.F.R. § 103.21 (2010) [hereinafter, Final CIP Rule].
[70] *See* Priscilla M. Reagan, *Old issues, new context: Privacy, information collection, and homeland security*, 21 GOVERNMENT INFORMATION QUARTERLY 481 (2004).
[71] *See generally*, Michael F. McEneney et al., *Customer Identification Requirements Under the USA PATRIOT Act*, 59 THE BUSINESS LAWYER 1287 (2004).
[72] *Id.*
[73] 31 U.S.C. § 5318A(b)(1)(A) (emphasis added).
[74] *Id.*
[75] David Parker, *Viewpoint: Terrorist Financing and Prepaid Cards: Ban Them!*, PATTECH (Jan. 19, 2016), https://www.bankingtech.com/2016/01/viewpoint-terrorist-financing-and-prepaid-cards-ban-them/ (last visited Jun. 16, 2017).

(SDD) and Standard Due Diligence. A third requires Enhanced Due Diligence for high-risk products and people. SDD is simply capturing at purchase, the name and address of the individual; they are checked against sanctions lists, but the details are not verified against official documents or databases. The cards typically are only sent to a cardholder's home address, thus, ensuring multiple cards cannot be applied for by the same person. There are also gift card products where no details are taken at purchase. However, if they are later registered by the users, e.g., for online use or reloads, the users are checked against sanctions lists.

Control of electronic payment services in the E.U. had a very similar genesis to the USA PATRIOT ACT. To prevent terrorist funding, measures aimed at the freezing of funds and economic resources of suspected individuals and entities was taken in the form of E.U. legislation, including Regulation 2580/2001[76] and Regulation 881/2002.[77] To that same end, measures aimed at protecting the financial system against the channelling of funds and economic resources for terrorist purposes have been taken. Directive 2005/60 contains several measures aimed at combating the misuse of the financial system for money laundering and terrorist financing. However, the European Commission understood that these measures did not fully prevent terrorists and other criminals from having access to payment systems to move their funds.

The Regulation 1781/2006[78] attempts to strengthen governmental action against money laundering and terrorism funding. It recognizes the full traceability of transfers of funds as a "particularly important and valuable tool in the prevention, investigation and detection of money laundering or terrorist financing.[79] To ensure the transmission of information on the payer throughout the payment chain, the European Commission deemed it appropriate to provide for a system imposing the obligation on payment service providers to have transfers of funds accompanied by accurate and meaningful information on the payer.[80] Regulation 1781/2006 also takes on anonymous transfers as a "potential terrorist financing threat."[81] The Regulation was thus designed to enable the payment service provider of the payee to avoid or correct such situations when it becomes aware that information on the payer is missing or incomplete. In this regard, the European Commission understood that flexibility in these transactions should be allowed, as it concerns the extent of information on the payer on a risk-sensitive basis. In addition, the accuracy and completeness of information on the payer remained the responsibility of the payment service provider.[82] Where the payer's payment service provider is situated outside the territory of the European Community, enhanced customer due diligence should

[76] Council Regulation 2580/200, 2001 O.J. (L 344) 3 (EC).
[77] Council Regulation 881/2002, 2002 O.J. (L 139) 4 (EC).
[78] Council Regulation 1781/2006, 2006 O.J. (L 345) (EC).
[79] *Id.* ¶ 6.
[80] *Id.*
[81] *Id.* ¶ 16.
[82] *Id.*

be applied — in accordance with Directive 2005/60 — in respect of cross-border correspondent banking relationships with that payment service provider.[83]

As payment systems continued to evolve at a rapid pace, the European Union attempted to catch up to the new technologies emerging in the industry. The Directive 2009/110, better known as the E-Money Directive,[84] was the result of this attempt. The E-Money Directive aims to enable new, innovative and secure electronic money services to be designed, to provide market access to new companies, and to foster real and effective competition between all E.U. market participants. The Directive focuses on modernizing E.U. rules on electronic money, especially bringing the prudential regime for electronic money institutions, into line with the requirements for payment institutions in the Payment Services Directive. The E-Money Directive continues to hold many of the main principles that electronic money/payment legislation holds, compelling electronic money institutions to "inform the competent authorities in advance of any material change in measures taken for safeguarding of funds that have been received in exchange for electronic money issued."[85]

Finally, payment card systems across the E.U. are regulated by the Directive 2015/2366, better known as the revised Directive on Payment Services or PSD2. The original Directive on Payment Services (PSD)[86] provided the legal foundation for the creation of an E.U.-wide single market for payments. PSD aimed at establishing a modern and comprehensive set of rules applicable to all payment services in the European Union. The target is to make cross-border payments "as easy, efficient and secure as national payments within a Member State."[87] It also sought to improve competition by opening payment markets to new entrants, thus fostering greater efficiency and cost-reduction. At the same time the Directive provides the necessary legal platform for the Single Euro Payments Area (SEPA). SEPA is where more than 500 million citizens, over twenty million businesses and European public authorities can make and receive payments in euro under the same basic conditions, rights and obligations, regardless of their location.

The PSD2 revises PSD in many ways. Relevant to this paper, PSD2 expanded the reach of the original PSD, including transactions where at least one party is located within E.U. borders (also known as *one leg out* transactions).[88] PSD2 also compels banks to open their markets to external parties. It holds that "[i]n order to stimulate the competition that can be provided by such closed payment systems to established mainstream payment systems, it would not be appropriate to grant third parties access to those closed proprietary payment

---

[83] Council Regulation 1781/2006, *supra* note 78.
[84] Council Directive 2009/110, 2009 O.J. (L267) 7 (EC). (The E-Money Directive entered into force in all EU countries on 30 April 2011).
[85] *Id.* art. 3(2).
[86] Council Directive 2007/64, 2007 O.J. (L 319) 1 (EC).
[87] European Commission, *Directive on Payment Services (PSD)*, http://ec.europa.eu/finance/payments/framework/index_en.htm (last visited Jun. 16, 2018).
[88] Council Directive, 2015/2366, art. 82(1)(c), 2015 O.J. (L 337) 58 (EU).

systems." These Third-Party Players (TPP) are divided in two types: (1) Account Information Service Providers (AISPs), and (2) Payment Initiation Service Providers (PISPs). AISPs are providers that can connect to bank accounts and retrieve information from them. PISPs are players that can initiate payment transactions. This is a radical change in this industry, as currently there are not many payment options that can take money from one's account and send them elsewhere.[89]

Along with Regulation 2015/751,[90] PSD2 complements a general revised E.U. legal framework on payment services. This Regulation, in turn, introduces rules on the charging of interchange fees for card-based transactions and aims to further accelerate the achievement of an effective integrated market for card-based payments.[91]

The European Commission makes clear that PSD2 respects the fundamental rights and observes the principles recognized by the Charter of Fundamental Rights of the E.U., including the right to respect for private and family life, the right to protection of personal data, the freedom to conduct a business, the right to an effective remedy and the right to not be tried or punished twice in criminal proceedings for the same offence. The European Commission also points out that PSD2 must be implemented in accordance with those rights and principles.[92]

This Directive also introduces a neutral definition of acquiring of payment transactions in order to capture not only the traditional acquiring models structured around the use of payment cards, but also different business models, including those where more than one acquirer is involved. This should ensure that merchants receive the same protection, regardless of the payment instrument used, where the activity is the same as the acquiring of card transactions. Technical services provided to payment service providers, such as the mere processing and storage of data or the operation of terminals, should not be considered to constitute acquiring. Moreover, some acquiring models do not provide for an actual transfer of funds by the acquirer to the payee because the parties may agree upon other forms of settlement.[93]

III. PRE-PAID CARDS AND PRIVACY SHIELD: CHANGING THE INDUSTRY

The pre-paid payment card industry, like others in the payment card and other financial industries, has been affected by the *Schrems* decision and all its consequences discussed here. The payment card industry depends on a complex chain of interconnected parts for its proper functioning, and the free exchange of data between each of the individual parts in the chain is crucial. To understand

---

[89] Alessandro Longoni, *PSD2 - What changes?* FINEXTRA (May 30, 2016), https://www.finextra.com/blogposting/12668/psd2---what-changes.
[90] Council Regulation, 2015/751, 2015 O.J. (L 123) 58, 1 (EU).
[91] Council Directive, 2015/2366, at ¶ 2.
[92] *Id.* at ¶ 66.
[93] *Id.* at ¶ 10.

how it affects this industry, one must first understand the basic workings of its everyday transactions. Most payment card transactions involve four participants: (1) a purchaser; (2) an issuer — bank or other financial institution; (3) a merchant; and (4) an acquirer.[94] Although the purchaser, issuer, merchant, and acquirer are the nominal parties to the transaction, the network under which the card has been issued — *i.e.* Visa, MasterCard — is also involved.[95] The networks, which are associations of member institutions that issue branded cards, provide information and transaction-processing services with respect to the transaction between the acquirer and the issuer.[96] With this in mind, while payment card issuers may be located and/or incorporated physically in a particular country, *i.e.* an E.U. Member State, their database servers and data processors may be located in another part of the world — namely the United States. The transfer of data across borders between the E.U. and the United States falls within the scope of the Privacy Shield Principles.

Unlike other financial institutions, however, the pre-paid payment card's tumultuous beginnings and questionable practices — many of which still linger today — are directly at odds not only with national regulations for security purposes, but also at crossed purposes with the Privacy Shield Principles. Considering all the regulation of the pre-paid card system, both in the United States and the E.U., the industry is being affected in different ways. This occurs primarily because pre-paid products used to be anonymous, which has always been one of the biggest draws of the industry's products.

While regulation has been occurring since the conception of the USA PATRIOT ACT and Regulation 1781/2006, the whole industry is being pushed towards newer, stricter standards of K.Y.B./K.Y.C. regulations. For instance, during the summer of 2016, the European Commission proposed stricter rules on the use of virtual currencies and prepaid cards in an attempt to reduce anonymous payments and curb the financing of terrorism. Virtual currency exchange platforms must increase checks on the identities of people exchanging virtual currencies, such as Bitcoin, for real currencies and report suspicious transactions. Under the Commission's proposals the threshold for making anonymous payments with pre-paid cards was lowered to 150 euros ($167.28) from 250 euros. Frans Timmermans, the European Commission's First Vice-President, stated that "Member States will be able to get and share vital information about who really owns companies or trusts, who is dealing in online currencies, and who is using pre-paid cards."[97]

Along with the creation of the Privacy Shield Framework and the *Schrems* decision, other events have plagued the years 2015 and 2016. Following terrorist attacks in Paris on November 2015, the E.U. Executive announced it would step

---

[94] RONALD J. MANN, CHARGING AHEAD: THE GROWTH AND REGULATION OF PAYMENT CARD MARKETS 20–21 (2006).
[95] *Id.*
[96] *Id.*
[97] Foo Yun Chee, *EU proposes stricter rules on Bitcoin, prepaid cards in terrorism fight*, http://www.reuters.com/article/us-eu-security-financing-idUSKCN0ZL1RH.

up measures to cut off terrorists' access to funds. This came to be due to statements by the French authorities, where they announced that they had acquired proof that pre-paid cards had been used by the Paris attackers. This did not just affect the pre-paid card industry. The European Commission also proposed increasing the amount of checks banks must carry out on financial flows from risky third countries, namely states with poor AML rules and difficulties countering terrorism financing.[98]

Amid tighter K.Y.B./K.Y.C. regulations, the adage of stricter data transfer regulations places another constraint — and burden — on the pre-paid card industry. Although the CJEU has no jurisdiction over the N.S.A., it does have jurisdiction over the European operations of American firms,[99] and vice versa. In order to be able to exchange data across borders between the United States and the E.U., these companies must be subscribed to the Privacy Shield Framework. If they are not listed as certified under Privacy Shield, which is voluntary, or they do not comply with the Principles, which is compulsory, E.U. customer data cannot be stored in the United States. A large portion of this data includes K.Y.C. data that must be kept for national security purposes and governmental reach of the data. This leaves many U.S. companies that are currently storing E.U. information domestically in the lurch. Due to how recent the *Schrems* case was decided, these U.S. businesses currently exist in a legal gray area, where it is almost impossible to move this data oversees to the E.U. at this point. After all, unlike judicial decisions, company restructuring does not happen overnight. As regulations on data protection in both the United States and the E.U. continue to emerge, compliance with the Privacy Principles could imply a cease of operations due to inability to transfer data without breaching international obligations, and even possibly incurring in internationally wrongful acts.

CONCLUSION: WAS CHANGE LONG OVER DUE?

One could say that as the pre-paid card industry expands, and its consumer population grows, the more regulated it becomes. Nonetheless, the pre-paid payment card system is usually mostly popular among the underbanked and the unbanked. Yet global trends, particularly in the United States and the E.U., show that the underbanked and unbanked population are in a minority, with surveys showing that only 7% of Americans are unbanked and 19.9% of American households are underbanked.[100] Recent studies also show that 7% of all E.U. consumers — *i.e.* thirty million Europeans above eighteen years old — do not

[98] Foo Yun Chee, *supra* note 97.
[99] Henry Farrell & Abraham Newman, *The Transatlantic Data War: Europe Fights Back Against the NSA*, FOREIGN AFFAIRS (2016), https://www.foreignaffairs.com/articles/united-states/2015-12-14/transatlantic-data-war.
[100] FEDERAL DEPOSIT INSURANCE CORPORATION, FDIC NATIONAL SURVEY OF UNBANKED AND UNDERBANKED HOUSEHOLDS (2015), https://www.fdic.gov/householdsurvey/2015/2015report.pdf.

have a bank account.[101] As the pre-paid payment card industry attempts to become more legitimized in the eyes of the average consumer, and become a global player outside of the unbanked/underbanked — as well as less legitimate — markets, it must comply with new and emerging policies of data protection and information disclosure.

Another fact to consider is that the Safe Harbor Privacy Principles and the rest of the legal framework that the pre-paid payment card industry depends on were put in place twenty years ago. This brings up the question of whether this system is still suitable for modern international data transfers. For instance, the contractual allocation of roles (*i.e.* controller and processor) previously held under the *safe harbor scheme* did not seem to be an effective solution, considering that the allocation of those roles is a substantial one, neither seems valid the same contractual approach to the informed consent. As an author points out regarding the old safety scheme, "there [was] an issue of intelligibility of the information given for the [principle of] consent: new systems are complex and in constant change, thus making a static description hard."[102]

While U.S. business are overwhelmed by the recent changes in data security and regulation, Europe observers were not as surprised. This trend towards E.U. restriction on data and protectionism over citizen privacy had been happening since the *Google v. Agencia Española de Protección de Datos* decision[103]. In this case, the CJEU challenged the very business model of U.S. e-commerce firms, which used vast pools of personal data to sell ads and model consumer behavior.[104] The ruling made this increasingly difficult in the all-important European market, and caused, *inter alia,* that non-U.S. cloud computing firms have cancelled ten percent of their contracts with U.S. firms over privacy concerns.[105] In that case, many suggested that the United States should introduce new binding rules to protect the privacy of both U.S. and European consumers and make real concessions on the national intelligence surveillance of its allies.[106] For example, some had suggested introducing national data breach legislation, increasing the authority of the Privacy and Civil Liberties Oversight Board to include the private sector, and expanding the jurisdiction of the Privacy Act to cover non-citizens.[107] Maybe if the United States had headed some of that advice, the current situation might have come around organically, or been avoided altogether.

---

[101] COMMISSION STAFF WORKING PAPER, COMMISSION RECOMMENDATION ON ACCESS TO A BASIC PAYMENT ACCOUNT, http://ec.europa.eu/finance/finservices-retail/docs/inclusion/sec_2011_907_en.pdf.

[102] El Khoury, *supra* note 24, at 664.

[103] C-131/12, Google v. Agencia Española de Protección Datos, 2014 E.C.R 317.

[104] *Id.*

[105] Henry Farrell & Abraham Newman, *Forget Me Not: What the EU's New Internet Privacy Ruling Means for the United States*, FOREIGN AFFAIRS, May 19, 2014, https://www.foreignaffairs.com/articles/united-states/2014-05-19/forget-me-not.

[106] *Id.*

[107] *Id.*

Equally so, the E.U. should recognize that overly sweeping privacy regulations would hurt free expression as well as U.S. business interests. The Internet rights conversation is no longer a monologue but an argument between competing visions of privacy in a digital age.[108] But, as Henry Farrell and Abraham Newman have observed, "the United States has also undercut its friends." For example, in the service of counterterrorism it forced a Belgium-based financial-processing entity to provide a trove of information on worldwide electronic fund transfers, systematically breaking E.U. privacy law.[109] "[W]hen the United States breaks the rules itself in ways that undermine the basic constitutional guidelines of other countries, it should expect a backlash."[110] The more the United States seeks to exploit the system it has created, the more foreign states and businesses will challenge it.[111] A more integrated world economy benefits U.S. companies, allowing them to find new markets and build complex international supply chains that lower their costs. At the same time, the explosion of cross-border exchange has increased the importance of the U.S. dollar and the U.S. market as foreign firms seek access to American banks and consumers to raise money and sell goods.[112]

Interdependence has already begun to work against the United States rather than for it.[113] As U.S. businesses have entered international markets, they have become more vulnerable to other countries' rules and more anxious about domestic policies and actions that may irritate other governments. This is an especially big problem for technology companies, whose insatiable hunger for detailed personal information indirectly feeds the U.S. surveillance state. As recently as 2018, Congressional testimony by a U.S. tech giant, Mark Zuckerberg, has shown the vulnerabilities of this flawed system. Since foreign countries cannot directly indict the N.S.A., they tend to turn to the targets whose behavior they can affect — U.S. businesses — to force the U.S. government to change its rules.

---

[108] Farrell & Newman, *supra* note 105.
[109] Farrell & Newman, *supra* note 99.
[110] *Id.*
[111] *Id.*
[112] *Id.*
[113] *Id.*