Pace International Law Review

Volume 31
Issue 1 *Winter 2018*

Article 5

December 2018

Cashless Societies and the Rise of the Independent Cryptocurrencies: How Governments Can Use Privacy Laws to Compete with Independent Cryptocurrencies

Matla Garcia Chavolla
Elisabeth Haub School of Law at Pace University

CASHLESS SOCIETIES AND THE RISE OF THE INDEPENDENT CRYPTOCURRENCIES: HOW GOVERNMENTS CAN USE PRIVACY LAWS TO COMPETE WITH INDEPENDENT CRYPTOCURRENCIES

COMMENT

Matla Garcia Chavolla*

ABSTRACT

Many individuals (including governments) envision living in a future world where physical currency is a thing of the past. Many countries have made great strides in their efforts to go cashless. At the same time, there is increasing awareness among citizens of the decreasing amount of privacy in their lives. The potential hazards cashless societies pose to financial privacy may incentivize citizens to hold some of their money in independent cryptocurrencies. This article argues that in order for governments in cashless societies to keep firm control over their money supply, they should enact stronger privacy law protections for its citizens in order to decrease the real or perceived loss of (financial) privacy. This paper compares the privacy laws that exist today in both the United States and the European Union and suggests combining elements of both legal systems in order create a more privacy-friendly legal framework that can enable governments to complete against independent cryptocurrencies.

---

* Matla Garcia Chavolla is a student at Elisabeth Haub School of Law. I am grateful to Professor John T. Bandler for his review of this work and valuable feedback. Any errors are mine.

TABLE OF CONTENTS

I. INTRODUCTION: A BRAVE NEW WORLD

It seems only fitting that the first country to invent paper would also be the first to use paper currency as well.[1] There is evidence that China used paper money as early as the T'ang dynasty (618—907 CE).[2] About fourteen hundred years later, paper currency is still in use today—although in some countries increasingly less so.[3] Although cash remains the highest used payment method in the United States (32% of all transactions in 2015), purchases made with debit and credit cards account for 48% of transactions made in 2015.[4]. In contrast, cash transactions account for only 2% of all payments made in Sweden in 2015.[5] On November 8, 2016, Indian Prime Minister Narendra Modi officially declared that 86% of the cash in circulation in India to "no longer be legal tender."[6] For a country that is about 90% cash reliant, this posed significant problems, but it is one example of how some governments are deeply committed to going cashless.[7]

---

[1] JACK WEATHERFORD, THE HISTORY OF MONEY 126 (1997).

[2] *Id.*; *see Tang dynasty*, ENCYCLOPAEDIA BRITANNICA, https://www.britannica.com/topic/Tang-dynasty (last visited Dec. 21, 2018).

[3] *See* Jeremy Gaunt, *Cashless society getting closer, survey finds*, REUTERS, Apr. 25, 2017, 8:09 PM, https://www.reuters.com/article/us-global-economy-cash/cashless-society-getting-closer-survey-finds-idUSKBN17S001.

[4] Patrick Gillespie, *Cash is still king for Americans*, CNN MONEY (Nov. 4, 2016, 2:32 PM), http://money.cnn.com/2016/11/04/news/economy/cash-is-king-san-francisco-fed/index.html.

[5] Jon Henley, *Sweden leads the race to become cashless society*, THE GUARDIAN (June 4, 2016, 11:00 AM), https://www.theguardian.com/business/2016/jun/04/sweden-cashless-society-cards-phone-apps-leading-europe.

[6] Murali Krishnan, *One year after demonetization – Has India eliminated 'black money'?*, DW (Nov. 8, 2017), http://www.dw.com/en/one-year-after-demonetization-has-india-eliminated-black-money/a-41276486 (quoting Indian Prime Minister Modi's television address); *see* Bhaskar Chakravorti, *Early Lessons from India's Demonetization Experiment*, HARV. BUS. REV. (Mar. 14, 2017), https://hbr.org/2017/03/early-lessons-from-indias-demonetization-experiment.

[7] Chakravorti, *supra* note 6; Zeenat Saberin, *Desperate Measures*, VICE NEWS (Dec. 1, 2016), https://news.vice.com/story/india-discontinued-86-percent-of-its-circulated-currency-and-the-poor-are-in-crisis.

At the same time, a new revolution in technology is steadily becoming more mainstream: cryptocurrencies. Bitcoin, the first cryptocurrency, was created in 2009[8] and since then a myriad of other cryptocurrencies have been launched in bitcoin's wake.[9] Cryptocurrencies are different than traditional government regulated currencies because governments do not issue them or control them.[10] This lack of government oversight might become increasingly attractive to citizens living in a cashless society where their every financial transaction could conceivably be susceptible to recording and monitoring by government agents. Privacy in a cashless society might become increasingly valuable to citizens—especially given the emphasis being placed on privacy in today's virtual world.[11] This paper will discuss the possible competitive role of cryptocurrencies for the money supply in cashless societies and suggest ways in which governments can shape privacy law in order to successfully compete against independent cryptocurrencies.

Part I of this paper discusses why governments would want to transition into a cashless society. Part II of this paper discusses why independent cryptocurrencies are going to be competing with government-backed digital currencies (or electronic payment systems) for control over the supply of money. Part III of this paper will provide an overview of existing privacy law in the United States and the European Union. Part IV will analyze the different privacy

---

[8] Charles Bovaird, *Cryptocurrency's Total Market Cap Has Risen Nearly 800% This Year*, FORBES (Aug. 27, 2017, 6:08 PM), https://www.forbes.com/sites/cbovaird/2017/08/27/cryptocurrencys-total-market-cap-has-risen-nearly-800-this-year/#552643ba67c7; Jake Frankenfield, *Bitcoin*, INVESTOPEDIA (updated Aug. 5, 2018), https://www.investopedia.com/terms/b/bitcoin.asp (last visited Dec. 21, 2018).

[9] Divya Joshi, *List of top virtual currencies in 2017 and what differentiates them*, BUS. INSIDER (Oct. 19, 2017, 5:07 PM), http://www.businessinsider.com/list-top-cryptocurrencies-analysis-comparison-2017-10.

[10] DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION 5 (2016).

[11] Elizabeth Dwoskin & Tony Romm, *Facebook makes its privacy controls simpler as company faces data reckoning*, WASH. POST (Mar. 28, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/03/28/facebooks-makes-its-privacy-controls-simpler-as-company-faces-data-reckoning/?utm_term=.b8c81633e2be.

laws and discuss which ones would better allow governments to compete against independent cryptocurrencies for control over the supply of money.

II. WHY GO CASHLESS?

A. To Combat 'Black Money'

There are two main reasons why a government might want to transition into a cashless society. First, a cashless society would force people to use government regulated virtual money, which is more traceable by the government.[12] Cash transactions provide anonymity in transactions and help people "conceal [their] activities from the government" to "avoid laws [and paying] taxes."[13] When the Indian government made its surprising announcement back in November 2016, it stated that its move was motivated by the desire to eliminate so-called 'black money' as well as fake currency and terror financing.[14] 'Black money' is a term used in the country referring to "unaccounted, untaxed wealth."[15] Any government would be eager to go cashless for the sake of rooting out any untaxed wealth and the proceeds of illegal activity. This could become a big enough motivating factor in pushing other countries into going cashless.

B. To Successfully Implement Negative Interest Rates

The second reason why a government might want to go cashless concerns its ability to successfully implement its own monetary policy.[16] Monetary policy is implemented by the actions of a country's central bank that determines the size and growth rate

---

[12] Kenneth Rogoff, *Costs and Benefits to Phasing Out Paper Currency*, 29 NBER MACROECONS. ANN. 445–46 (2015).

[13] *Id*. at 447.

[14] Krishnan, *supra* note 6.

[15] *Id.*

[16] *The Federal Reserve's response to the financial crisis and actions to foster maximum employment and price stability*, BD. OF GOVERNORS OF THE FED. RESERVE SYS., https://www.federalreserve.gov/monetarypolicy/bst_crisisresponse.htm (last visited Dec. 21, 2018).

of the country's money supply, which then affects interest rates.[17] For example, if a central bank determines that inflation is increasing at a high rate, it will reduce the supply of money in order to bring inflation down to a more acceptable level.[18] In response to the financial crisis of 2008, the Federal Reserve, the central bank of the United States, sought to substantially decrease long-term interest rates and ease the overall financial conditions of the United States.[19] As a result, interest rates in the United States remain historically low, notwithstanding the Federal Reserve's recent push to raise interest rates.[20] Interest rates worldwide also remain historically low.[21] In some countries, like Japan and Sweden, central banks have dipped interest rates low enough to even have them turn negative.[22]

With interest rates at historical lows, some economists are worried about how central banks around the world could respond effectively to the next financial crisis if interest rates are already near

---

[17] James Chen, *Monetary Policy*, INVESTOPEDIA (updated Oct. 19, 2018), https://www.investopedia.com/terms/b/bitcoin.asp (last visited Dec. 21, 2018).

[18] *See id.*

[19] BD. OF GOVERNORS OF THE FED. RESERVE SYS., *supra* note 16.

[20] *See* Akin Oyedele, *The Fed just raised interest rates again—here's how it happens and why it matters*, YAHOO! FIN. (Sept. 26, 2018), https://finance.yahoo.com/news/fed-raise-interest-rates-again-123000207.html; *see also* Elena Holodny, *The 5,000-year history of interest rates shows just how historically low US rates are right now*, BUS. INSIDER (June 17, 2016, 9:46 AM), http://www.businessinsider.com/chart-5000-years-of-interest-rates-history-2016-6; *Federal Reserve Raises Benchmark Interest Rate*, NAT'L PUB. RADIO (June 14, 2017, 4:35 PM), https://www.npr.org/2017/06/14/532969122/federal-reserve-raises-benchmark-interest-rate.

[21] Bob Bryan, *Central bankers are doing something that hasn't happened in 5,000 years—and drastically changing the world economy*, BUS. INSIDER (Aug. 19, 2016, 2:24 PM), http://www.businessinsider.com/record-low-interest-rate-impact-2016-8; Associated Press, *European Central Bank keeps interest rates at record low*, L.A. TIMES (July 21, 2016, 5:50 AM), http://www.latimes.com/business/la-fi-europe-interest-rates-20160721-snap-story.html.

[22] Nicholas Megaw, *Riksbank defends negative interest rates*, FIN. TIMES (Mar. 22, 2017), https://www.ft.com/content/0d148a34-b668-3b14-b95c-c0fadd26dec8; Jonathan Soble, *Japan's Negative Interest Rates Explained*, N.Y. TIMES (Sept. 20, 2016), https://www.nytimes.com/2016/09/21/business/international/japan-boj-negative-interest-rates.html.

zero.[23] One proposed measure central banks could implement in the next financial crisis is negative interest rates.[24] Negative interest rates would mean that people would have to pay banks to keep their money in a bank account[25] or other financial institution.[26] Negative interest rates in Sweden and Japan have largely been confined to banks, i.e., central banks charge other banks a fee for keeping some cash stashed at the central bank.[27] So far, Swedish and Japanese banks have not passed on those fees to the general public who keep cash stashed in their own private bank accounts.[28] However, as in the case of Japan, even though those fees have only been charged to banks and not the general population so far, fears about having to pay banks to hold their money have driven some people in Japan to buy safes and store cash in their houses.[29] It seems that some of the Japanese population would rather store their money at home than face the potential threat that their banks may start to charge them for saving money in a bank account. This fear has become a reality for wealthy depositors at two major German banks, fueling demand for safe deposit boxes.[30] How much longer before regular retail depositors get hit with these charges as well?

---

[23] *How should recessions be fought when interest rates are low?*, THE ECONOMIST (Oct. 21, 2017), https://www.economist.com/news/finance-and-economics/21730416-both-monetary-policy-and-fiscal-policy-answers-remain-contentious-how-should.

[24] Ann Saphir, *Fed's Williams calls for global rethink of monetary policy*, REUTERS, Nov. 16, 2017, 4:42 PM, https://www.reuters.com/article/us-usa-fed-williams/feds-williams-calls-for-global-rethink-of-monetary-policy-idUSKBN1DG33N.

[25] Soble, *supra* note 22.

[26] *Id.*

[27] Richard Milne, *Sweden's central bank chief says negative rates 'undramatic'*, FIN. TIMES (Oct. 17, 2016), https://www.ft.com/content/b5c03c3e-936b-11e6-a1dc-bdf38d484582; Soble, *supra* note 22.

[28] Milne, *supra* note 27.

[29] Lucinda Shen, *Japan's Negative Interest Rates Are Driving up Sales of Safes*, FORTUNE (Feb. 23, 2016), http://fortune.com/2016/02/23/japans-negative-interest-rate-driving-up-safe-sales/.

[30] *The German savers who must pay interest to their own bank*, DW (Mar. 19, 2017), http://www.dw.com/en/the-german-savers-who-must-pay-interest-to-their-own-bank/a-38013400; James Shotter, *German banks charges negative rates on large deposits*, FIN. TIMES (Aug. 11, 2016, 3:24 PM), https://www.ft.com/content/39b009c6-5fc2-11e6-b38c-7b39cbb1138a; *Negative*

It is argued that the "[very] existence of paper currency [which] makes it difficult for central banks to take . . . interests rates much below zero."[31] "As long as central banks [and regular banks] stand ready to convert electronic deposits to zero-interest paper currency in unlimited amounts, it suddenly becomes very hard to push interest rates below levels of . . . –0.25 to –0.50%."[32] The challenge paper currency poses to central banks successfully implementing a negative interest rate policy is that if interest rates are pushed even further negative, savers today (not in a cashless society) will likely respond by taking their money out of the bank and hoard their paper money somewhere else, thereby defeating a central bank's ability to implement negative interest rates onto the economy. However, "if all central bank [and regular bank] liabilities were electronic, paying a negative interest on reserves [or bank accounts] (basically charging a fee) would be trivial."[33] Essentially, this means that negative interest rates would be much easier to implement in a cashless society since banks would no longer have to "convert electronic deposits to . . . paper currency in unlimited amounts."[34] In a cashless society, there is no paper currency available in which to escape negative interest rates. But, this is where independent cryptocurrencies may be able to help.

III. GOVERNMENTS WILL HAVE TO COMPETE WITH INDEPENDENT CRYPTOCURRENCIES OVER THE CONTROL OF THE MONEY SUPPLY IN CASHLESS SOCIETIES

Governments in cashless societies will likely face increasing competition from independent cryptocurrencies over the control of citizens' wealth. Citizens who used to enjoy a certain degree of financial privacy by using cash would have to look for alternative mediums of exchange to get similar assurances of privacy in a

---

ECB rates fuel demand for safe deposit boxes, German banks say, REUTERS, Mar. 17, 2016, 9:50 AM, https://www.reuters.com/article/germany-banks-savings/negative-ecb-rates-fuel-demand-for-safe-deposit-boxes-german-banks-say-idUSL5N16P45T.

[31] Rogoff, *supra* note 12, at 445.

[32] *Id.* at 446.

[33] *Id.*

[34] *Id.*

cashless society. These citizens could turn to something more traditional—like gold—or they could opt for the more modern alternative: independent cryptocurrencies.

A. Independent Cryptocurrencies Can Undermine Governments' Objectives of a Cashless Society

Cryptocurrencies remain largely unregulated[35] as governments struggle to determine how to even begin to regulate them.[36] Despite the paucity of regulation, the total market capitalization of all cryptocurrencies combined has surged to $230.9 billion.[37] It would stand to reason that even if societies become cashless, independent cryptocurrencies would still exist. However, the very existence of cryptocurrencies could serve to thwart governments' goals of severely curtailing the use of 'black money' and successfully implementing negative interest rates.

Cryptocurrencies could limit the government's ability to stamp out 'black money' in a completely cashless society because their unregulated status make them highly resistant to censorship.[38] This is because while it is possible to observe a bitcoin transaction in process, it is not possible to stop it—and this is what makes cryptocurrencies different from conventional banking (where banks

---

[35] Paul Sydlansky, *Investing in Cryptocurrency: The Risks*, INVESTOPEDIA (Sept. 14, 2017), https://www.investopedia.com/advisor-network/articles/investing-cryptocurrency-risks/.

[36] *Investor Bulletin: Initial Coin Offerings*, U.S. SEC. & EXCH. COMM'N, https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings (last visited Dec. 21, 2018); *A surge in the value of crypto-currencies provokes alarm*, THE ECONOMIST (May 18, 2017), https://www.economist.com/news/finance-and-economics/21722235-bitcoin-far-only-game-town-surge-value-crypto-currencies.

[37] Charles Bovaird, *Why The Crypto Market Has Appreciated More Than 1,200% This Year*, FORBES (Nov. 17, 2017, 1:46 PM), https://www.forbes.com/sites/cbovaird/2017/11/17/why-the-crypto-market-has-appreciated-more-than-1200-this-year/#5cae72be6eed.

[38] Alex Hern, *Everything you wanted to know about bitcoin but were afraid to ask*, THE GUARDIAN (Nov. 11, 2017, 2:00 PM), https://www.theguardian.com/technology/2017/nov/11/everything-you-ever-wanted-to-know-about-bitcoin-but-were-to-afraid-to-ask-cryptocurrencies.

can freeze accounts and enforce regulations).[39] This has made cryptocurrencies a haven for cybercrime and drug trading.[40] Therefore, even if a government is successfully able to transition into a completely cashless society, criminal elements could put their illicit gains in cryptocurrencies to evade government scrutiny. This would still be the case regardless of whether or not governments start to regulate a group or even all of the currently existing cryptocurrencies since a new cryptocurrency can be created that completely evades government scrutiny like they have been popping up now.[41]

Cryptocurrencies could also limit a central bank's ability to successfully implement negative interest rates by taking the place of paper currency as an alternative to storing money in a government regulated bank or other financial institution. If banks start charging their customers negative interest rates, those same customers could choose to store their money in independent cryptocurrencies that at the very least won't charge them negative interest rates. Cryptocurrencies, like cash, would then severely limit a central bank's ability to successfully implement negative interest rates in a financial crisis.

B. A Cashless Society Could Pose a Threat to Financial Privacy

The seemingly beneficial independence of these digital currencies could also be its biggest drawback. The value of these digital currencies can be very volatile[42] and the lack of regulation deters most mainstream investors, including regular, everyday bank depositors, from delving into this new market.[43] However, this lack

---

[39] *Id.*

[40] *Id.*

[41] Joshi, *supra* note 9.

[42] Jemima Kelly, *Bubbly bitcoin no worth the wager: investors*, REUTERS, Nov. 17, 2017, 11:22 AM, https://www.reuters.com/article/us-investment-summit-bitcoin/bubbly-bitcoin-not-worth-the-wager-investors-idUSKBN1DH249; Arjun Kharpal, *Bitcoin is on track for its worst first quarter ever with over $114 billion wiped off its value*, CNBC (Mar. 30, 2018, 8:48 AM), https://www.cnbc.com/2018/03/30/bitcoin-price-is-on-track-for-its-worst-first-quarter-ever.html.

[43] *Id.*

of government oversight can become a big virtue, and therefore overlooked by investors, if societies do indeed become cashless. This is because "it is far from clear that . . . government[s] can credibly issue a fully anonymous electronic currency"[44] in the way paper currency currently provides some level of anonymity. Having every financial transaction go digital would mean having every single financial transaction recorded somewhere, either by banks or other third parties. This information could prove a coveted target for storage, collection, and surveillance for national security agencies, similar to what the internet has become.[45] While the exposure of the United States' National Security Agency's warrantless internet surveillance program has not deterred people from using the internet, the threat of widespread financial surveillance in a cashless society could push more people into using independent cryptocurrencies.

Privacy laws seek to properly balance the need for government oversight in certain financial transactions with the right of privacy its citizens seek to remain respected. A comparative analysis of different privacy laws in the United States and the European Union supports the conclusion that an amalgamation of these different types of privacy laws would provide governments with the competitive edge they need to compete successfully against independent currencies.

---

[44] Rogoff, *supra* note 12, at 451.

[45] *See* Jared Keller, *Nearly Four Years After The Snowden Revelations The NSA Backs Off (Some) Warrantless Surveillance*, PAC. STANDARD (May 1, 2017), https://psmag.com/news/nearly-four-years-after-the-snowden-revelations-the-nsa-backs-off-some-warrantless-surveillance; Michael B. Kelley & Brian Jones, *Here's The $2 Billion Facility Where The NSA Stores And Analyzes Your Communications*, BUS. INSIDER (June 7, 2013, 12:55 PM), http://www.businessinsider.com/pictures-of-the-nsas-utah-data-center-2013-6.

IV. PRIVACY LAW IN THE UNITED STATES AND THE EUROPEAN UNION

A. Privacy Law in the United States

Privacy, in the United States, is defined as "liberty from an intrusive government"[46] and privacy law focuses on protecting personal privacy and—that point where individuals come into conflict with the government—criminal law.[47] This conflict implicates the Fourth Amendment of the U.S. Constitution that regulates searches and seizures by the federal government.[48] The protections of the Fourth Amendment was later incorporated by the Supreme Court into the U.S. Constitution's Fourteenth Amendment's Due Process Clause and applied against the individual states.[49]

Under this amendment, a search conducted by a government official occurs "when the government intrudes on a person's reasonable expectation of privacy."[50] An individual has a reasonable expectation of privacy when that individual has "a subjective expectation of privacy in the information [sought]" and society also recognizes that expectation as reasonable.[51] "The Supreme Court 'has inferred that a warrant must generally be secured' before a search by law enforcement may be executed."[52] The warrant requirement "ensures the a neutral magistrate, as opposed to a zealous officer, determines that probable cause

---

[46] JOHN T. SOMA ET AL., PRIVACY LAW IN A NUTSHELL 47 (2d ed. 2014).

[47] *Id.* at 48.

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

[49] *Mapp v. Ohio*, 367 U.S. 643 (1961).

[50] Justin Santolli, Note, *The Terrorist Finance Tracking Program: Illuminating the Shortcomings of the European Union's Antiquated Data Privacy Directive*, 40 GEO. WASH. INT'L L. REV. 553, 575 (2008).

[51] *Id.*

[52] Tristan M. Ellis, Note, *Reading Riley Broadly: A Call for a Clear Rule Excluding All Warrantless Searches of Mobile Digital Devices Incident to Arrest*, 80 BROOK. L. REV. 463, 470 (2015) (quoting Kentucky v. King, 563 U.S. 452, 459 (2011)).

exists."[53] This means that "there is a fair probability that contraband or evidence of a crime will be found in a particular place."[54] A search warrant: (1) "must be issued by a neutral, disinterested magistrates"; (2) "those seeking the warrant must demonstrate to the magistrate their probable cause to believe that 'the evidence sought will aid in a particular apprehension or conviction' for a particular offense"; and (3) "[it] must particularly describe the 'things to be seized' as well as the place to be searched.[55]

Unlike the European Union, general data protection laws are avoided in the United States "in favor of specific laws governing [specific sectors] . . . and information collected during certain types of financial transactions."[56] This is typically called the "sectoral approach"[57] which "relies on a mix of legislation and self-regulation" with "a strong bias toward self-regulation, where companies and industry bodies establish codes of practice."[58] In most situations, the default position in the United States is that "either no privacy protection applies beyond the privacy torts—not all of which are even recognized in every state—or a limited amount of protection flowing from contractual agreements" apply.[59] This approach has been recently highlighted in the response towards the massive data breach experienced by Equifax.[60] The response has largely comprised of private rights of action against Equifax,[61]

---

[53] Dylan Bonfigli, Note, *Get a Warrant: A Bright-Line Rule for Digital Searches Under the Private-Search Doctrine*, 90 S. CALIF. L. REV. 307, 311 (2017).

[54] *Id.* at 312 (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

[55] Dalia v. United States, 441 U.S. 238, 255 (1979) (internal quotation marks omitted).

[56] SOMA ET AL., *supra* note 46, at 48.

[57] *Id.*

[58] *Id.*

[59] *Id.* at 49.

[60] *See generally* Spencer Kimball & Liz Moyer, *Equifax data breach may affect 2.5 million more consumers than originally stated*, CNBC BUS. (Oct. 2, 2017, 4:39 PM), https://www.cnbc.com/2017/10/02/equifax-2-point-5-million-more-consumers-may-be-affected-by-data-breach-than-originally-stated.html.

[61] *See* Tara Swaminatha, *Equifax now hit with a rare 50-state-class-action lawsuit*, CSO (Nov. 22, 2017, 5:39 AM), https://www.csoonline.com/article/3238076/data-breach/equifax-now-hit-with-a-rare-50-state-class-action-lawsuit.html.

countless government investigations,[62] offerings of free credit monitoring and identity theft protection (but not without initially—and later backtracking on—requiring affected consumers give up their right to sue if they wanted the free services),[63] and threats of massive fines from the government.[64]

I concentrate my survey of privacy law in the United States on both financial privacy law and data protection law. Data protection law encompass "laws governing the collection, storage, use and dissemination to third-parties of both personally identifying information (PII) and non-PII about consumers that is collected, stored or used online."[65] In a cashless society, all financial transactions would be digitally recorded. This digitally recorded financial information would be analogous to information that is contained on the internet. Therefore, apart from reviewing regular financial privacy laws, I will also review data protection laws that apply to personal information that appears online since these laws would most likely also be applicable to digitally recorded financial data in a cashless society.

1. Financial Privacy Law in the United States

The perfect starting point from which to start a review of financial privacy law in the United States would be the U.S. Constitution. The Supreme Court "sought to clarify the scope of financial privacy"[66] in *United States v. Miller*.[67] In this case, the government had successfully convicted Mitchell Miller of running an unregistered still.[68] On appeal, Miller petitioned the Supreme

[62] *See id.*

[63] Jim Puzzanghera, *Senators want 'massive' fines for data breaches at Equifax and other credit reporting firms*, L.A. TIMES (Jan. 10, 2018), http://www.latimes.com/business/la-fi-equifax-data-breach-fines-20180110-story.html.

[64] *Id.*

[65] Ian C. Ballon, 3 E-COMMERCE AND INTERNET LAW: TREATISE WITH FORMS 26.01 (2d ed. 2017).

[66] SOMA ET AL., *supra* note 46, at 87.

[67] 425 U.S. 435 (1976).

[68] *Id.* at 436.

Court to uphold the Court of Appeal's reversal of his conviction.[69] The Court of Appeals reversed after finding that Miller's motion to suppress copies of bank records that were retained by Miller's banks in compliance with the Bank Secrecy Act of 1970 should have been granted by the lower court since it found that these documents were protected by the Constitution's "zone of privacy."[70] The Supreme Court reversed and held that the subpoenaed materials were not Miller's private papers and were instead "business records of the banks,"[71] and, therefore, the Court perceived "no legitimate 'expectation of privacy' in their contents"[72] in spite of the fact that these records are being kept by the bank pursuant to the Bank Secrecy Act's recordkeeping requirement.[73] Thus, the Supreme Court determined in *Miller* that "an individual does not have a reasonable expectation of privacy in information that he or she 'voluntarily conveys'" to third parties.[74] However, *Miller's* holding with regard to the lack of reasonable expectation of privacy in information that a person has voluntarily disclosed to third parties has indirectly been called into question by *Riley v. California*.[75]

In *Riley v. California*, the Supreme Court held "that the information contained on a cell phone, because of [the] high privacy interests, could not be searched incident to arrest without a warrant."[76] While the Supreme Court did not address the implications of the third party doctrine in its holding in *Riley v. California*,[77] the Supreme Court's observation that a large amount of the data used on a cell phone is not actually stored in the device itself, but instead with third parties (like cloud computing),[78] implicates the third party doctrine. Since the Supreme Court in *Riley*

---

[69] *Id.* at 435.
[70] *Id.* at 440.
[71] *Id.*
[72] *Id.* at 442.
[73] *Id.*
[74] Santolli, *supra* note 50, at 575.
[75] __ U.S. __, 134 S. Ct. 2473 (2014); Isabella Blizard, Comment, *Phone Sweet Phone: The Future of the Private Search Doctrine Following Riley v. California*, 49 U. PAC. L. REV. 207, 215–16 (2017).
[76] *Id.* at 214.
[77] *Id.* at 215.
[78] Blizard, *supra* note 75, at 215.

did not explicitly overrule the third-party doctrine, I must resort to agreeing with scholars who have alluded to the removal of the third-party doctrine from case law based on the analysis undertaken in *Riley*.[79]

In response to *United States v. Miller*, Congress passed the Right to Financial Privacy Act ("RFPA") in 1978.[80] The RFPA focuses on requiring that the government provide notice to the affected individual "where a government agency seeks financial records."[81] It does not require the individual's consent to the disclosure if disclosure is sought pursuant to a judicial subpoena or search warrant.[82] The RFPA does accord bank customers some right to challenge administrative subpoenas of financial records possessed by banks.[83] But the RFPA limits the kind of customers who are covered by it and the types of records they may seek to have protected, and it also prescribes strict procedural rules to which a customer must adhere to when challenging a subpoena.[84] An example of the Act's strict procedural rules is that a customer "cannot appeal an adverse determination until the Government has completed its investigation."[85] The RFPA also contains some exceptions to the notice requirement.[86] For example, if the disclosure is pursuant to a court order, notice may not be given until after the financial information has been obtained if the government agency shows that notice will result in flight from prosecution or evidence destruction.[87]

Providing customers of banks that their financial activities are being monitored by government agents is sure to become a big issue in a cashless world. Notice would inform a customer that they are the target of a government investigation and would also provide them with the opportunity to challenge that type of surveillance if they can seek to challenge the government's actions in court. It

---

[79] *Id.*
[80] SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735 (1984).
[81] SOMA ET AL., *supra* note 46, at 91.
[82] *Id.*
[83] *O'Brien*, 467 U.S. at 735.
[84] *Id.* at 745.
[85] *Id.*
[86] SOMA ET AL., *supra* note 46, at 92.
[87] *Id.*

would give citizens a chance to safeguard their financial privacy and not be blindsided by the investigation after the fact.

The Bank Secrecy Act ("BSA") was passed by Congress in 1970.[88] Its aim was to prevent money laundering and required financial institutions to maintain certain records and to report some transactions.[89] After this law was passed, the U.S. Treasury Department issued regulations that required financial institutions to report any transaction that involved more than $10,000,[90] and also required them to report related transactions that, combined, exceeded $10,000.[91] In 1999, the Financial Modernization Act, also known as the Gramm-Leach-Bliley Act ("GLBA"), allowed financial institutions to join with one another and create financial holding companies.[92] This consolidation in the financial services industry created a lot of concern over a small group of institutions having control over the financial information of millions of people.[93] To ease these concerns, the GLBA required financial institutions to disclose their privacy policies to all customers and to provide them with an opportunity to opt out of disclosing financial information to non-affiliated third parties.[94]

Recently, financial privacy laws in the United States had an impact on financial privacy in the international community. After the September 11, 2001 terrorist attacks in the United States, the U.S. Congress passed what is known as the Patriot Act in 2001.[95] The Patriot Act "amended financial privacy law to provide law enforcement with better means of catching money launderers and

---

[88] *Id.* at 78.

[89] *Id.*

[90] *Id.*; *see also* 31 C.F.R. § 1010.311 (2019) (filing obligations for reports of transactions in currency).

[91] SOMA ET AL., *supra* note 46, at 78–79; *see also* 31 U.S.C. § 5324 (2019) (prohibiting structuring transactions with the goal of evading reporting requirements).

[92] John S. Wisiackas, Comment, *Foreign Account Tax Compliance Act: What It Could Mean for the Future of Financial Privacy and International Law*, 31 EMORY INT'L L. REV. 585, 591 (2017).

[93] *Id.*

[94] *Id.*

[95] *Id.* at 591–92.

international terrorists."[96] It outlined a new set of reporting requirements for financial institutions which included "mandating financial institutions to turn over any and all records if the Treasury Department determined an account or transaction to be 'of primary money laundering concern,' even if the financial institution was located outside of the United States."[97] On March 19, 2010 the Foreign Account Tax Compliance Act ("FATCA") was passed by the U.S. Congress in an effort to help "the IRS detect tax evasion by U.S. taxpayers with undeclared assets in foreign institutions."[98] FATCA "requires U.S. taxpayers with foreign financial assets to report income earned on these assets to the IRS"[99] and it also requires foreign financial institutions "to report personal financial information directly to the IRS regarding any clients that are (or should be) paying U.S. taxes, regardless of the fact that these [foreign financial institutions] are not subject to U.S. law."[100]

The reporting requirements FATCA burdens individual U.S. taxpayers with are concerning to many and the burden it imposes on foreign financial institutions is equally, if not more, controversial.[101] Those who feel that "the economic and personal burdens on U.S. citizens, [foreign financial institutions], and foreign governments have become excessive" are challenging FATCA all over the world.[102] A number of those who are affected by FATCA and are unwilling to bear the costs "have chosen a variety of different paths to avoid having to comply, ranging from selling their U.S. investments to renouncing their citizenship or green cards,"[103] and some foreign financial institutions have responded "by dropping their U.S. tax-paying clients [leaving] many of the over six million U.S. citizens living aboard and working overseas unable to obtain a foreign bank account."[104] It is clear that the United States will be

---

[96] *Id.* at 592.
[97] *Id.*
[98] Wisiackas, *supra note* 92, at 593–94.
[99] *Id.* at 594.
[100] *Id.* at 595.
[101] *Id.* at 586.
[102] *Id.* at 601.
[103] *Id.* at 603.
[104] *Id.*

continuing to leverage its economic importance to shape the world of international (financial) privacy law for decades.

B. Privacy Law in the European Union

1. Private Sector Data Protection in the European Union

The motivation driving privacy law in the European Union differs greatly from that of the United States. To start off, the European Union recognizes privacy as a fundamental human right.[105] Historically, Europe has displayed a greater distrust of corporations than the United States.[106] European privacy law has mostly focused on "protecting consumers' personal information from being improperly collected or misused by commercial entities."[107] This is in great contrast to the approach taken in the United States where emphasis is placed on protecting personal privacy from an intrusive government.[108] Generally, in most European countries, personal information about a consumer cannot be collected without the consumer's permission and they also "have the right to review the data and correct inaccuracies."[109] Companies that process consumer data are obligated to register their activities with the government and personal information about a consumer cannot be shared with other companies or across borders without the consumer's express permission.[110]

These rights mostly derive from the E.U. Directive on Data Protection of 1995 ("The Directive").[111] The Directive's purpose was to provide "analogous protections for personal information throughout the European Community"[112] and contained "eight core principles: purpose limitation, data quality, data security, sensitive data, transparency, data transfer, independent oversight, and

---

[105] Santolli, *supra* note 50, at 565.
[106] SOMA ET AL., *supra* note 46, at 46.
[107] *Id.*
[108] *See id.* at 47.
[109] *Id.* at 46.
[110] *Id.*
[111] *Id*. at 47.
[112] *Id.*

individual redress."[113] These principles were established to ensure that an individual consumer "has the ability to control his or her 'public image'"[114] and to establish protections for an individual against the media which can "publicize unpleasant or distorted details about his or her life."[115] Overall, The Directive was an attempt to empower individuals with the necessary tools "to regulate what personal information is disseminated to the public"[116] and "'cover[ed] all private sector processing of personal data.'"[117] Therefore, unlike the United States' sectoral approach, the European Union has chosen to enact a general data protection law that applies to the entire private sector—including the financial sector. Most notably, however, The Directive "[did] not apply to [data] transfers undertaken for public or state security."[118]

More recently, the European Parliament passed the General Data Protection Regulation ("GDPR") on April 14, 2016. The GDPR replaced The Directive and came into effect on May 25, 2018.[119] Although the GDPR still holds true to the key principles of data privacy from The Directive, "many changes have been proposed to the regulatory policies."[120] Some of the key changes the GDPR brings involve the use of "clear and plain language" to request consumer consent for data retention,[121] prompt breach notification to consumers,[122] the right of consumers to request a copy of all the personal data being retained by the company,[123] fines of up to 4% of a company's global turnover of the preceding year or

---

[113] Santolli, *supra* note 50, at 566.
[114] *Id.*
[115] *Id.*
[116] *Id.*
[117] *Id.* at 567 (quoting Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 13 (2000)).
[118] *Id.*
[119] *EU GDPR – Information Portal*, EU GDPR.ORG, https://www.eugdpr.org (last visited Dec. 22, 2018).
[120] *GDPR Key Changes*, EU GDPR.ORG, https://www.eugdpr.org/key-changes.html (last visited Dec. 22, 2018).
[121] *Id.*
[122] *Id.*
[123] *Id.*

€20 million (whichever is greater) in case of a breach,[124] and the right to be forgotten.[125]

2. Data Protection Regarding Law Enforcement in the European Union

On April 14, 2016, the European Parliament also passed the Police and Criminal Justice Authorities Directive ("PCJD") which aims to streamline the transfer of information between Member States' police and judicial authorities.[126] Before the PCJD, law enforcement in the European Union had "to apply different sets of data protection rules according to the origin of the personal data."[127] This harmonization of data protection laws in all member states of the European Union is aimed to facilitate police cooperation between member states.[128] The PCJD also applies to domestic processing of personal data by law enforcement.[129] Member states have until May 6, 2018 to pass any relevant legislation for compliance with the PCJD.[130] The PCJD reflects the key principles of processing personal data only when necessary, proportional and pursuant to a specific purpose.[131]

According to the PCJD, Member States must abide by certain principles relating to the processing of personal data.[132] Member states must ensure that personal data be:

(a) processed lawfully and fairly;

(b) collected for specified, explicit and legitimate purposes and not processed

---

[124] *Id.*

[125] *Id.*

[126] European Commission Statement 16-1403, Joint Statement on the final adoption of the new EU rules for personal data protection (Apr. 14, 2016).

[127] *Id.*

[128] *Id.*

[129] ARTHUR COX, *Data Protection Update - New Legislation*, LEXOLOGY (May 19, 2016), https://www.lexology.com/library/detail.aspx?g=917aa8d0-b85d-4633-a2ec-f678698f355e.

[130] *Id.*

[131] *Id.*

[132] Council Directive 2016/680, art. 4, 2016 O.J. (L 119) 107 (EC).

> in a manner that is incompatible with those purposes;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are processed;
>
> (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed;
>
> (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.[133]

The definition of "lawful" processing of personal data is broad and guidance on what constitutes fair processing of such data is scarce.[134] A processing of personal data is lawful "if and to the extent that processing is necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law."[135]

---

[133] *Id.*

[134] *See* Council Directive, *supra* note 132, art. 8, at 109; Paul de Hert & Vagelis Papakonstantinou, *The New Police and Criminal Justice Data Protection Directive: A First Analysis*, 7 NEW J. EUR. CRIM. L. 7, 11 (2016).

[135] Council Directive, *supra* note 132, art. 8(1), at 109.

According to Article 1(1), the purposes for the processing of personal data by competent authorities covered by the PCJD are: "the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security."[136] In essence, "for the legality of the processing to be established . . . only the performance of a task within [the PCJD's] scope need occur, as described in the Member State [or E.U.] law implementing it."[137] While fairness is not explicitly defined in a separate article of its own, the PCJD notes that "fair processing is a distinct notion from the right to a fair trial."[138] The PCJD goes on to state that:

> Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of their personal data and how to exercise their rights in relation to the processing. In particular, the specific purposes for which the personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate and relevant for the purposes for which they are processed. It should, in particular, be ensured that the personal data collected are not excessive and not kept longer than is necessary for the purpose for which they are processed. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the data are not kept longer than necessary,

[136] *Id.* art. 1(1), at 105.
[137] de Hert & Papakonstantinou, *supra* note 134, at 11.
[138] Council Directive, *supra* note 132, subdiv. 26, at 93.

> time limits should be established by the controller for erasure or for a periodic review. Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use.[139]

Essentially, fairness requires notice to citizens of their rights over their personal data and narrowly tailored collection of personal data by law enforcement. Overall, the PCJD provides member states and the European Union with the guiding principles to which their data protection laws must adhere.

V. COMPARATIVE ANALYSIS OF PRIVACY LAW IN THE UNITED STATES AND THE EUROPEAN UNION

A. What is Money?

There are many definitions of money. One defines money as "[a]nything of value that serves as a (1) generally accepted medium of financial exchange, (2) legal tender for repayment of debt, (3) standard of value, (4) unit of accounting measure, and (5) means to save or store purchasing power."[140] To optimally perform all of these functions, "money has to be available, affordable, durable, fungible, portable and reliable."[141] I would argue that a certain amount of privacy and personal autonomy should also be included in this definition. While large segments of the world (mostly U.S.) population can tolerate growing government encroachment on their privacy over the internet and other wireless

---

[139] *Id.*

[140] *Money*, BUSINESS DICTIONARY, http://www.businessdictionary.com/definition/money.html (last visited Feb. 20, 2018).

[141] NIALL FERGUSON, THE ASCENT OF MONEY: A FINANCIAL HISTORY OF THE WORLD 24 (2008).

forms of communication,[142] it is doubtful that the same amount of people would be comfortable with their government keeping detailed records of their financial life. All previous versions of money including cowrie shells,[143] metals, and even paper currency have an inherent quality of anonymity to them. It would be unprecedented to have everybody's financial transactions recorded in a database and accessible to law enforcement for an indeterminate amount of time. However, this would be possible in an entirely cashless society and in order to safeguard their financial privacy, a significant portion of the population in a cashless society might turn to alternative methods of payment, like gold or cryptocurrency.

This is where the importance of privacy law in a new cashless world is clear. Privacy law can play an important role in preventing a citizen flight from state-sanctioned cashless societies into non-state issued cryptocurrencies. If citizens are satisfied with their rights to privacy, including financial privacy, and truly come to believe that their government will respect their privacy rights, their confidence in the state-sanctioned cashless society will grow and stifle competition from non-state issued cryptocurrencies. If citizens find their privacy laws lacking, some will decide that it is in their best interest to store their wealth in alternative payment systems like cryptocurrencies. It is an unfortunate stereotype that all citizens who place a high value on their privacy are looking to evade taxes or are involved in criminal enterprises. As the United States' Supreme Court stated, people do have legitimate

---

[142] *See* James Ball, *NSA stores metadata of millions of web users for up to a year, secret files show*, THE GUARDIAN (Sept. 20, 2013, 12:35 PM), https://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents; *see also* James Vincent, *NSA collected 151 million phone records in 2016, despite surveillance law changes*, THE VERGE (May 3, 2017, 4:22 AM), https://www.theverge.com/2017/5/3/15527882/nsa-collecting-phone-records-us-citizen-metadata; Melody Kramer, *The NSA Data: Where Does It Go?*, NAT'L GEOGRAPHIC (June 12, 2013), https://news.nationalgeographic.com/news/2013/06/130612-nsa-utah-data-center-storage-zettabyte-snowden/; *see also* Ms. Smith, *NSA whistleblower discusses 'How the NSA tracks you*', CSO (Aug. 7, 2017, 8:11 AM), https://www.csoonline.com/article/3213033/security/nsa-whistleblower-william-binney-presented-how-the-nsa-tracks-you-at-sha2017.html.

[143] WEATHERFORD, *supra* note 1, at xi.

expectations of privacy.[144] Even though a society might change its concept of what is a reasonable expectation of privacy an individual can have over their financial records (which is likely to change in order to facilitate the creation of a cashless society by the government), a citizen will use all avenues available to them to ensure the level of privacy that they think is adequate for them (similar to how some choose to use blackout curtains on their bedroom windows).

B. European Union vs. the United States: Differences in their Approaches to Privacy

The European Union has focused more on providing E.U. citizens with a comprehensive baseline of privacy rights in both the public and private sector, whereas the United States has focused more on private sector autonomy and emphasizing the search warrant requirement. In terms of which is the best system to provide citizens with a greater understanding of their rights to privacy, the European Union's privacy law model clearly wins. The European Union has established an exhaustive list of privacy rights that E.U. citizens enjoy. In contrast, the United States' Supreme Court has merely stuck to determining that there are "penumbral rights" emanating from constitutional provisions[145] and that certain amendments create "zones of privacy."[146] This has been interpreted to create a "concept of an unwritten penumbra right of privacy emanating from the Bill of Rights as a guarantee under the Constitution."[147] It is clear that many U.S. citizens will be confused as to what exactly their "penumbra right to privacy" entails. Although many Supreme Court cases have clarified the scope of this penumbra right to privacy, this is a malleable concept that the Supreme Court changes to accommodate changes in society's attitudes towards reasonable expectations of privacy. Therefore, the

---

[144] *See* Katz v. United States, 389 U.S. 347 (1967); *see also* Kyllo v. United States, 533 U.S. 27 (2001).

[145] David Luban, *The Warren Court and the Concept of a Right*, 34 HARV. C.R.-C.L. L. REV. 7, 28 (1999).

[146] *Id.*

[147] Scott E. Squillace, *Removal of a Nutrient Feeding Tube and the Need for a Living Will*, 3 J. CONTEMP. HEALTH L. & POL'Y 253, 255 (1987).

clear delineation of privacy rights that the European system affords is better at informing citizens of their privacy rights. Since knowledge is power, a citizenry that is better informed of their rights will be in a better position to see that they are enforced and safeguarded from private and public intrusion.

The United States' Supreme Court's decision to impose a general Fourth Amendment requirement to the federal, state, and local governments provides the United States with an advantage over the European Union's privacy law model. At least in terms of Fourth Amendment jurisprudence, the Supreme Court's case law regarding search warrant requirements applies across the board throughout all levels of government in the United States. The European Union's privacy law model works at a disadvantage in this respect since each member state is allowed to enact their own legislation regarding processing of personal data by law enforcement and gets to determine what is a "lawful" processing of that data. The European Union's federalism can work against it in the area of privacy law since; even though the overall guiding principles of privacy law apply to all member states, each member state can still choose to enact different versions of privacy law they determine to meet those guiding principles. Variations in privacy law across member states could end up causing confusion for E.U. citizens and also create tension among the member states.

The future of consumer privacy law in the European Union and the United States seem diametrically opposed, whereas the future of privacy law in the public sector seem to be converging. The United States seems content in their laissez-faire attitude towards privacy law in the private sector. It seems that the tradition of "address[ing] privacy concerns beyond the criminal context . . . in a manner that would have the least possible impact on economic activity beyond what was perceived as being necessary to address a particular immediate concern"[148] remains strong in the United States and is unlikely to change in the near future. In the European Union, however, the landscape in privacy law viz a viz the private sector could not be more different. There are strict regulations companies must adhere to with regards to the processing of consumer data and

[148] SOMA ET AL., *supra* note 46, at 48.

there are more rights enjoyed by E.U. citizens with regards to their personal information when compared to those of U.S. citizens (most notably the right to be forgotten). In contrast, when it comes to protecting personal data from the government, the European Union and the United States seem to agree that the government is entitled to more leeway in how they process personal information from citizens. In the European Union, member states get to enact their own privacy laws that protect their citizens' personal information from government intrusion. The tendency of recent financial privacy legislation in the United States is to lean towards greater governmental access of an individual's financial information—including financial information located outside of the United States as is the case with FATCA and the Patriot Act. So, at least in the financial sector, the privacy law protections have been greatly loosened in the United States.

C. Privacy Law in a Cashless Society

In a cashless society, the most optimal starting point would be in recognizing that privacy is a fundamental human right. There might be no other point in history where such minute details of a person's life have been able to be recorded and stored by companies and government agencies. While much of this loss in privacy has been self-inflicted, the importance of maintaining privacy in an increasingly virtual world (let alone a cashless society) cannot be overstated. Since governments would be monitoring data that financial institutions keep recorded on their customers, enacting general data protection laws that apply to the entire private sector—no matter the industry—would be most beneficial. Certain privacy laws can be modified depending on the type of industry, but having data protection laws that apply generally will provide citizens with a greater understanding of their privacy rights and aid them in their quest to ensure that their rights are respected. The right to review the data private institutions—including financial institutions—have about them and also the right to correct any inaccuracies is essential as well especially since there is the potential of governmental scrutiny over these records.

With respect to the government's access to a person's financial records, privacy law should look more like the laws

governing in the United States with respect to government searches. The government should first seek to obtain a search warrant from a judge and, if the search warrant is granted, provide notice to the individual being investigated of the search of his financial records (unless certain exceptions apply—like the risk of evidence being destroyed). Individuals must be afforded the opportunity to be able to challenge the search warrant unless certain exceptions apply. In addition, if transactions above a certain limit must be reported to appropriate governmental authorities the threshold amount perhaps should be increased above $10,000 since that figure was set by the U.S. Treasury Department in the 1980s.

VI. CONCLUSION

There are clear advantages and disadvantages to both the European and American systems of privacy law. I believe that the best system to compete against independent cryptocurrencies would resemble an amalgamation of both the United States' and the European Union's privacy laws. The European model of privacy law with respect to private institutions would be the best baseline for privacy law in a cashless society. Layered on top of that would be the additional protections that exist in the United States' privacy law with respect to governmental intrusion on an individual's privacy. Of course, with the added benefit that these protections would apply across the entire cashless society and not merely be a guideline as is the case with the European Union's privacy laws governing the state's review of private personal data. This privacy law model would be much more efficient and easier for citizens to comprehend as opposed to letting member states each enact their own versions of privacy law. Variations in governmental data protection laws can create confusion among citizens and tension among different member states that create their own data protection laws. The adoption of a single privacy law model would provide citizens with the necessary clarity in their rights to privacy and ways to safeguard it as well as instill an appropriate level of confidence in a cashless society that will be needed to compete against independent cryptocurrencies.