PEPPERDINE UNIVERSITY

The Journal of Business, Entrepreneurship & the Law

Volume 17 | Issue 1 Article 4

6-15-2024

# Going Cashless: Privacy Implications for Gun Control in a Digital Economy

Liza Goldenberg

# GOING CASHLESS: PRIVACY IMPLICATIONS FOR GUN CONTROL IN A DIGITAL ECONOMY

Liza Goldenberg[1]



[1] Pepperdine Caruso School of Law, J.D. 2024; University of California, Los Angeles, B.A. cum laude 2021. I thank Professor Gregory S. McNeal for providing extensive feedback as my Comment developed. I am also indebted to Professor Bernard James for sharpening my understanding of constitutional law, and to Kenrick Shoemaker for reading more drafts of this Comment than I can count. Lastly, I extend a most special thank you to my family for always supporting me and to Daniel for inspiring my research and keeping me sane throughout the process.

## I. INTRODUCTION

As the international community applies innovative technology to address global crises like environmental degradation and world hunger,[2] humans might not realize that their revolutionary aims threaten to drive a once abundant resource into extinction.[3] Across the world, top central banks are preparing for a cashless future by researching ways to implement central bank digital currency (CBDC) as an alternative to physical cash.[4] The central bank of the United States, commonly known as the Federal Reserve, has followed suit with the rest of the world and is currently researching and experimenting with a CBDC.[5]

---

[2] *See* Dan Wellers et al., *Technology for Preserving Biodiversity*, SAP, https://www.sap.com/insights/viewpoints/technology-for-biology-preserving-biodiversity.html (last visited Feb. 8, 2023) (describing several sensors that can "detect and protect species at risk"); *Five Ways that High-Tech Maps Can Help Protect Biodiversity*, INT'L TELECOMM. UNION (Apr. 22, 2022), https://www.itu.int/hub/2022/04/high-tech-maps-can-help-protect-biodiversity/ (detailing how supercomputers can generate high-tech maps that predict migration locations for various species as climate change alters ecosystems and forces a global redistribution); *Technological Advances Leading the Fight to End World Hunger*, U. TEX. AUSTIN (Dec. 24, 2021), https://sites.utexas.edu/discovery/2021/12/24/technological-advances-leading-the-fight-to-end-world-hunger/ (noting how artificial intelligence applications in the agricultural industry can increase production efficiency and improve food distribution toward reducing world hunger).

[3] Mike Kresse, *Will We See the End of Cash by 2030?*, FIS, https://www.fisglobal.com/en-au/fintech2030/connectivity/cashless-society-2030 (last visited Feb. 8, 2023) ("In a single generation, cash has fallen from the undisputed king of payments to nearly the verge of extinction . . . . Cash is being replaced over time as technology produces alternatives . . . .").

[4] *See* Jeremy Srouji & Dominique Torre, *The Global Pandemic, Laboratory of the Cashless Economy?*, 10 INT'L J. FIN. STUD. (2022) (noting that a 2020 study involving sixty-six central banks around the world found that 80% of these banks had already been researching ways to implement a CBDC); *see also* Kilian Laverty, *CBDC and the Fragility of a Cashless Society*, THE HILL (Mar. 18, 2022, 6:30 PM), https://thehill.com/blogs/congress-blog/technology/598837-cbdc-and-the-fragility-of-a-cashless-society/ ("There are currently over 90 countries worldwide that are examining, developing, or implementing a form of CBDC.").

[5] *Central Bank Digital Currency (CBDC)*, BD. GOV. FED. RSRV. SYS., https://www.federalreserve.gov/central-bank-digital-currency.htm (last updated Apr. 20, 2023).

While the disadvantages of a digital currency are clear for cash-reliant industries like small restaurants, laundromats, and food trucks,[6] the move away from cash carries a threat that the average consumer may not be aware of: financial censorship.[7] Researchers warn that major financial institutions like credit card companies and banks have restricted "legal transactions that may indirectly be associated with criminal acts . . . or extreme opinions," turning the economy's allegedly impartial facilitators into "moral arbiters."[8] Financial censorship has become especially controversial for firearm-related transactions, as gun control activists blame credit card companies for enabling mass shootings.[9] Although certain financial institutions have agreed that they will not restrict transactions for legal firearms,[10] in September 2022, major credit card companies such as American Express, Mastercard, and Visa sided with gun control activists and expressed plans to implement a new merchant code that would track firearm-related transactions with greater precision to "help flag potential mass shooters and gun traffickers."[11] As of March 2023, however, reports circulate that these credit-card companies have paused their implementation of the new sales code due to "concerns about improper tracking of consumer behavior."[12]

This paper will examine how, given the United States' shift toward a cashless economy, the country's top credit-card companies' potential decision to implement a new merchant code for firearm-related transactions as a method of gun control will backfire, jeopardizing consumer privacy and leading to unregulated transactions through

---

[6] Jennifer Taylor, *9 Businesses That Are Still Cash-Only*, GOBANKINGRATES (Apr. 2, 2016), https://www.gobankingrates.com/money/business/9-businesses-still-cash-only/.

[7] *See* Marco Pagani et al., *Financial Censorship Controversy: Financial Services Leading Social Change?*, 20 J. ACCT. & FIN. 101, 101–03 (2020).

[8] *Id.* at 101–02.

[9] *Id.* at 101 (quoting statement of former Democratic presidential candidate Beto O'Rourke: "Credit cards have enabled many of America's mass shootings in the last decade—and with Washington unwilling to act, they need to cut off the sales of weapons of war today.").

[10] *Id.* at 102 (noting Wells Fargo CEO has affirmed his stance against regulating "what product or services Americans can buy").

[11] Ramishah Maruf, *Credit Card Companies Will Adopt New Sales Code for Gun Transactions*, CNN (Sept. 11, 2022, 3:41 PM), https://www.cnn.com/2022/09/11/business/visa-mastercard-american-express-gun-purchase-code/index.html.

[12] Ross Kerber, *Amex, Mastercard, Visa Pause Work on New Firearms Merchant Code*, REUTERS (Mar. 9, 2023), https://www.reuters.com/business/finance/mastercard-pause-work-new-payments-code-firearms-sellers-2023-03-09/.

cryptocurrencies.[13] Since the majority of gun violence stems from firearm transactions not involving credit cards,[14] credit-card companies should abandon the new merchant code that dissuades Americans from exercising their fundamental rights.[15] The American economy should focus on slowing the shift toward a digital economy so that federal and state governments can implement legislation that safeguards privacy rights within the context of new technology.[16] Part I will trace the public policy and market factors that have spurred the global shift toward a digital economy.[17] Part II will dissect federal Fourth Amendment case precedent as it pertains to modern technology and the latest social trends.[18] Part III will analyze various state laws and their insufficiencies in safeguarding privacy rights given new, intrusive technology.[19] Part IV will discuss the International Organization for Standardization's (ISO) new policy and the different privacy concerns that may arise.[20] Part V will highlight the deficiencies in the ISO's new policy.[21] Part VI will outline three methods to slow the United States' shift toward a cashless economy, which will secure additional time for federal and state governments to address concerns for fundamental rights pertaining to digital-payment systems.[22]

## II. THE GLOBAL SHIFT TOWARD A DIGITAL ECONOMY

In the eighteenth and nineteenth centuries, cash's physical limitations spurred popularity for paper checks and letters of credit,[23] and Anglo-Saxon public policy promoted checks over cash.[24] It was not until

---

[13] *See* Mariel Alper & Lauren Glaze, *Source and Use of Firearms Involved in Crimes: Survey of Prison Inmates, 2016*, BUREAU OF JUST. STAT. 1,1 (Jan. 2019), https://bjs.ojp.gov/content/pub/pdf/suficspi16.pdf.

[14] *Id.* at 1 ("Among prisoners who possessed a gun during their offense, 90% did not obtain it from a retail source.").

[15] *See id.*

[16] *See generally id.*

[17] *See supra*, Part I.

[18] *See infra*, Part II.

[19] *See infra*, Part III.

[20] *See infra*, Part IV.

[21] *See infra*, Part V.

[22] *See infra*, Part VI.

[23] Bernardo Bátiz-Lazo et al., *How the Future Shaped the Past: The Case of the Cashless Society*, 15 CAMBRIDGE U. PRESS 103, 108 (2014).

[24] Stephen Quinn & William Roberds, *The Evolution of the Check as a Means of Payment: A Historical Survey*, 93 FED. RSRV. BANK ATLANTA ECON. REV. 1, 4, 7–8 (2008).

the twentieth century that Visa became the first to pioneer "an internationally accepted debit card that would eventually become the main alternative to cash and checks."[25] By 2020, cash represented only "20.5% of global point-of-sale transactions."[26] Experts estimate that this figure will drop to "12.7% by 2024," which means that "more than $2 trillion dollars of cash that was in global circulation in 2020 won't be around in 2024."[27]

Digital-payment systems are easy to implement because market actors instigate the change themselves: mobile-payment providers sell their system to both merchants and consumers, who each play a significant role in the mobile-payment process.[28] Because most merchants and consumers already own and use credit cards for their daily financial transactions, mobile-payment providers turn to credit-card companies "to leverage existing services" toward innovative technology and away from cash-based transactions.[29] However, many consumers might not realize that leading credit-card companies, such as Visa, American Express, and Mastercard, sustain "a complex data-selling ecosystem."[30] These credit-card giants justify their data exploitation as essential for services such as marketing analytics, reward programs, and fraud detection.[31] While there are positives to these practices, such as protection from identity theft, credit card companies are accumulating vast amounts of consumer purchase data at nearly the exact moment a transaction occurs.[32] There are federal laws targeting privacy rights in the context of credit card transactions, but they are not able to keep pace with technological

---

[25] Bátiz-Lazo et al., *supra* note 23, at 123.
[26] Kresse, *supra* note 3.
[27] *Id.*
[28] Chris Jay Hoofnagle et al., *Mobile Payments: Consumer Benefits & New Privacy Concerns*, SSRN 1, 4 (Apr. 24, 2012) (BCLT Research Paper), http://dx.doi.org/10.2139/ssrn.2045580 ("Providers must convince merchants to build infrastructure at the point of sale. To do so, they must persuade enough consumers to adopt mobile payments that merchants find the system profitable.").
[29] *Id.*
[30] Burt Helm, *Credit Card Companies Are Tracking Shoppers Like Never Before: Inside the Next Phase of Surveillance Capitalism*, FAST CO. (May 12, 2020), https://www.fastcompany.com/90490923/credit-card-companies-are-tracking-shoppers-like-never-before-inside-the-next-phase-of-surveillance-capitalism.
[31] *Id.*
[32] *Id.* (detailing that purchase data can be tracked and analyzed "in near real time").

innovation and are, therefore, insufficient to constrain the "spy in your wallet."[33]

Groups at various ends of the political spectrum have become aware of the role that credit card companies play in the data-selling ecosystem.[34] As of recent policy proposals, these groups have paid special attention to how credit card transaction surveillance may impact a person's privacy rights.[35] Left-wing groups maintain that such surveillance enables credit card companies to "identify gun and ammunition sales" and is therefore "a potential tool in combating gun violence."[36] On the other hand, right-wing groups believe that any such financial records will eventually pass to the government, serving as "nothing more than a capitulation to anti-gun politicians and activists bent on eroding the rights of law-abiding Americans one transaction at a time."[37] In addition to tracking individuals whose purchase history might raise concern, right-wing groups fear that such surveillance will create "a national registry of gun owners,"[38] which is federally prohibited.[39]

---

[33] *See* Geoffrey A. Fowler, *The Spy in Your Wallet: Credit Cards Have A Privacy Problem*, WASH. POST (Aug. 26, 2019, 8:00 AM), https://www.washingtonpost.com/technology/2019/08/26/spy-your-wallet-credit-cards-have-privacy-problem/.

[34] Angi Gonzalez & Eden Harris, *Democrats Cheer Credit Card Companies Agreeing to Track Gun Sales*, SPECTRUM NEWS NY1 (Oct. 5, 2022, 5:17 PM), https://www.ny1.com/nyc/all-boroughs/politics/2022/10/05/visa--master-card--american-express--to-comply-with-a-request-to-track-gun-and-ammunition-sales ("Democrats are considering the creation of the new merchant code another triumph, but Republicans call it as a threat to Second Amendment rights, alleging that it opens the door to corporate surveillance.").

[35] Aimee Picchi, *NRA Slams Push to Track Guns Purchased with Credit Cards*, CBS NEWS (Sept. 12, 2022, 2:17 PM), https://www.cbsnews.com/news/nra-credit-card-sales-tracking-gun-purchases-iso/; Gonzalez & Harris, *supra* note 34.

[36] Gonzalez & Harris, *supra* note 34.

[37] Picchi, *supra* note 35.

[38] *Id.*

[39] 18 U.S.C. § 926(a)(3).

## III. UNDERSTANDING THE FOURTH AMENDMENT

### A. *Modern Interpretations*

While the United States Constitution does not explicitly mention the right to privacy, it does protect "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. . . ."[40] The Supreme Court has reasoned that this language, found in the Fourth Amendment, implies a right to privacy.[41] In determining the extent of this right, relying on the Fourth Amendment language proved futile because rapid technological developments broadened the government's surveillance capabilities far beyond what had existed at the time of the Fourth Amendment's ratification.[42] In *Katz v. United States*, the Court finally abandoned its textualist approach and adopted the "reasonable expectation of privacy" test,[43] concluding that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[44] The test, however, does not define what expectations of privacy are reasonable, leaving lower courts guessing and depending on, at most, two Court decisions per year, to set the standard.[45]

---

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

[41] Jed Rubenfeld, *The Right of Privacy*, 102 HARV. L. REV. 737, 745 (1989), https://www.jstor.org/stable/pdf/1341305 (explaining *Griswold v. Connecticut* where "the Court stated that a 'right to privacy' could be discerned in the 'penumbras' of the first, third, fourth, fifth, and ninth amendments.").

[42] Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (admitting that "technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes. . . .").

[43] *See* Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233, 247, 249 (2019), https://repository.law.umich.edu/cgi/viewcontent.cgi?article=3832&context=mlr ("[E]arly cases, although at times conclusory in their reasoning, recognized that Fourth Amendment protections only reached searches of the items enumerated in its text." (alteration in original)); *id.* at 249 ("The *Katz* majority made no effort to connect this new analysis to the constitutional text. . . . proclaiming that 'the Fourth Amendment protects people, not places'. . . . The test became known as the 'reasonable expectation of privacy' test . . . ."); *see* Katz v. United States, 389 U.S. 347 (1967).

[44] Katz v. United States, 389 U.S. 347, 351 (1967) (citation omitted).

[45] Bellin, *supra* note 43, at 236 ("Reasoning by decree in a case or two each year, the Court will label applications of some technologies 'searches,' leave others unrestricted as 'non-searches,' and never opine on the rest. For the vast majority of potential search scenarios . . . lower courts, citizens, and the police will be left guessing about what the Constitution permits."); *see id.* at 251 ("The

As Fourth Amendment cases reached the Court, the Justices began to define the reasonable expectation of privacy as it pertains to daily occurrences.[46] In the 1970s, the Court established the third-party doctrine, stating that a person "does not enjoy a reasonable expectation of privacy when he or she shares information with a third party" because this "person knowingly exposes private information and assumes the risk that it will be revealed."[47] In *United States v. Miller*, the Court articulated that a person subject to the third-party doctrine has disclosed their information "voluntarily."[48] Essentially, the Court has decided "to treat secrecy as a prerequisite for privacy."[49]

Because the Court has not had much opportunity to hear Fourth Amendment cases that grapple with modern technology, lower courts remain uneasy with their decisions that reluctantly apply aged precedent to maintain a balance among federal powers.[50] For example, a 1986 Court decision "upheld warrantless aerial observations of curtilage."[51] Today, that decision inspires lower courts to find that the Fourth Amendment protects law enforcement's ability to use technology "to more efficiently conduct their investigations" in situations where people are neither interacting with the government nor with third parties—in other words, in purely private situations.[52] Lower courts are also bound to find a Fourth

---

privacy we can reasonably expect depends on the privacy the Supreme Court tells us we have.").

[46] Smith v. Maryland, 442 U.S. 735 (1979) (defining the reasonable expectation of privacy for telephonic communications); United States v. Miller, 425 U.S. 435 (1976) (defining the reasonable expectation of privacy for bank records).

[47] Isabelle Canaan, *A Fourth Amendment Loophole?: An Exploration of Privacy and Protection Through the Muslim Pro Case*, 6 COLUM. HUM. RTS. L. REV. ONLINE 95, 100 (2022), https://hrlr.law.columbia.edu/files/2022/03/Canaan-A-Fourth-Amendment-Loophole-3_3_2022.pdf.

[48] *Miller*, 425 U.S. at 442–43.

[49] United States v. Jones, 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring).

[50] United States v. Tuggle, 4 F.4th 505, 526 (7th Cir. 2021) ("[W]e are not without unease about the implications of that surveillance for future cases. The eighteen-month duration of the government's pole camera surveillance—roughly four and twenty times the duration of the data collection in *Carpenter* and *Jones*, respectively—is concerning, even if permissible. . . . Drawing our own line, however, risks violating Supreme Court precedent . . . .").

[51] United States v. Houston, 813 F.3d 282, 288 (6th Cir. 2016) (citing California v. Ciraolo, 476 U.S. 207 (1986)).

[52] *Houston*, 813 F.3d at 288.

Amendment search on occasions where the government is gathering and analyzing personal information to deduce "familial, political, professional, religious, and sexual associations."[53] The difficulty lies in determining what type of personal information would reveal such associations since the Court has already granted government access to arguably private information: a person's Internet search history, call history, and bank records.[54]

In 2020, a Fifth Circuit case grappled with the Court's ambiguity and applied it to the world's first cryptocurrency: Bitcoin.[55] The Fifth Circuit decided that Bitcoin users do not have a Fourth Amendment right in the records of their transactions because Bitcoin transactions are recorded on a publicly accessible blockchain that reveals "the amount of Bitcoin transferred," the "address of the sending party," and the "address of the receiving party."[56] Further, a person's affirmative act to transfer Bitcoin has implied that the person voluntarily shared this information with third parties.[57] Overall, when it comes to technology-based transactions like cryptocurrency transfers, courts have not found a privacy interest because they are still not convinced that such transactions are "a pervasive [or] insistent part of daily life," or that such records provide third parties with "an intimate window into a person's life."[58]

---

[53] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (finding that "[m]apping a cell phone's location over the course of 127 days" enabled the government to infer such information); *Jones*, 565 U.S. 413, 416 (finding that attaching a GPS monitoring device on a person's car revealed such information to the government) (Sotomayor, J., concurring).

[54] RICHARD M. THOMPSON II, CONG. RSCH. SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 1 (2014); *see also Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) ("This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

[55] United States v. Gratkowski, 964 F.3d 307, 311–12 (5th Cir. 2020); Julie Pinkerton, *The History of Bitcoin, the First Cryptocurrency*, U.S. NEWS (Aug. 7, 2023), https://money.usnews.com/investing/articles/the-history-of-bitcoin.

[56] *Gratkowski*, 964 F.3d at 311–12.

[57] *See id.* ("[T]he voluntariness of the exposure weigh heavily against finding a privacy interest in an individual's information on the Bitcoin blockchain . . . [T]ransferring and receiving Bitcoin requires an 'affirmative act' by the Bitcoin address holder.").

[58] *Id.* at 312 (citing *Carpenter*, 138 S. Ct. at 2220, 2217).

### B. *Implications for a Cashless Society*

Critics of the aged third-party doctrine argue that people engaging with third parties do not always voluntarily convey their information.[59] Responding to *Miller*, these critics maintain that "it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[60] Their perspective reflects the reality of a country turning cashless, for in 2017, cash payments represented only 9% of consumer transactions in the United States.[61] The following year, "[i]ncreasing numbers of merchants and eateries went cashless, credit card companies encouraged even more businesses to exclusively accept electronic payment, and many national banks implemented new policies prohibiting cash deposits into certain personal accounts."[62] When COVID-19 spread across the country, these practices only intensified since both personal decisions to quarantine and government-ordered social distancing practically required people to use digital payment systems.[63] COVID-19 revolutionized the digital economy because it unveiled that many cash-based businesses could successfully transition to digital payment systems, thereby spreading e-commerce to new product categories.[64] At least in the United States, it is safe to say that "[c]ashless

---

[59] THOMPSON, *supra* note 54, at 18, 20.
[60] *Id.* at 18.
[61] Nicole Lindsey, *Privacy Implications and Path Forward of a Cashless Society*, CPO MAG. (Oct. 9, 2017), https://www.cpomagazine.com/data-privacy/privacy-implications-path-forward-cashless-society/ ("[C]ash represents just 9% of the value of all payments made by consumers.").
[62] Tamara Kurtzman, *Cashing Out*, 42 L.A. LAW. 22, 22 (Mar. 2019), https://lalawyer.advanced-pub.com/?issueID=1&pageID=24.
[63] Mar Negreiro, *The Rise of E-commerce and the Cashless Society*, EUR. PARL. RSCH. SERV. 4 (Mar. 2020), https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649341/EPRS_BRI(2020)649341_EN.pdf; *see also E-commerce in the Times of COVID-19*, OECD (Oct. 7, 2020), https://read.oecd-ilibrary.org/view/?ref=137_137212-t0fjgnerdb&title=E-commerce-in-the-time-of-COVID-19 ("Regulatory flexibility in response to the COVID-19 crisis is observable in a number of countries, including the easing of caps on contact-less payments . . . ."); Kim Porter, *What To Do When Cash Isn't Accepted*, AARP (Jan. 11, 2023), https://www.aarp.org/money/budgeting-saving/info-2023/no-cash-accepted-trend.html ("The share of cashless businesses more than doubled from February 2020 to February 2021.").
[64] Negreiro, *supra* note 63, at 4. (reporting that COVID-19 "restrictions are resulting in e-commerce spreading even further to product categories").

payments are the new norm."[65] Thus, any court that currently refuses to recognize the pervasiveness of cashless transactions is ignorant of the economic reality.[66]

There are perceived benefits to a digital economy.[67] Cash management is an expense in itself: financial and environmental.[68] As of 2018, cash management cost 2% of Japan's Gross Domestic Product (GDP) and 3.2% of India's GDP,[69] equating to roughly 100.82 billion USD[70] and 86.46 billion USD,[71] respectively. A great portion of cash management costs are spent on production, which depends on raw materials such as cotton.[72] Cotton cultivation requires toxic pesticides and consumes fresh water, depleting the earth's environment.[73] Furthermore, countries incur transportation costs to bring cash into circulation, as well as expend energy to power ATMs to keep cash in circulation.[74] On top of eliminating expenses, people perceive that cashless economies will "reduce tax avoidance and financial crime, as digital payments are more easily tracked than cash."[75]

---

[65] Lindsey, *supra* note 61.
[66] *Contra* United States v. Gratkowski, 964 F.3d 307, 312 (5th Cir. 2020) (holding that cryptocurrency transactions are not a pervasive part of daily life and do not reveal intimate facts about a person).
[67] Manibog & Alvarez, *infra* note 68, at 11.
[68] *See* S. Rochemont, *An Addendum to a Cashless Society - Benefits, Risks and Issues (2018 Addendum)*, 21 INST. & FAC. OF ACTUARIES 11 (Oct. 2018), https://www.actuaries.org.uk/system/files/field/document/Issue%2021-%20Environmental%20Sustainability%20of%20a%20Cashless%20Society%20-%20disc.pdf (highlighting the cost of maintaining cash in various countries, as well as the depletion of natural resources during cash production); Syralyn Manibog & Ma Teresa S. Alvarez, *Perceived Benefits, Problems, and Challenges Towards Cashless Financial Transactions*, 7 GLOB. RSCH. & DEV. J. FOR ENG'G 8, 11 (2022) (reporting that a cashless economy will reduce "[t]he cost of printing and transporting the currency notes to all over the country" (alteration in original)).
[69] Rochemont, *supra* note 68.
[70] *Japan GDP 1960-2023*, MACROTRENDS, https://www.macrotrends.net/countries/JPN/japan/gdp-gross-domestic-product (last updated 2023). In 2018, Japan reported a GDP worth 5.037 trillion USD. *Id.*
[71] *India GDP 1960-2023*, MACROTRENDS, https://www.macrotrends.net/countries/IND/india/gdp-gross-domestic-product (last updated 2023). In 2018, India reported a GDP worth 2.702 trillion USD. *Id.*
[72] Rochemont, *supra* note 68, at 11.
[73] *Id.*
[74] *Id.* at 26.
[75] *The Cashless Society: What It Means for Merchants*, DISCOVER (Sept. 28, 2022), https://insights.discoverglobalnetwork.com/global-trends/cashless-

Although there might be benefits in moving toward a digital economy, experts raise genuine concerns.[76] People whose identities are stolen may lose their purchasing power until their financial institutions resolve the problem.[77] For example, QR codes—enabling peer-to-peer, instant digital funds transfer—"[c]ould be compromised by hacking or simply sticking [a] fraudulent QR code on top of [a] genuine one."[78] In addition to new methods for privacy intrusions, "[b]anks remain inaccessible in many developing countries,"[79] implying a global socioeconomic divide if accessibility does not improve before the world fully adopts digital currencies.[80] Conversely, consumers should remain vigilant in countries with greater bank accessibility because such states might aim to attain a cashless economy to implement a digital authoritarian regime.[81]

Despite the trends, most Americans oppose a cashless society.[82] While Americans may understand the importance of "eradicating

---

society-and-what-it-means-for-merchants; *see also* Manibog & Alvarez, *supra* note 68, at 11 (suggesting that a cashless system will curb corruption, money laundering, tax evasion, and other illegal activity).

[76] Rochemont, *supra* note 68, at 6 (listing concerns such as privacy intrusions, hidden agendas, economic exclusion, and totalitarian regimes).

[77] Discover, *supra* note 75.

[78] *Decoding QR Codes: Are They Useful for Merchant Payments in Emerging Markets?*, GSMA (Apr. 24, 2017), https://www.gsma.com/mobilefordevelopment/blog/decoding-qr-codes-are-they-useful-for-merchant-payments-in-emerging-markets/.

[79] Rochemont, *supra* note 68, at 27 (alteration in original); *see also* DISCOVER, *supra* note 75 (noting "barriers to access for the unbanked" as one of the "important drawbacks that could come with eliminating cash altogether").

[80] *See id.*

[81] Laverty, *supra* note 4 (discussing China's plan, currently in development, to issue a "digital currency" that "would be linked to a social credit score that gives the Chinese government instant knowledge and control over its citizens' finances" (alteration in original)); *see also id.* (recounting when "Canadian Prime Minister Justin Trudeau froze the bank accounts of protesters" in order "to squash the voices of those who disagree with his preferred policies").

[82] *See* Sarah Feldman, *Americans Don't Buy into a Cashless World*, STATISTA, (Apr. 9, 2019), https://www.statista.com/chart/17667/support-of-cashless-payments-united-states/ (reporting that "[n]early two-thirds of Americans were against a cashless society"); Bill Hardekopf, *Is a Cashless Society Good for America?*, FORBES (Feb. 24, 2020),

counterfeiters, suppressing illegal markets, and curbing tax evasion,"[83] these concerns are not their priority.[84] A bipartisan majority recognizes fundamental rights and expresses the strongest support for rights currently in jeopardy, such as the right to privacy of personal data.[85] Cash remains popular because its "peer-to-peer, permissionless, and privacy-preserving" qualities further the all-American concern for preserving privacy rights.[86] Americans also prioritize their freedom of speech,[87] and anonymity in communications and transactions is important to reduce any chilling effect on speech because it enables people to shop at or donate to merchants representing controversial causes.[88] For example, in 2010, after the United States government condemned WikiLeaks for releasing confidential government information to the public, Visa and Mastercard stopped processing all Wikileaks donations, depleting most of the organization's donation-based funding.[89] In 2014, when the United States Department of Justice carried out Operation Choke Point, Americans saw that their right to privacy in financial transactions impacts their right to bear arms and

---

https://www.forbes.com/sites/billhardekopf/2020/02/24/is-a-cashless-society-good-for-america/ (noting that "82% of Americans still carry cash").

[83] Domagoj Sajter, *Privacy, Identity, and the Perils of the Cashless Society in* CULTURE, SOCIETY, IDENTITY - EUROPEAN REALITIES, (Mar. 20, 2013), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285438.

[84] *Reimagining Rights and Responsibilities in the United States*, CARR CTR. FOR HUM. RTS. POL'Y [hereinafter *Reimagining Rights*], https://carrcenter.hks.harvard.edu/reimagining-rights-responsibilities-united-states (last visited Sept. 23, 2023). Americans prioritize their right to privacy of personal data over "eradicating counterfeiters, suppressing illegal markets, and curbing tax evasion." *Id.*

[85] *Id.* (noting that national surveys estimate that a bipartisan majority of 93% of Americans considers the right to privacy of personal data an important right).

[86] Jerry Brito, *The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society*, COIN CTR. REP. 4 (Feb. 2019), https://www.coincenter.org/app/uploads/2020/05/the-case-for-electronic-cash-coin-center.pdf.

[87] *See Reimagining Rights*, *supra* note 84 (displaying that an average of 94% of Americans believe freedom of speech is one of the "essential rights important to being an American today").

[88] *See* Sajter, *supra* note 83, at 5 ("Anonymity reinforces pluralism of thoughts, opinions and behaviors in the society . . . . Possibility of identity exposure would probably reduce funding for peculiar, provocative, contentious and disputatious ideas, persons and organizations." (footnote omitted)).

[89] Michael Holden, *WikiLeaks Says "Blockade" Threatens Its Existence*, REUTERS (Oct. 24, 2011), https://www.reuters.com/article/us-britain-wikileaks/wikileaks-says-blockade-threatens-its-existence-idUSTRE79N46K20111024 ("In the 24 hours before credit card donations were blocked, the organization said it had received $135,000. Now, it is receiving on average about 7,000 euros ($9,700) a month.").

their right to free expression.[90] During Operation Choke Point, the government targeted legal sectors—such as ammunition sales, escort services, and allegedly racist materials—by "choking off financial services to [these] legal industries."[91]

## IV. STATE SHORTCOMINGS IN A CASHLESS SOCIETY

While Supreme Court precedent and the cashless trend threaten privacy interests in a technology-dependent America, the "right to be let alone" falls largely upon the states.[92] Federal statutes implicating privacy rights have stipulated that their reach "does not preempt state law."[93] As of 2022, eleven state constitutions have incorporated provisions targeting the right to privacy.[94] In addition to constitutional amendments, state statutes have provided a legislative defense against privacy intrusions.[95] Some of the most recent U.S. statutes are the California Consumer Privacy Act and the Colorado Privacy Act, both of which target data privacy intrusions.[96] California and Colorado successfully implemented legislation targeting data privacy because their drafters emphasized that basic privacy

---

[90] Todd Zywicki, *"Operation Choke Point"*, THE WASH. POST (May 24, 2014, 2:17 PM), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/24/operation-choke-point/.
[91] *Id.*
[92] THOMPSON, *supra* note 54, at 6.
[93] Stephanie A. Kuhlmann, *Do Not Track Me Online: The Logistical Struggles over the Right "To Be Let Alone" Online*, 22 DEPAUL J. ART, TECH., & INTELL. PROP. L. 229, 254 (2011).
[94] Becky Sullivan, *With Roe Overturned, State Constitutions Are Now at the Center of the Abortion Fight*, NPR (June 29, 2022, 5:00 AM), https://www.npr.org/2022/06/29/1108251712/roe-v-wade-abortion-ruling-state-constitutions.
[95] Robert S. Peck, *The Right to Be Left Alone*, 15 HUM. RTS. 27, 28 (1987) ("New York and Wisconsin have gone the statutory route to recognize the right of privacy.").
[96] Margot E. Kaminski, *The Case for Data Privacy Rights (or 'Please, a Little Optimism')*, 97 NOTRE DAME L. REV. REFLECTION 385, 395 (2022), https://scholar.law.colorado.edu/faculty-articles/1556. The California Consumer Privacy Act and Colorado Privacy Act both recognize that the United States is currently living in the "data analytics age" and that it is necessary to update legislation to address modern concerns. *Id.*

rights were already embedded within their respective state constitutions years prior.[97]

Nonetheless, even if additional states amended their constitutions and passed legislation securing data privacy, they might face the same hurdle as states that have already passed such legislation: current state privacy laws fail to keep up with technological advancement.[98] For example, the New York Civil Rights Law requires that any "violation of right of privacy must occur within the state of New York, regardless of where the plaintiff or defendant resides."[99] New York's outdated provisions ignore the arguably boundaryless cyberspace and the various forms of e-money technology that come with it.[100] Instead, states should draft two sets of laws to craft "a legally significant border" that will address privacy intrusions in two legitimate realms: the physical world and cyberspace.[101] Furthermore, many state courts adopt a theory similar to the

---

[97] *Id.* Other states might not be successful in passing similar statutes because their constitutions are not embedded with a right to privacy. *Id.* (highlighting that both Acts are "framed by preambles touting the existence of a privacy right in each respective state constitution").

[98] Kuhlmann, *supra* note 93, at 257 ("The abundance of privacy-related proposed legislation currently in Congress suggests that 'a consensus has formed in Washington that the patchwork of federal and state privacy laws have not kept pace with the development of the Internet.'") (quoting Sara Forden, *Online Privacy: Can the U.S. Get Its Act Together?*, BLOOMBERG BUSINESSWEEK (May 12, 2011, 2:00 PM), https://www.bloomberg.com/news/articles/2011-05-12/online-privacy-can-the-u-dot-s-dot-get-its-act-together?embedded-checkout=true.)

[99] *New York Right of Privacy Has Its Limits*, RODRIQUES L., https://rodriqueslaw.com/blog/new-york-right-privacy-has-its-limits/ (last visited Jan. 4, 2023).

[100] David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1370 (1996) ("Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location. The rise of the global computer network is destroying the link between geographical location and: (1) the *power* of local governments to assert control over online behavior; (2) the *effects* of online behavior on individuals or things; (3) the *legitimacy* of a local sovereign's efforts to regulate global phenomena; and (4) the ability of physical location to give *notice* of which sets of rules apply."); John D. Muller, *Selected Developments in the Law of Cyberspace Payments*, 54 AM. BAR ASS'N. BUS. L. 403, 420 (1998) ("Current e-money technology is capable of delivering products with varying effects on privacy, ranging from fully anonymous, cash-like systems, in which no personally identifiable transaction records are created, to fully auditable systems that can identify and store every transaction conducted by every consumer.").

[101] Johnson & Post, *supra* note 100, at 1378.

Court's *Miller* decision,[102] and maintain that "privacy rights do not exist in voluntarily disclosed information unless the relationship is fiduciary in nature, or maintains confidential characteristics, such as medical information."[103] Given the arguments presented in Part I, such reasoning is outdated because today's America depends on technology and practically requires people to share their personal information with third parties if they wish to participate in the average American lifestyle.[104] Only two states, Michigan and Missouri, have addressed Information Age privacy challenges by providing constitutional protections specifically for electronic communications and data.[105] Even the California Song-Beverly Credit Card Act, "which prohibits merchants from requesting personal information at the register when a consumer pays with a credit card," does not protect consumers from credit card companies that process detailed transaction information.[106]

States face another obstacle within the privacy law sector, depending not only on whether a case falls under the jurisdiction of a federal or state court but also on what level of federal or state court.[107] Although certain states might afford their citizens greater privacy protections than the Constitution,[108] these safeguards are not always valid in federal courts.[109] As mentioned earlier, only select federal statutes

---

[102] *See* United States v. Miller, 425 U.S. 435, 443 (1976).
[103] Kuhlmann, *supra* note 93, at 233.
[104] *See* Lindsey, *supra* note 61 ("Who pays their rent with cash? In fact, who even pays for a coffee from the local Starbucks with cash anymore? Cashless payments are the new norm.").
[105] Jonathan S. Feld & Andrew T. VanEgmond, *Michigan Voters Add Constitutional Protections for Electronic Data and Communications*, DYKEMA (Nov. 12, 2020), https://www.thefirewall-blog.com/2020/11/michigan-voters-add-constitutional-protections-for-electronic-data-and-communications/; Becca Stanek, *Missouri Passes Constitutional Amendment to Protect Electronic Privacy*, TIME (Aug. 6, 2014, 6:41 PM), https://time.com/3087608/missouri-electronic-privacy-amendment/.
[106] Hoofnagle et al., *supra* note 28, at 2 (alteration in original).
[107] Riley M. Wavra, *State Constitutional Rights Be Damned: Reconsidering the Indifference to State Constitutional Violations in Federal Criminal Proceedings*, 82 MONT. L. REV. 237, 238 (2021) ("[T]hese heightened protections evaporate when evidence procured by state or local officials only finds its way into a federal courthouse.").
[108] *Id.*
[109] Federal statutes can preempt state statutes. Peter Swire, *US Federal Privacy Preemption Part 1: History of Federal Preemption of Stricter State Laws*, IAPP

regulating privacy law explicitly state that they do not preempt state law.[110] Aside from these select statutes, preemption is a common occurrence.[111] Preempting stricter privacy legislation preserves a relatively uniform law throughout the country, avoiding "a 'patchwork' of state laws" that make it difficult for Americans to operate within an industry across state lines.[112] Despite the federal government's commonly exercised preemption power, research indicates that "state privacy law innovation has often been an important step toward eventual federal privacy protections."[113]

## V. THE ISO'S NEW POLICY AND PRIVACY CONCERNS

After Operation Choke Point, it became clear that credit card transactions are key to intrusive government surveillance.[114] For example, extensive credit card surveillance will likely impose a chilling effect on expression promoting minority views,[115] since "donating privately to a sensitive political cause could become near-impossible."[116] Anonymity is essential to a democratic society because it protects people who wish to express unpopular opinions without damaging their reputations.[117] It is absolutely crucial for issues like gun control—one of the most controversial topics in the United States.[118] Second Amendment activists

---

(Jan. 9, 2019), https://iapp.org/news/a/us-federal-privacy-preemption-part-1-history-of-federal-preemption-of-stricter-state-laws/.

[110] Kuhlmann, *supra* note 93, at 254.

[111] Swire, *supra* note 109 (noting that "[p]ractical politics is probably the best explanation for the increasing use of preemption over time").

[112] *Id.*

[113] *Id.*

[114] *See* Zywicki, *supra* note 90 ("[T]hrough strangling the providers of financial services to the targeted industries, the government can 'choke off' the oxygen (money) needed for these industries to survive. Without an ability to process payments, the businesses—especially online vendors—cannot survive."); Lindsey, *supra* note 61 ("Since most e-transactions eventually flow through one of several choke points–Visa, MasterCard, and PayPal–it's theoretically possible to choke off certain unwanted activity simply by making it impossible for businesses or individuals to use those payment platforms.").

[115] Kaminski, *supra* note 96, at 396.

[116] Amber Baldet, *The Currency of the Future Is Personal Data*, QUARTZ (Sept. 25, 2018), https://qz.com/1381355/the-currency-of-the-future-is-personal-data.

[117] *See* Sajter, *supra* note 83, at 5 ("Anonymity reinforces pluralism of thoughts, opinions and behaviors in the society, as many people rely on it when they finance and contribute to unpopular and/or controversial projects, activities, and NGOs. Possibility of identity exposure would probably reduce funding for peculiar, provocative, contentious and disputatious ideas, persons and organizations.").

[118] *See* Katherine Schaeffer, *Key Facts About Americans and Guns*, PEW RSCH. CTR. (Sept. 13, 2023), https://www.pewresearch.org/short-

have argued that credit card companies' potential implementation of a new merchant code for firearm-related transactions "would unfairly surveil legal gun purchases."[119] Activists for other causes, such as abortion rights, have also expressed privacy concerns, noting that "[w]ith abortion bans enacted in more than a dozen states . . . credit card histories could become evidence in abortion-related prosecutions."[120] Overall, there remains a disconnect between individual rights and data privacy laws.[121]

The International Organization for Standardization (ISO)— "an independent, non-governmental international organization with a membership of 169 national standards bodies"— implemented a new merchant code on September 9, 2022, prior to which "gun store sales were classified under a general merchandise or sporting goods category."[122] If America's major credit card companies enact the new merchant code, their consumer transaction records will "separately categorize sales at gun and ammunition stores."[123] Even though providers such as Visa, Mastercard, and American Express paused operations to implement the code, they previously divulged their intent to adopt the new code and have not since indicated any possibility of abandoning that plan.[124] Given recent progress

---

reads/2023/09/13/key-facts-about-americans-and-guns/; *see also* Brian Duignan, *Gun Control in the U.S.*, BRITANNICA, https://www.britannica.com/story/gun-control-in-the-us (last visited Jan. 4, 2023) ("Nowhere in the world is gun control more controversial than in the United States….").

[119] Maruf, *supra* note 11.

[120] Becky Sullivan, *A New Credit Card Code is a First Step Toward Preventing Gun Violence, Advocates Say*, NPR (Sept. 25, 2022, 11:34 AM), https://www.npr.org/2022/09/15/1123059843/credit-card-code-gun-sales-visa-mastercard-american-exrpess.

[121] Kaminski, *supra* note 96, at 386 ("Individual rights are not sufficient by themselves, but they are necessary for data privacy. . . . We give up on individual rights at our peril. It's not clear data privacy laws will be enacted, or succeed at regulating, without them.").

[122] *About Us*, ISO, https://www.iso.org/about-us.html (last visited Sept. 20, 2023); Maruf, *supra* note 11 (citing *Merchant Category Codes*, CITIBANK 8 (2015), https://www.citibank.com/tts/solutions/commercial-cards/assets/docs/govt/Merchant-Category-Codes.pdf); *see also* Sullivan, *supra* note 120 ("[F]or years, gun shops have been categorized as miscellaneous retail or sporting goods stores."); *Description for 5941: Sporting Goods Stores and Bicycle Shops*, U.S. DEP'T LAB., https://www.osha.gov/sic-manual/5941 (last visited Nov. 18, 2022).

[123] Maruf, *supra* note 11.

[124] Kerber, *supra* note 12; Sullivan, *supra* note 120.

toward a digital economy, coupled with the fact that the largest credit card companies in America have expressed support for the new code, some fear the new policy could create "a national registry of gun owners."[125] These fears are not entirely irrational considering the breadth of consumer data generated across these three companies: in 2019, Visa took the lead with 185.5 billion credit card transactions, while Mastercard recorded 108.4 billion and American Express recorded 8.8 billion.[126] Moreover, data processing naturally raises consumer concerns, even if consumers consented to the data processing, because "[i]nformation could be used out of context," "in ways that fail to comport with social values," or to "enable manipulation and even violence."[127]

Privacy concerns may also arise when Americans begin to consider societies that have already adopted a system that allows for digital transaction tracing.[128] For instance, China's transaction tracing could jeopardize organizations that champion freedom and democracy, or advocate for disruptive protests.[129] Given the risks, it is arguable that "a cashless society can only be achieved if privacy concerns are ignored."[130]

## VI. DEFICIENCIES IN THE ISO'S NEW POLICY

Proponents of the ISO's new policy claim that it will mitigate gun violence because "electronic payments were used to purchase the guns and ammunition used in some of the country's most lethal mass shootings, including in Aurora, Colorado, San Bernardino, California, Orlando, Florida and Las Vegas."[131] In fact, left-leaning entities such as Amalgamated Bank, Senator Elizabeth Warren, and New York City

---

[125] *See* Maruf, *supra* note 11. Enabling financial institutions to track firearm related transactions with greater precision will generate data that targets gun-owners. *See id.*

[126] John Taskinsoy, *A Move Towards a Cashless Society Accelerates with the Novel Coronavirus Induced Global Lockdown,* SSRN 1, 20-21 (Dec.12, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3747750 (citing *Global Network Cards in 2019,* NILSON REPORT (June 2020), https://nilsonreport.com/publication_chart_and_graphs_archive.php?1=1&year=2020).

[127] Kaminski, *supra* note 96, at 387.

[128] *See* Lindsey, *supra* note 61 (mentioning "societies such as China, where it is even easier to crack down on any online transactions deemed to pose a threat to the state").

[129] *Id.*

[130] *Id.*

[131] Maruf, *supra* note 11.

Mayor Eric Adams "pressured the ISO to implement the code."[132] These entities might not have been entirely misguided in their aims, for the "Hunting equipment" merchant code makes up the largest share of marketable businesses in the United States within the "Sporting Goods and Bicycle Shops" merchant code.[133] By implementing an additional category code for gun and ammunition stores, the new policy could generate even more effective law enforcement by using existing technology to identify the transacting parties.[134]

Nonetheless, the policy may not be targeting the right type of consumer, for one study reports that "(less than 2%) of all prisoners had obtained a firearm from a retail source and possessed, carried, or used it during the offense for which they were imprisoned."[135] Furthermore, "[l]awful gun owners commit less than one in five gun crimes in America, and of 893 guns from crime scenes in 2008, eight of ten perpetrators were not legal gun owners."[136] On the other hand, "prisoners who had possessed

---

[132] *Id.*; Jeffery C. Mays, *Adams Endorses Primary Candidates, Hoping to Defeat Left-Wing Democrats*, N.Y. TIMES (Aug. 20, 2022), https://www.nytimes.com/2022/08/20/nyregion/eric-adams-endorsements.html (confirming that Eric Adams identifies as a Democrat); Tucker Higgins & Dan Mangan, *Elizabeth Warren Drops Out of 2020 Presidential Race After Disappointing Super Tuesday Showing*, CNBC (Mar. 5, 2020), https://www.cnbc.com/2020/03/05/elizabeth-warren-drops-out-of-presidential-race.html (confirming that Elizabeth Warren identifies as a Democrat); *Labor of Love*, AMALGAMATED BANK (Oct. 21, 2019), https://www.amalgamatedbank.com/news/labor-of-love ("The campaigns of the top five Democratic presidential candidates in mid September — former Vice President Joe Biden, Senators Bernie Sanders, Elizabeth Warren and Kamala Harris, and South Bend, Indiana, Mayor Pete Buttigieg — all bank with Amalgamated. . . . Amalgamated's left-of-center client base and support for progressive causes cuts against the grain of an industry that tends to be politically conservative.").

[133] *Industry: 5941—Sporting Goods Stores and Bicycle Shops*, NAICS ASS'N, https://www.naics.com/sic-industry-description/?code=5941 (last visited Sept. 19, 2023) (reporting that there are 17,683 marketable businesses in the United States for hunting equipment).

[134] *See* Sajter, *supra* note 83, at 5 (highlighting that "[c]ashless payments can be traced, since all e- and m-payments leave digital trails" and, therefore, "[i]dentity of the transaction parties could be revealed, and with it anonymity and privacy of the participants would be lost, which would lead to more effective law enforcement").

[135] Alper & Glaze, *supra* note 13.

[136] *See* Matt Ledder, *Blockchain for Gun Safety*, GEO. UNIV. LIBR. 1,18 (2019).

a firearm during the offense for which they were serving time" most commonly obtained their firearm off-the-street or through the underground market, while the next most common source was another person.[137] Another study, targeting national firearms purchases in 2015, "found that only about half of guns are purchased at retailers," while the other half are bought "from family members or friends, from private sales online, or at gun shows."[138] Firearms purchased at gun shows or through illicit markets are consumer-to-consumer sales,[139] which means third parties are not necessarily involved and, if they are, the transaction record may not reveal the type of item purchased. Thus, it is unclear what impact, if any, the ISO's policy will have on gun violence.[140] Researchers have also noted a link between poverty and gun violence: gun violence increases as poverty rates increase.[141] Since some states have already banned mandates for cashless commerce to protect their poverty-ridden residents,[142] the ISO's new policy will fail to account for these segments of society that are most likely to apply their firearms toward a violent purpose.[143]

The ISO's new policy may also simply transfer people wishing to evade surveillance from one form of digital payment to another.[144] For instance, one study comparing two types of Dark Web firearms vendors—ones operating through shops and others through cryptomarkets—found

---

[137] Alper & Glaze, *supra* note 13, at 7.
[138] Sullivan, *supra* note 120.
[139] Thomas J. Holt & Jin Ree Lee, *A Crime Script Model of Dark Web Firearms Purchasing*, AM. J. CRIM. JUST. 2 (2022).
[140] Sullivan, *supra* note 120 ("[E]xperts say it's unclear what impact the new policy will actually have, if any, on gun violence.").
[141] *See* David Noonan, *Gun Homicide Linked to Poor Social Mobility*, SCI. AM. (Dec. 17, 2019), https://www.scientificamerican.com/article/gun-homicide-linked-to-poor-social-mobility/ (discussing one study that "found that 'increases in the neighborhood percentages of residents in poverty' were associated with a 27 percent higher rate of gun homicides"); Algernon Austin, *Poverty Correlates with the Recent Increase in Gun Violence*, CTR. FOR ECON. & POL'Y RSCH. (Sept. 26, 2022), https://cepr.net/poverty-correlates-with-the-recent-increase-in-gun-violence/.
[142] John Taskinsoy, *A Move Towards a Cashless Society Accelerates with the Novel Coronavirus Induced Global Lockdown*, SSRN 24 (Dec. 15, 2020), http://dx.doi.org/10.2139/ssrn.3747750 (noting that "some U.S. states have banned cashless commerce in order to protect low-income, unbanked and underbanked residents").
[143] *See* Noonan, *supra* 141.
[144] *See* Lindsey, *supra* note 61 (stating that cryptocurrencies "would theoretically help individuals evade government oversight of their transactions and restore privacy to their online activities").

that both required payments through cryptocurrency.[145] Furthermore, certain cryptocurrencies, such as Guncoin,[146] are designed to cater to firearm related transactions. Cryptocurrency is ideal for illicit transactions because, unlike credit card transactions, it "completely circumvents the global financial system," eliminating the need for third-party processors like MasterCard.[147] While most cryptocurrency transactions are recorded on a publicly accessible blockchain and thereby government accessible through the third-party doctrine,[148] the ISO's new policy does not yet extend to cryptocurrencies. It is also less likely that such a policy will reach cryptocurrencies in the near future because cryptocurrency designers actively seek "to create a financial instrument that masks user behavior and meta-data which could be inferred to reveal identity."[149] This goal stems from an even more common belief among cryptocurrency designers: freedom, specifically, freedom from governments, banks, and surveillance.[150]

Even if a regulation similar to the ISO's new policy does extend to cryptocurrency, and even though most cryptocurrency transactions are recorded on a publicly accessible blockchain, it is crucial to remember that there are several cryptocurrencies operating entirely without a centralized ledger.[151] Right now, these cryptocurrencies are completely void of third-

---

[145] Holt & Lee, *supra* note 139, at 12.
[146] Prashanta Chandra Panda & Nisarg Jani, *Growth of Cryptocurrency and Illegal Activities*, 5th International Conference on Economic Growth and Sustainable Development: Emerging Trends 14 (2019), https://www.researchgate.net/profile/Nisarg-Jani-2/publication/343229318_Growth_of_Cryptocurrency_and_Illegal_Activities/links/5f1e53d8299bf1720d6801cf/Growth-of-Cryptocurrency-and-Illegal-Activities.pdf.
[147] *See* Lindsey, *supra* note 61.
[148] United States v. Gratkowski, 964 F.3d 307, 311–12 (5th Cir. 2020).
[149] John Harvey & Ines Branco-Illodo, *Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in "Privacy Coin" Whitepapers*, 19 J. POL. MKTG. 107, 116 (2020).
[150] *Id.* at 121.
[151] *Privacy is Not a Currency*, IOTA FOUND. BLOG (Feb. 5, 2018), https://blog.iota.org/privacy-is-not-a-currency-63018fc45920/ ("IOTA provides data protection by default and by design, it relies on a trustless model. . . . [a] decentralized model of a distributed ledger. The man in the middle is replaced by mathematical computations, executed and validated in a nash equilibria of connected machines. IOTA brings a step closer to life with true digital identity in which the user is the principal owner. The central authority that keeps track

party involvement.[152] In applying a completely decentralized model, such cryptocurrencies protect privacy interests from the third-party doctrine's reach.[153] In fact, IOTA's cofounder David Sønstebø is so confident about his blockchain-free cryptocurrency that he maintains it "can assure the integrity of [the] data by securing it in a tamper-proof decentralized ledger."[154] Gun control activists support blockchain cryptocurrency due to its gun-tracing efficiency.[155] However, at this point, their proposition for a gun-tracing blockchain would track beyond firearm purchases: they propose a system of not only "extensive collaboration with various agencies of the federal government,"[156] but also one that requires each firearm owner to purchase an "electronic gun safe" that would trace "[e]very time a gun is manufactured, sold, or bought," as well as "the transaction from one individual's gun safe to the gun safe of the other individual."[157] Firstly, involving the federal government in such a system would implicate federal prohibitions against a national gun registry.[158] Secondly, such a system would equip the federal government with the third-party doctrine's privileges, since it could be argued that people purchasing firearms through a government-regulated blockchain are voluntarily disclosing their firearm-related transactions to the federal government.[159] Some states have already uncovered the vast potential for

---

and records all activity is obsolete, all activities are stored in the tangle distributed over a multitude of machines. Though transactions are transparent, performing surveillance activities on transactions remains complex and can be difficult.").

[152] *Id.*

[153] Without involvement from a third party, sharing information with a third party does not automatically occur and a person does not assume the risk that their information will be revealed. *See* Canaan, *supra* note 47, at 100.

[154] Mark Orcutt, *A Cryptocurrency Without a Blockchain Has Been Built to Outperform Bitcoin*, MIT TECH. REV. (Dec. 14, 2017), https://www.technologyreview.com/2017/12/14/104996/a-cryptocurrency-without-a-blockchain-has-been-built-to-outperform-bitcoin/.

[155] Matt Ledder, *Blockchain for Gun Safety*, GEO. U. LIBR. 8 (2019) (maintaining that "Implementing Blockchain has the potential to dramatically increase the effectiveness of background checks and gun-tracking").

[156] *Id.* at 13.

[157] *Id.* at 16.

[158] 18 U.S.C. § 926(a)(3).

[159] *See* Ledder, *supra* note 155, at 9; United States v. Gratkowski, 964 F.3d 307, 311-12 (5th Cir. 2020) ("[T]he voluntariness of the exposure weigh heavily against finding a privacy interest in an individual's information on the Bitcoin blockchain . . . [t]ransferring and receiving Bitcoin requires an 'affirmative act' by the Bitcoin address holder.").

privacy intrusions when blockchain technology is applied to gun tracing and thereby banned the use of blockchain technology for this purpose.[160]

## VII. SLOWING THE SHIFT TOWARD A DIGITAL ECONOMY

Even if credit card companies decide to abandon the ISO's new policy, federal and state laws and precedents are not yet equipped to safeguard basic rights and freedoms against modern, intrusive technology.[161] The shift toward a cashless America accelerated in response to health crises, such as the 2014 Ebola epidemic and the 2019 COVID pandemic.[162] Even before these health crises, however, Congress had been overwhelmed with proposed legislation on privacy rights.[163] The volume of this legislation suggests that lawmakers were aware that "federal and state privacy laws have not kept pace with the development of the Internet."[164]

As of January 2023, at least 5.9 million Americans still do not have a bank account.[165] Therefore, imposing a digital economy in the United States at this current moment will pose a major access problem for millions of Americans.[166] One of the most significant pieces of pending legislation to halt the cashless shift is the Payment Choice Act, which would "prohibit retail businesses from refusing cash payments" in certain circumstances, such as when a transaction value is less than $2,000.[167] While the bill already passed in the House of Representatives twice, it still required approval from the Senate before it could become law.[168] For now,

---

[160] *See* Ledder, *supra* note 155, at 20 ("Arizona lawmakers passed a bill banning the use of Blockchain or any other decentralized technology to track firearms").
[161] THOMPSON, *supra* note 54, at 1; *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring); Kuhlmann, *supra* note 93, at 257.
[162] Corey Runkel, *Pandemic Catalyzes Transition to Cashless Benefits*, YALE SCH. MGMT. (Aug. 4, 2020), https://som.yale.edu/blog/pandemic-catalyzes-transition-to-cashless-benefits (noting that mobile payment applications such as Venmo and Cash App provided "CARES Act stimulus payments from the IRS through their apps" for both tax filers and non-tax filers, encouraging citizens to make accounts with these cashless forms of payment).
[163] Kuhlmann, *supra* note 93, at 257.
[164] *Id.*
[165] Porter, *supra* note 63.
[166] *Id.*
[167] Payment Choice Act, H.R. 4395, 117th Cong. (2021).
[168] Scarlett Heinbuch, *What the Payment Choice Act Means for Cash*, FED. RSRV. BANK ATLANTA (Oct. 24, 2022), https://www.atlantafed.org/blogs/take-

federal and state governments could benefit from extra time to develop viable solutions that will protect new technology and fundamental rights simultaneously.[169]

Various businesses, from airlines and hotels to grocery stores and coffee shops, offer loyalty programs[170] "to deter customers from defecting to their competitors."[171] Digital payment providers successfully incorporated these loyalty programs into their services,[172] not only making the transition easier for consumers, but also incentivizing consumers to transition.[173] An incentive based system may also encourage people to revert to cash-based payments.[174] For example, business owners can "offer a discount on cash purchases" or "a small gift at checkout" for cash payments.[175] Because several states have laws against credit card surcharges, it is important to note that cash discounts are still legal in these

---

on-payments/2022/10/24/payment-choice-act-and-what-it-means-for-cash ("The bill passed in the house twice . . . The bill would need to be passed by the Senate to be enacted and we will keep an eye on its progress.").

[169] Julia Griffith, *A Losing Game: The Law Is Struggling to Keep up with Technology*, J. HIGH TECH. L. (Apr. 12, 2019), https://sites.suffolk.edu/jhtl/2019/04/12/a-losing-game-the-law-is-struggling-to-keep-up-with-technology/ ("Technology seems to be advancing at a rate that the law simply cannot keep up with. It has been estimated that the law is at least five years behind developing a technology."); Bellin, *supra* note 43, at 236, 251 ("Reasoning by decree in a case or two each year, the Court will label applications of some technologies 'searches,' leave others unrestricted as 'non-searches,' and . . . lower courts, citizens, and the police will be left guessing about what the Constitution permits . . . The privacy we can reasonably expect depends on the privacy the Supreme Court tells us we have.").

[170] Ibhrahim Zakaria et al., *The Relationship Between Loyalty Program, Customer Satisfaction and Customer Loyalty in Retail Industry: A Case Study*, 129 PROCEDIA - SOC. & BEHAV. SCI. 23, 23 (2014) ("Loyalty programs are frequently referred to as 'points' or 'rewards' programs.").

[171] *Id.*

[172] Porter, *supra* note 63 ("Also note that you don't lose out on rewards points or rebates by using a mobile payment instead of a card; the same benefits apply, based on the account the payment is tied to.").

[173] *Id.*

[174] Joe Craparotta, *3 Ways to Boost Your Bottom Line with Cash Sales*, CURA GRP. (Nov. 13, 2018), https://www.curagroup.com/blog/3-ways-to-boost-your-bottom-line-with-cash-sales (encouraging "customer incentives" as a way to "[m]ake cash sales more desirable to customers.") (alteration in original).

[175] *Id.*

states, as discounts and surcharges produce different effects on the listed price.[176]

Invented in the 1960s, automated teller machines, commonly known as ATMs, have also played a key role in cash circulation by enabling bank customers to instantly withdraw cash.[177] In recent years, ATM use in the United States has declined, partly because of the lack of innovation in the machine since its invention.[178] Redesigning the ATM might play a large part in reinvigorating the use of physical cash.[179] In 2013, Diebold, "one of the world's biggest manufacturers of ATMs," revealed its latest innovation: a small, tablet ATM that "relies on cloud processing to allow customers to use their smartphones to access their cash at ATMs," eliminating the need for a card.[180] Such a device "marr[ies] the mobile to the physical," slowing the transition away from cash.[181] While it was predicted that Diebold's cardless ATM invention would dominate the ATM industry by 2018, COVID-19 disrupted America's financial market and led consumers toward mobile payment processes.[182] Nonetheless, cardless ATM options continue to grow and may curb the trend away from cash.[183]

---

[176] Ben Dwyer, *Cash Discounting for Credit Card Fees: Is it Legal?*, CARDFELLOW (Feb 19, 2023), https://www.cardfellow.com/blog/cash-discount-eliminate-processing-fees/.

[177] John Egan & Mitch Strohm, *ATMs (Automated Teller Machines): What Are They?*, FORBES (Nov. 22, 2021), https://www.forbes.com/advisor/banking/atm-automated-teller-machine/.

[178] Linda Rodriguez McRobbie, *The ATM Is Dead. Long Live the ATM!*, SMITHSONIAN MAG. (Jan. 8, 2015), https://www.smithsonianmag.com/history/atm-dead-long-live-atm-180953838/ (stating that "[t]here is significant evidence that ATM usage is on the decline in North America" (alteration in original)).

[179] *Id.* (maintaining that "ATMS actually offer a lot of opportunity" and that "equipping . . . ATMs with more powers" will unveil this opportunity).

[180] *Id.* (alteration in original).

[181] *Id.* (alteration in original).

[182] Craig Guillot, *The ATM of the Future Will Be Much More Personalized*, FIN. BRAND (Dec. 13, 2021), https://thefinancialbrand.com/news/banking-branch-transformation/atm-of-the-future-more-personalized-itm-mobile-126398/.

[183] *See id.* ("Megabanks like Bank of America and Chase already offer a cardless option at some ATMs, but more widespread adoption continues to grow.").

Lastly, it may be possible to restrain the shift by educating Americans on the advantages and disadvantages of a cashless economy.[184] One of the most influential theories for this argument is the Technology Acceptance Model (TAM), which emerged in the 1980s.[185] The TAM posits that two factors—"[p]erceived [u]sefulness"[186] and "[p]erceived [e]ase of [u]se"[187]—convey how a user perceives a particular technology and determines if the user will accept this technology.[188] Researchers have built on Davis' work, offering "security" as a strong predictor of user technology acceptance.[189] Confidentiality, specifically the assurance that "transactions are protected from possible eavesdroppers[,]" is one of the factors influencing a user's perception of security, and it could be the biggest reason that users refuse digital payment systems.[190] If consumers

---

[184] Bindu K. Nambiar & Kartikeya Bolar, *Factors Influencing Customer Preference of Cardless Technology Over the Card for Cash Withdrawals: An Extended Technology Acceptance Model*, J. FIN. SERV. MKTG. 2 (2022) (highlighting that "[c]ustomer's judgements about the capabilities (such as required knowledge, skill, and self-efficacy) to use [cashless] technology may impact their intentions" (alteration in original)).

[185] *See Fred Davis*, TEX. TECH UNIV. (2023), https://www.depts.ttu.edu/rawlsbusiness/people/faculty/isqs/fred-davis/index.php. Professor Fred D. Davis first proposed the TAM in the 1980s. *See* Nambiar & Bolar, *supra* note 184, at 62. Since Professor Davis introduced the TAM, it "has been extensively used to measure the adoption of various technologies and technology-enabled services." *Id.* In fact, the TAM leads "in explaining users' behavior toward technology[,]" surpassing psychology-based models such as the theory of reasonable action (TRA) and the theory of planned behavior (TPB). Nikola Marangunić & Andrina Granić, *Technology Acceptance Model: A Literature Review from 1986 to 2013*, 14 UNIVERSAL ACCESS INFO. SOC'Y 81, 81 (2015).

[186] *See* PC Lai, *The Literature Review of Technology Adoption Models and Theories for the Novelty Technology*, 14 J. INFO. SYS. & TECH. MGMT. 21, 26 (Apr. 19, 2017) (defining perceived usefulness as the "user's subjective likelihood that the use of a certain system . . . will improve his/her action").

[187] *Id.* (defining perceived ease of use as "the degree to which the potential user expects the target system to be effortless").

[188] Penny Thompson, *Foundations of Educational Technology*, OKLA. ST. U. LIBRARIES 127 (2019), https://shareok.org/bitstream/handle/11244/323771/Foundations-of-Educational-Technology-1556900633._print.pdf?sequence=1&isAllowed=y.

[189] PC Lai, *Design and Security Impact on Consumers' Intention To Use Single Platform E-Payment*, 22 INTERDISC. INFO. SCIS. 111, 113 (2016). Lai's research revolves around consumer willingness to use MySIM, an e-payment platform, showcasing that perceived security is especially relevant in digital payment platforms. *Id.*

[190] *Id.*

learn that the government is able to apply the third-party doctrine to surveil their financial transactions,[191] consumers may not be so willing to accept digital payment methods.[192] Furthermore, if consumers learn that financial institutions, and in turn, the government, can monitor specific transactions—such as firearm-related transactions—with greater precision, consumers might abstain from using digital payment methods for any such transactions.[193]

## VIII. CONCLUSION

While the major credit card companies that wanted to implement the ISO's new merchant code policy have paused operations due to the "legal uncertainty" of such a system, they have "stopped short of saying they would reject the code outright," leaving threats to fundamental rights looming. [194] Governing bodies, like the ISO, frequently implement new technology without evidence-based research that calculates risks and returns.[195] For example, a precise merchant code for firearms-related transactions threatens to unleash personal information in the event of a data breach carried out by private groups or individuals.[196] In turn, people may feel uncomfortable donating to controversial politicians or issues.[197] Furthermore, these major credit card companies incorrectly assumed that people value security over privacy.[198] Compromising privacy rights for a population that is not responsible for the country's increase in gun violence

---

[191] Canaan, *supra* note 47, at 100.
[192] *Id.*
[193] Maruf, *supra* note 11.
[194] Kerber, *supra* note 12.
[195] Hans Vermeersh & Evelien De Pauw, *The Acceptance of New Security Oriented Technologies: A 'Framing' Experiment*, in SURVEILLANCE, PRIVACY AND SECURITY: CITIZENS' PERSPECTIVES 52, 53 (Michael Friedewald et al. eds., 2017).
[196] Lauren I. Labrecque et al., *When Data Security Goes Wrong: Examining the Impact Of Stress, Social Contract Violation, and Data Type on Consumer Coping Responses Following a Data Breach*, 135 J. BUS. RSCH. 559, 563 (2021) (referring to a "recent data breach of a crowdfunding website where donations to support controversial figures including far-right activists were made public, damaging the reputations of many, including public officials").
[197] *Id.*
[198] *Id.*

is not an effective solution.[199] In treating secrecy as a prerequisite for Fourth Amendment privacy protection,[200] the Supreme Court fails to safeguard Americans from government surveillance through modern technology that depends on private information to function.[201] While states play a more active role in shaping privacy law, state legislation has not been able to keep pace with new technology and often mirrors ineffective Supreme Court precedent.[202] These federal and statutory weaknesses raise added concerns as the United States moves to remove paper cash from circulation, leaving a more extensive paper trail for the government to surveil since information shared with a financial institution is deemed "voluntarily" shared and subject to the third-party doctrine's reach.[203]

Overall, extensive surveillance in people's daily undertakings may generate distrust toward the government and threaten American democracy.[204] If major credit card companies reinstate their plans to implement the ISO's new merchant code prematurely, they will be able to track firearm-related transactions with greater precision, empowering themselves with information regarding an area of the market that the

---

[199] Ledder, *supra* note 155, at 7; Susanne Edward, *Why the Bad Guys Are Useful to Gun-Control Groups*, NATIONAL RIFLE ASSOCIATION (Mar. 25, 2024) ("Among prisoners who possessed a firearm when they committed the offense for which they were imprisoned and who reported the source from which they obtained it, the most-common source (43%) was off the street or the underground market. Another 7% of state and 5% of federal prisoners stole the firearm . . . .").

[200] United States v. Jones, 565 U.S. 400, 418 (2012) (Sotomayor, J., concurring).

[201] For example, biometrics technology collects "physiological and behavioral data that allow for precise recognition capabilities," and social media technology gathers "demographics, psychological, geographic, and behavioral data[.]" Sara Quach et al., *Digital Technologies: Tensions in Privacy and Data*, 50 J. ACAD. MKTG. SCI. 1299, 1302 (2022) https://pubmed.ncbi.nlm.nih.gov/35281634/; *see also Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) ("People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.").

[202] *See* Johnson & Post, *supra* note 100, at 1370; Muller, *supra* note 100, at 420; Kuhlmann, *supra* note 93, at 233.

[203] *Miller*, 425 U.S. at 443.

[204] *See* Sajter, *supra* note 83, at 5 ("[T]he notion of constant supervision of all of the citizens' activities indicates vanishing of governments' trust in its own electorate, which is a process that destabilizes the very foundations of the modern society . . . Constantly monitored cashless society, subsequently, could lead to a cycle of distrust between government and citizens, which could have vast consequences.").

government previously deemed to be private.[205] The ISO's new policy will also indirectly endanger the right to bear arms, freedom of expression, and freedom of association, because any support for Second Amendment friendly businesses will be documented on a bank statement and subject to potential government examination.[206]

At the present, it is not certain if these credit card companies will ever implement the more precise merchant code.[207] Furthermore, it is not even certain that these credit card companies will disclose the information they obtain to the government.[208] Nonetheless, given the current state of the law, these companies are legally able to reveal a great deal of information, posing a threat to Americans and their right to privacy.[209]

[205] Sullivan, *supra* note 120 ("[F]or years, gun shops have been categorized as miscellaneous retail or sporting goods stores.").
[206] The third-party doctrine enables the government to access bank records. THOMPSON, *supra* note 54, at 1.
[207] Kerber, *supra* note 12.
[208] The third-party doctrine only enables, and does not require, third parties to share information with the government. THOMPSON, *supra* note 54, at 1.
[209] *Id.*