Distortions in the Market for Privacy & Entrepreneurial Reactions

Walter Smith

Dr. Herbener

ECON 401

4 December 2020

In an article written for *The Atlantic*, journalist and author Franklin Foer laments the way "Big Tech", meaning corporations like Amazon, Google, Facebook, and Apple, have used the CoronaVirus pandemic and economic lockdowns to cozy up to the United States Government. He argues that "partnerships between the state and powerful tech companies must be kept shallow at best."[1] In Foer's opinion, the best way to limit these relationships is to create a Federal Agency that would "scrutinize" information flows and how businesses use personal data. Foer is not alone in wanting more oversight. Years of data breaches, violations, and horror stories have led journalists to call for greater state action – for more regulation and greater oversight of data companies. Journalists are not the sole champions of more state action; ineffective and outdated legislation has even led economists to push for more or better legislation of data privacy in the pages of top economics journals.

Technological progress in data storage and transmission has made it cheaper than even to collect and send data.[2] That progress had led data to be exchanged between different entities at a vaster level and faster rate than at any point in history. Businesses and states obtain and use unprecedented amounts of personal data. However, they do so with different goals and generate very different outcomes. Alongside the development of surveillance goods and in part because of the vastness and rate at which data is recorded and exchanged, privacy-conscious entrepreneurs have developed nascent privacy-enhancing technology, primarily by implementing encryption, in hopes of raising levels of individual privacy. The implementation of encryption to goods, particularly to cryptocurrencies, can be understood as the latest entrepreneurial and market reaction to state intervention, specifically to the unprecedented encroachment of privacy being undertaken by the public-private partnership of corporations with the U.S. government.

---

[1]Foer, Franklin. "What Big Tech Wants Out of the Pandemic." *The Atlantic*, July 2020. Accessed November 3, 2020. https://www.theatlantic.com/magazine/archive/2020/07/big-tech-pandemic-power-grab/612238/

[2]Acquisti, Alessandro, et al, "The Economics of Privacy." *Journal of Economic Literature*, 2016, 451-2.

Privacy and Information Goods

Before examining how the public and private sector partner together to distort markets, an economic account of privacy and information is necessary. Because of the many contexts in which it is applied, formulating a definition of privacy is challenging. In their survey of the literature on economics and privacy, Alessandro Acquisti, Curtis Taylor, Liad Wagman Privacy state "the economics of privacy concerns the trade-offs associated with balancing of public and private spheres between individuals, organizations, and governments."[3] This paper focuses on personal data privacy, which is defined as "the control over and safeguarding of personal information."[4] Personal information is relevant knowledge about a person and their associations.[5] Because personal information is individualistic it is up to the subjective judgment of a person to determine which information is relevant. As such, personal info means different things to different people; it can consist of physical facts like eye color, subjective tastes, and preferences like religious views or sexual preference, or information like transaction history.

Privacy is not an economic good in Mengarin terms – it cannot be bought or sold directly.[6] Rather, the good's bought or sold in the market for privacy are Privacy-Enhancing Technologies (PETs), which protect or secure said information. Professor Peter Klein, in a lecture given at the *Mises Institute*, offers a useful analogy for understanding privacy. Love, like privacy, is not a tangible good that can be bought and sold but an "abstraction". Goods and services can be bought that are related to love or generate love but are not love themselves.[7]

---

[3]Ibid, 443.
[4]Ibid.
[5] Stigler, George J. "An Introduction to Privacy in Economics and Politics." The Journal of Legal Studies, 1980, 624. https://www.jstor.org/stable/724174, 624.
[6]Menger, Carl. *Principles Of Economics*, Auburn, Alabama: The Ludwig Von Mises Institute (2007), 52.
[7]Klein, Peter. "The Economics of Data Privacy." Mises Institute. Lecture. Accessed November 10, 2020. https://mises.org/library/economics-data-privacy-1

When analyzing privacy and information "using economics" what's being analyzed is "specific goods and services … called information goods."

The value of the good, whether it is the information itself or a PET, depends on the circumstances of the information – how useful are the means at satisfying that end and how is that end valued by the person seeking it. Information goods are bought for the information within; PETs are purchased to guard that info from others wanting to access and use it. The information could be a person's eye color or a Social Security Number. A PET could then be a pair of sunglasses or a safe that protects the social security card.[8] Because personal information is individualized, it is mostly up to the individual to initially control what information is available and who it is made available to, at least initially. Economist Kenneth Laudon writes "When individuals claim that information about them (or their own behavior) is private, they generally mean that they do not want this information shared with others, and/or that they would like to control the dissemination of this information."[9]

Like all economic goods, information goods are transacted with. And once the original owner of that good exchanges it (in the case of data, discloses it) they have negligible control and no right over how that good is used. But unlike other goods, such as cars or phones, information is unique. Information goods have second-order effects, meaning information affects the person even after it is sold.[10] If a person sells their car to another person and that person, in turn, sells the car, it has no effect on the original owner. Personal data, once sold, can be used to identify, target, contact, and discriminate against the original owner. And it can be sold again, to another person, without the seller losing that information.[11] While information given to producers does

---

[8]Ibid.
[9]Laudon, Kenneth C, "Markets and Privacy," NYU Faculty Digital Archives (Stern School of Business, New York University, July 1993) 2.
[10]Acquisti, et al, "The Economics", 452.
[11]Ibid, 454.

have obvious benefits – more informed producers and sellers can better meet consumers' prefaces – personal information can also be used in more nefarious ways. Some of the ways states and organizations harm individuals will be detailed later on.

Markets for Information and Privacy Goods:

It is important to note knowledge is generated or exchanged in any transaction, even in fully anonymous auctions. For instance, in any exchange, purchasers reveal they value the good they received more highly than the good they parted with. While some individuals are more privacy-conscious and want to "leak" as little knowledge about themselves as possible, most people do not mind sharing relevant or useful knowledge with producers. Sharing information is beneficial – it allows sellers and buyers to find each other faster, reducing search costs and it can even lower the cost of some goods.[12] Regardless of a person's level of privacy consciousness, whatever knowledge is revealed belongs to the data collector so long as it was received voluntarily and not through coercion, even if the data sharer regrets it post-fact. Intervention is unnecessary so long as "the usual conditions of competition prevail … the efficient amount of information will appear, given the tastes of the parties for knowledge and privacy."[13]

Today, markets for information and for privacy goods exist. In information markets, it is common for individuals to sell their data in exchange for "free" services like access to social media websites like Facebook or search engines like Google. Intermediaries collect, merge, arrange, store, purchase and sell data to other organizations or directly to the government agencies. [14] There are a range of markets for information and a range of markets for privacy goods.[15]

---

[12]Stigler, "An Introduction", 627.
[13]Stigler, "An Introduction", 627.
[14]Ibid, 474.
[15]Ibid, 473.

These markets function incidentally to state regulation or state distribution of property rights over personal information. Economist Eli Noam, employing the Coase theorem, has demonstrated that outcomes in information markets depend not on the initial allocation of rights over the data, but on who values the data more highly, on who is willing to purchase the right.[16] If the person from whom the data is generated is allocated the right the data will only be shared voluntarily if the price offered for the data outbids their valuation of the date. Similarly, the data originators will have to purchase barriers or protection to guard their information if the data collectors are granted the right over the data. Regulation merely determines who pays, either for data or for privacy.[17] Under current U.S. regulation (except for a few small exceptions), data collectors own the information they collect, while individuals only have an "interest" in that information.[18]

Even if they are unaware, individuals ultimately choose how much information they share about themselves initially. Simply by nature, information is initially held with the individual. But because the information is leaked in transactions, individuals wanting to withhold information must pay to do so.[19] Individuals wanting to guard themselves can work to reveal as little information as possible, limiting transactions to only necessary information and purchasing and using PETs to enhance privacy. Or they can make all of their information fully accessible and updated. Most individuals do not seem to mind sharing information – despite numerous studies suggesting "internet users" primary concern online is privacy, consumer behavior suggests otherwise. Data indicates "most consumers remain avid users of information

---

[16]Noam, Eli M. 1997. "Privacy and Self-Regulation: Markets for Electronic Privacy." *In Privacy and Self-Regulation in the Information Age*. Washington, DC: US Department of Commerce, National Tele-communications and Information Administration. Accessed November 24, 2020.https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy.
[17]Ibid, pg.
[18]Laudon, Kenneth C. "Markets and Privacy." Communications of the ACM, 1996, 96.
[19]Acquisti, et al, "The Economics", 446-7.

technologies that track and share their personal information."[20] This may be because restricting access to data initially and revoking control over information once it's released is extremely difficult, especially since most individuals have almost no knowledge of how dispersed their data is. Or it may be because individuals do not mind sharing information if they deem it useful. Whatever the case, most information, once it's out the door and into information markets, is likely gone for good.[21]

Free Market For Privacy

Before looking at state action and market reactions; it is useful to conveive of a free market for information and privacy. Economists have found that because the sharing of information is (initially) an individual choice and context-dependent, social and personal welfare can be both enhanced or reduced by the revealing of information.[22] Letting individuals make decentralized decisions produces more prosperity because data collectors and data sellers have more incentive to meet consumer demand under free markets than centralized ones.

In a free market for privacy, it is feasible to suspect social media companies would face more downward pressure on the amount of data they harvest. Instead of acquiring as much knowledge as possible to sell to both governments and other businesses, data collectors would solely acquire data that is useful to other businesses. One key point that will be expounded upon later is that these other businesses also face profit incentives and work towards consumer satisfaction through voluntary exchange.

Part of user experience is offering better privacy or more control over one's own data; users wanting more privacy opt to transact with more privacy-respecting companies. And companies, in a free market, would compete to offer better privacy; Acquisti, with his co-authors

[20]Acquisti, et al, "The Economics", 476.
[21]Ibid, 448.
[22]Ibid, 463.

writes “with regulation struggling to keep pace, industry competition has been behind both new privacy-enhancing technology and privacy-invasive technologies.”[23] Companies have curtailed their data collection or made consumers more aware of it because of competition and consumer demand for greater privacy and control of data.[24] Business has often and continues to increase privacy not because of the regulation but in spite of it.

Under voluntary exchange, if a consumer is unhappy with how their data is shared or used, they can delete their account, ending their contract with the company. While those companies still own the previous data they collected, users will no longer share new data with those companies. And because they are in a free market, users have the possibility to purchase their data back. Or they could opt to only transact with companies that agree to delete all previous user data if users delete their accounts. While not in existence currently, economists have even conceived of National Information Markets in which data is bought and sold directly for cash.[25] As will be seen below, getting information back and having diverse services options, such as different ads, fewer ads, no ads, is more likely in an elective market where service providers try to meet consumer demand than under political regimes.

State Regulation

As part of the information and privacy markets today, state regulation with respect to privacy, despite not controlling the final outcome of data exchanges, must be considered to clearly grasp how information and privacy markets are distorted. University of Chicago Economist George Stigler, discussing U.S. regulation, writes a “variety of laws” exist which “restrict possession or dissemination of information about individuals, or conversely compel its

[23]Acquisti, et al, "The Economics", 451-2.
[24]Ibid, 484.
[25]Laudon, "Markets", 1996, 100.

dissemination."[26] These laws exist on a "spectrum". On one side of the spectrum "protection of data relies entirely on consumer's marketplace behavior", on the other side "privacy regulation would establish strict default protection of personal data and limitations over its usage."[27] States operate at various points on this spectrum; China, for example, has some of the harshest regulations in the world, which makes individual privacy almost non-existent.[28] The U.S. lies closer to the consumer side of the spectrum, although it will be shone it also has regulations and practices that undermine individual privacy.

The depth and breadth of economic research into regulation of data and privacy are too large to fit into any single paper, and much of it is outside the scope of this paper. However, some research findings are key to understanding state intervention and market reactions.

In "Market and Privacy", Laudon states that in the U.S., privacy law comes from three sources: common law, The Constitution, and Federal and state statutes.[29] Common law protects individuals "against intrusions of other private parties", The Constitution protects against "government instructions into private life", and Federal and state statutes protect "against governmental intrusions and uses of information" and "the use of personal information by private organizations."[30]

Writing in 1996, Laundon argues that "the existing legal approach to privacy in the U.S. – whether common law, Constitutional, or statutory – has many well-known limitations."[31] All three types of laws have proven ineffective. Laudon cites a 1994 study that found "76% of U.S. citizens have lost all control over personal information. Despite "enormous legal armament …

[26]Stigler, "An Introduction", 624.
[27]Acquisti, et al, "The Economics", 453.
[28]Schneier, Data, Chapter 5.
[29]Laudon, "Markets", 1996, 91.
[30]Ibid, 92
[31]Ibid, 94.

most citizens feel their privacy has declined."[32] 24 years later, individuals are even less secure and they feel even less secure – according to Pew Research Center between 81% and 84% of US adults now feel they have little to no control over the data companies and governments collect.[33] Before a solution can be suggested for enhancing privacy, it must be discovered who is responsible for unprecedented surveillance, and what are the economic consequences of the surveillance.

The Who:

In 2015, the American Civil Liberties Union revealed that Michigan police had been using cell phones to track people for almost 10 years.[34] According to Pew Research, 96% of adult American's carry cellular devices.[35] As will be detailed below, Michigan police are hardly alone in observing and tracking their citizens.

U.S. regulation is designed, in name, to protect personal privacy; in reality they "are confusing, piecemeal, and riddled with loopholes", and federal agencies use "legal loopholes" to "widely share personal information within the government" without individual consent or knowledge.[36] Despite assurances that it wants to protect privacy, US action indicates the opposite.

Stigler, in an piece for *The University of Chicago Press*, wrote "Governments (at all levels) are now collecting information of a quantity and in a personal detail unknown in

---

[32]Ibid.
[33]Auxier, Brook, et al. "Americans and Privacy: Concerned, Confused and Feeling a Lack of Control Over Their Personal Information." *Pew Research Center*, November 2019. Accessed November 30, 2020. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/
[34]Kruth, Rebecca. "ACLU: Michigan State Police have been tracking cell phones for years." *Michigan Radio*, October 2015. Accessed November 30, 2020. https://www.michiganradio.org/post/aclu-michigan-state-police-have-been-tracking-cell-phones-years
[35]Pew Research. "Mobile Fact Sheet" *Pew Research Center*. Accessed November 30, 2020. https://www.pewresearch.org/internet/fact-sheet/mobile/
[36]Laudon, "Markets", 1996, 95.

history."[37] Writing in 1980, Stigler's words are more relevant today than when he penned them. At times in history have states gathered more data and no government in history has been as effective at gathering and surveying individuals as The US government.[38] The US government (including Federal, State, and local government) is the largest surveillance state in the World. The FBI has over 640 million photos of US citizens, almost double the population of the US.[39] The government has more data than any corporation.[40] Moreover, the US military is deployed in over 75% of countries around the globe; the number of countries under surveillance is even higher. Estimates on the cost of "intelligence" in the US annually range up to $72 billion.[41] The US government spends more on data collection than any other government or any company.

In his book, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, cryptographer Bruce Schneier details the rise and practices of one infamous agency that has spied on American citizens for years – the National Security Agency or NSA. After the terrorist attacks of September 11, 2001, the NSA moved from spying primarily on foreigners to spying on both foreign and domestic threats at an unprecedented level.[42] Legislation, like Section 15 of 2001's Patriot Act, allowed the NSA to collect tangible things like telephone records for an investigation at an unmatched level.[43]

Surveillance is not just conducted by the NSA – Schneier writes "the US intelligence community is actually composed of 17 different agencies." These agencies in many ways operate

---

[37]Stigler, "An Introduction", 623.
[38]Schneier, Bruce. *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton & Company (2016), Digital, Chapter 5.
[39]Gulian, Neema. "The FBI Has Access to Over 640 Million Photos of US Through its Facial Recognition Technology." *ACLU*, June 2019. Accessed November 30, 2020. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through
[40]Schneier, Data, Chapter 5.
[41]Gulian, "The FBI."
[42]Ibid.
[43]"Section 215 of the Patriot Act." *Electronics Frontier Foundation.* Accessed November 30, 2020. https://www.eff.org/files/2018/11/25/215_one_pager_-_2018.11.pdf

in the dark, spying on individuals without public awareness or judicial oversight.[44] These agencies can collect data directly or indirectly through subpoenas like National Security Letters (NSLs) that force companies to hand over third-party data (i.e. a Google user's emails).[45] The NSA can even track the movements of individuals by accessing their cell phone GPS; in 2009 cell service provider Sprint received over 8 million law enforcement requests for GPS location data alone.[46] And tracking is only getting cheaper. Prior to the cell phones, personal surveillance, which was a primary way tracking was conducted, cost up to $170,000 per month; Sprint charges the NSA just $30 a month per line.[47] Because of the vastness, complexity, and hidden-nature of the agencies that undertake surveillance in the US, it is impossible to know and subsequently measure how much information the U.S. has, what type of data it has, and everything it does with that info. Schneier aptly sums up U.S. surveillance, writing "taken as a whole, there's a great deal of overenthusiastic, ideologically driven surveillance going on in the US."[48]

The Means: The Big Tech and Government Nexus

Governments acquire data in a variety of ways; they use censuses, require citizens to register and use government identification for licenses (i.e. driving), and observe individuals directly with techs like cameras or phone tracking. Laws, such as Know Your Customer Laws (KYC) or tax laws, force individuals, to share an overabundance of information, either directly or indirectly, with both businesses and the state.[49] Regulations, like those passed by the

[44]Schneier, *Data,* Chapter 7.
[45]Ibid.
[46]Bankston, Kevin"Surveillance Shocker: Spring Received 8 million law requests for GPS Data." *Electronics Frontier Foundation*, December 2009. Accessed November 30, 2020. https://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law
[47]Schneier, *Data,* Chapter 5.
[48]Ibid.
[49]Stigler, "An Introduction", 624.

Securities and Exchange Commission (SEC), forces financial institutions to report transactions by their customers that exceed $10,000.[50]

Most importantly for this paper, states obtain information from data aggregators and intermediaries, distorting information markets, and leading to greater investment in both surveillance technology and PETs. The nexus of corporate surveyorship on the state's behalf has been referred to as the "public-private surveillance partnership." In this partnership data, collectors and intermediaries trade personal information for competitive advantages and favors, such as contracts with the NSA, FBI, and other agencies. A *Washington Post* article, relying on documents leaked by former NSA consultant Edward Snowden, found 70% of the intelligence budget went to private companies.[51] This partnership is not only characterized by exchange, but also by a "revolving door" between working at the intelligence agencies and working at heavyweight government contracting companies that aid and embed surveillance. State agencies and private companies continually lobby to make surveillance possible. The FBI has even lobbied for legislation that would make producers build in "eavesdropping capabilities" on "all communications systems" including on videogames.

To better understand this nexus, which is more of "an alliance of interests" than a "formal agreement", it is useful to focus on one particular company.[52] Facebook, founded in February of 2004, is the largest social networking site in the world, with 2.7 billion active users alone.[53] Add-in Facebook-owned social media companies like Instagram, WhatsApp, and Messenger and 3.14 billion active users.[54] Just under 75% of Internet users have Facebook accounts.[55] Like other

---

[50]Ibid, chapter 6
[51]Schneier, *Data,* Chapter 5.
[52]Ibid.
[53] Active meaning the user logged-in within the last 30 days.
[54]J. Clement. "Cumulative Number of Monthly Facebook Users, as of 3rd Quarter 2020." *Statista*, November 2020. Accessed November 20, 2020.https://www.statista.com/statistics/947869/facebook-product-mau/
[55]Ibid.

social networks, Facebook acts "as intermediaries, selling advertising space to advertisements on one end and providing services and products to users on the other."[56] Unfortunately for consumers, other businesses are not the sole purchasers of consumer data.

Beginning in 2009, as part of its PRISM program, the NSA began acquiring data on "persons of interest" from nine Tech companies, including Facebook. Foreigners or U.S. citizens who communicated with people who were "reasonably suspected" of being outside the U.S. were allowed to be targeted[57]; other U.S. citizens' information was still collected (incidentally) and made available easily and openly available to the NSA. In 2013, Facebook was among a group of companies that negotiated with the U.S. government to create digital rooms for state request and retrieval of information. Although Facebook was and is required by the Foreign Intelligence Surveillance Act of 1978 to disclose certain information, Facebook (and the other companies) did not have to make it easier for agencies to do that. Facebook essentially volunteered to make it easier for the state to access that information.[58]

Social media networks like Facebook rely on network effects to fuel growth – more users means more data, more ads to sell, and more connections for their users. Like other companies, if Facebook violates contracts, black-balls users, or fails to meet users preferences in some way it will lose users and die.[59] Businesses, everywhere and in every industry, are constrained by the demands of buyers – social media companies are no different. Luckily for Facebook, it has escaped some of the restraints of consumer preference thanks to its partnership with the state.

---

[56]Acquisti, et al, "The Economics", 458.
[57]Schneier, *Data,* Chapter 6.
[58]Miller, Claire. "Tech Companies Concede to Surveillance Program." *The New York Times*, June 2013. Accessed November 30, 2020. https://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?ref=global-home&_r=1&&pagewanted=all
[59]Consider MySpace: the social media giant was considered a monopoly by many prior to being overtaken by Facebook.

In *Data and Goliath*, Schneir finds that big tech has been able to lobby for and get legislation passed that stifles competition.[60] As Ryan McKaken notes, big corporations have never minded regulation, relying on more capital and economies of scale to survive harsher regimes. Smaller businesses are the ones primarily harmed by regulation – these companies do not have the tools or capital to compete in a more regulated market and go under.[61] In regulated environments, big corporations are able to commit "regulatory capture", passing legislation that stops new competitors from entering, thus letting them dominate the market. In turn, this allows them to meet consumer demands even less. Facebook, since its founding, has pushed and lobbied for more digital regulation. In 2015 Facebook lobbied congress in favor of the Cybersecurity Information Sharing Act (CISA) which effectively encouraged companies to share even more data with the government.[62] Facebook spent more than any other tech company on lobbying in 2019 – spending over $16 million.[63] For instance, in 2019, it agreed to a twenty-year deal with the Federal Trade Commission (FTC) to government oversight.[64] Part of that agreement allows the "FTC to use the discovery tools … to monitor Facebook's compliance."[65] Since that agreement, Facebook Founder and CEO Mark Zuckerberg has continued to be outspoken about the need for more digital regulation.[66]

---

[60] Schneier, *Data,* Chapter 6.
[61]McMaken, Ryan. "Don't Regulate Facebook – That's What Zuckerberg Wants." *Ludwig Von Mises Institute*, April 2018. Accessed November 30, 2020. https://mises.org/wire/dont-regulate-facebook-thats-what-zuckerberg-wants
[62]Bennet, Corry. "Advocates Accuse Facebook of Secretly Lobbying for Cyber Bill." *The Hill*, November 2015. Accessed November 30, 2020. https://thehill.com/policy/cybersecurity/258060-advocate-acuses-facebook-of-secretly-lobbying-for-cyber-bill
[63]Foer, "What."
[64]"FTC imposes 5 billion penalty sweeping new privacy restrictions." *FTC.gov*, June 2019. Accessed November 30, 2020. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions
[65]Ibid.
[66]Macias, Amanda. "Facebook CEO Zuckerberg Calls for More Government Regulation." *CNBC*, February 2020. Accessed November 30, 2020. https://www.cnbc.com/2020/02/15/facebook-ceo-zuckerberg-calls-for-more-government-regulation-online-content.html

Despite outward posturing from legislators and regulators decrying "Big Tech" and calls for anti-trust legislation, the U.S. government is actually subsidizing a large number of US tech companies, including Facebook. Research published by *Tech Query* in July 2020 found " that the Department of Defense and federal law enforcement agencies including Immigration and Customs Enforcement, the FBI, the Drug Enforcement Agency and the Federal Bureau of Prisons, have secured thousands of deals with Google, Amazon, Microsoft, Dell, IBM, Hewlett Packard and even Facebook that have not been previously reported."[67] Former Google Researcher and Math Professor Jack Poulson investigated more than 30 million government contracts.[68] Most of the contracts are subcontracts – a contract where a state agency contracts with a company to contract with another company that would perform the task – which allow "tech companies to work on defense projects" without revealing "their involvement."[69] Because of the vastness of his research and the difficulty of analyzing the contracts, the majority of his research will not be covered here. However, some of his findings are important to the thesis of this paper.

Paulson found that among the big tech companies, only "Facebook, Apple, and Twitter" stayed out of "major military and law enforcement contracts."[70] Facebook, when compared with other companies such as Microsoft, IBM, or Verizon, has a tiny fraction of the contracts and subcontracts that they have. Yet, according to Paulson's research, Facebook still subcontracted with US government agencies 172 times. Again, Paulson's research did not find that Facebook

---

[67]Glasner, April. "Thousand of Contracts Highlight Quiet Ties Between Big Tech and ." *NBC*, July 2020. Accessed November 30, 2020. https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171

[68]Poulson, Jack. "Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated." *TechInquiry*, July 2020. Accessed November 30, 2020. https://techinquiry.org/SiliconValley-Military/#table-3

[69] Glasner, "Thousands."

[70]Poulson, "Report."

contracted with major military and or law enforcement agencies, but they did contract with others, such as the U.S. Agency for Global Media (USAGM).

A Congressional report on Big Tech released in late 2020 revealed that Facebook and other tech companies have mostly skirted around agencies like the Federal Trade Commission (FTC), breaking laws and their word.[71] Since most of the deals and decisions agencies like the FTC make happen behind closed docs, it is difficult to prove if the FTC's failure to enforce the law on Facebook had anything to do with preserving state interests. But Facebook's (and Big Techs) lobbying coupled with the state's interest in acquiring its data and letting it continue to partner with agencies like the USAGM certainly amounts to an economic incentive for agencies like the FTC to give Facebook (or other government partnered companies) more leeway when it comes to the law than other companies. Schneier argues the lack of legislation makes sense; He writes, "governments don't really want to limit their own access to data by crippling the corporate hand that feeds them."[72]

Lastly, it should be noted that Facebook and the PRISM program are hardly unique – "other programs" and partnerships exist that allow the state "to conduct mass surveillance."[73] One outcome of this partnership is the movement of surveillance data between the state and corporations at an unprecedented level. Some market outcomes are presented below.

Market Distortions:

Economist Henry Hazlitt, in his *Economics in One Lesson*, suggests that good economics consists in seeing the unseen – the second-order effects of actions and reactions.[74] The

[71]Ovide, Shira. "Congress Agrees: Big Tech is Broken." *The New York Times*, October 2020. Accessed November 1, 2020. https://www.nytimes.com/2020/10/07/technology/congress-big-tech.html
[72]Schneier, *Data,* Chapter 6.
[73]Ibid.
[74]Hazlitt, Henry. *Economics in One Lesson*. Auburn, Alabama: Ludwig von Mises Institute, 2019.

public-private partnership distorts information and privacy markets in a number of ways, many of them unseen. Below are listed some of the ways relevant to this paper.

1. Data gathering is more costly: the partnership employs different means and gathers different information than what occurs under a free market. This partnership is necessarily more costly as if it was not more costly it would have been readily employed in a free market.[75]
2. More data is gathered than necessary: data gathering is not only conducted in an inefficient manner, but data irrelevant to market operations is gathered. Producers gather more information than deemed necessary, which can be welfare reducing for both individuals and companies.[76]
3. Certain firms lose competitive advantages: firms forced to share data that was costly to acquire with states could lose seller information that benefits competitors at their expense. Firms that do not get government contracts for data are less competitive than firms that get contracts.
4. Increased investment in information markets: with more buyers of the data, abnormal profits are created for companies that collect data, leading to more investment in data collection.
5. Increasing investment and development in PETs: this partnership drives entrepreneurs and individuals to seek out more ways to protect their data. This additional investment drives the public-private state to increase their investment in privacy-invasive tech and even work to pass legislation that makes some types of PETs illegal

[75]Stigler, "An Introduction", 628, 642-3.
[76]Ibid.

6. Decreased investment in other industries: an obvious and natural result of more investment in surveillance and PETs is less investment in other industries, reducing societal wealth, not just the wealth of the individuals involved.
7. Consumer preferences less met: regulation passed to curtail the development of PETs on the state partnered corporations' behalf will stop other companies from successfully competing. As noted above, this lets these corporations shirk consumer wants.

Having examined the effects of this partnership it is time to identify who among the parties – government or business – is chiefly responsible.

Who is at Fault: Big Tech or the State?

Who is at fault for the distortions in privacy and information markets? Stigler notes "If knowledge did not arise out of, and normally get used in, transactions, there would be little in the subject [economics of privacy]."[77] Every business, whether a mom-and-pop, a startup, or a tech giant faces the economic incentives of profit and loss. Huge corporations only make abnormal profits and harvest abnormal amounts of data if the government enables them to become one. In *A History of Money and Banking in the United States* Economist Murray Rothbard writes, "monopoly has always been defined… as 'grant of exclusive privilege' by the government."[78] We have seen how private enterprise has partnered with the state to conduct surveillance in mass; in return, they have been able to dodge legal enforcement, lobby for legislation that stifled competition, obtained government contracts, and obtained abnormal or above market rates of data from users. Or in the words of Rothbard, they have been granted exclusive privileges by the state.

---

[77]Stigler, "An Introduction", 627.
[78]Rothbard, Murray N. *A History of Money and Banking in the United States: the Colonial Era to World War II.* Auburn, Alabama: Ludwig von Mises Institute (2005), 184.

Data collection technology is, like all economic goods, value-neutral. It can be used for ill or for good, for spying, or for better meeting consumer demands. The value of something being used for bad or good is ultimately subjective to the people involved. But, as will be explained below, markets face completely different incentives than states. The market faces incentives that motivate it to satisfy the desire of consumers, what every day voluntarily exchanging perceives as the 'good'.

Unlike business, the government does not face incentives of profit and loss. Instead, government officials want to maximize the goals of individuals or groups within the government, take and hold onto wealth for themselves, and partner with groups outside the government, rent-sharing at the cost of everyone else.[79]

When tech companies collect and trade data they do so in hopes of better meeting customer demand through voluntary exchange. Without a profit to be made they would not do it. There would be no profit if users did not voluntarily transact, revealing their preference for the data collection.

Moreover, if customers are unhappy with the use of their data, for instance with targeted advertising or spamming, companies are much more likely to evolve than states. Almost all websites have ad removal. Facebook even enables users to tell them why they did not like a specific ad and dictate which ones they want.

Now, consider how things change when coercion is involved. States buy, collect, and legally compel data from people and corporations. As we have seen, they do say at a higher level than any business and company, generating profits for companies that collect more data than they would in a purely competitive setting, all without meeting any consumer preference.

[79]Stigler, "An Introduction", 633.

To see the different incentives of states and corporations, consider this example, where an individual finds out the data collected about him is inaccurate. A company with inaccurate data would want to correct it because: 1) it wants its data to accurately reflect consumer preferences and 2) the company would and could receive payment for the error if it was useful as the consumer.[80] States, on the other hand, have no profit motive to correct their errors and do not desire to meet consumer preferences. That error could stop an individual from receiving a loan, visiting a country, or getting insurance to cover a medical procedure. This can and has happened. Instead of motivating the state to act on his behalf through pecuniary means, the individual would have to go through courts.[81] Not only is this more expensive, but it is less likely to succeed; the data is not the person's "right" nor are they even likely to know about the error in the case of the state.

Unlike markets, state incentives are entirely political. A database of personal information is dangerous in the hands of any government, foreign or domestic. Because states solely acquire wealth by "political means", not "economic means", data in state hands is a tool solely for extracting more wealth from the public and further securing the governments and special interest positions.[82] The shift from government on government surveillance to government on populace surveillance documented in *Data and Goliath* further demonstrates governments have a parasitic relationship with markets.[83] State's used to conduct surveillance in the name of "national security", spying primarily on hostile foreign governments. Today, states work together to spy on everyday people, the same people they depend on for their wealth.

---

[80]Ibid, 627.
[81]Schneier, *Data,* Chapter 7.
[82]Rothbard, Murrary. *Anatomy of the State*. Auburn, Alabama: Ludwig Von Mises Institute (2009), 15.
[83]Schneier, *Data,* Chapter 5.

The chronological order of events also indicates that states are the principal cause of market distortions. As detailed above, agencies like the FBI have lobbied to force producers and manufacturers to make product surveillance compatible. Companies were already building internet and communications infrastructure. The state stepped in, piggybacking on free-market progress, and lowered people's privacy by coercing or bargaining to make corporations share personal data and lower privacy. State's "didn't build a massive Internet eavesdropping system from scratch. It noticed the corporate world was already building one and tapped into it."[84] Before the state stepped in, many companies and entrepreneurs were making technology that made people more secure, not less. States started losing the ability to survey and legally compelled companies to make their users information available. Yes, corporations like Facebook agreed to partner with organizations like the NSA. Yes, they lied to the public about the programs and yes, they were rewarded for it, receiving lack government oversight, lobbying for and getting competition hindering legislation, and government contracts. But none of that would have happened without state intervention, without the state hindering Free Market Competition, and paying Big Tech to collect more data.

It is worth noting that companies (even Big Tech ones) have sometimes resisted the state's siren call. Twitter has "fought aggressively" against state action that affects user privacy. It, unlike Facebook, refused to make it easier for state agencies to access company data.[85] Similarly, Apple has refused a court order to open a user's iPhone; Apple CEO Tim Cook, in an open letter to customers wrote "the U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. They have asked us to build a backdoor to the iPhone." Cook called the state order "an unprecedented step which threatens the

[84]Ibid, Chapter 6.
[85]Miller, "Tech."

security of our customers." [86] Yes, companies like Facebook have worked with and been rewarded by the U.S. government. But these market distortions are ultimately the state's creation – they would not exist be it for the state. Moreover, as detailed above, the pushback of some entrepreneurs to protect privacy against the state proves these privacy and information market distortions are caused by state intervention. In the next section, I will detail how encryption technology is being used by entrepreneurs and privacy consciousness individuals to fight state surveillance. The investment in, development of, and use of this tech, particularly in cryptocurrencies, can be understood as an entrepreneurial reaction to government surveillance while also meeting market demand for privacy.

The First Cryptocurrency

In 2010, FBI general counsel Valerie Caproni remarked "No one should be promising their customers that they will thumb their nose at a U.S. court order. They can promise strong encryption. They just need to figure out how they can provide us [the state] plane text."[87] In other words, no business should provide absolutely secure services to its customers.

When faced with state oppression and regulation, entrepreneurs have resorted to any means necessary to produce and sell their goods. In the socialist Soviet Union, for example, entrepreneurs resorted to importing goods from Western countries and selling them at "illegal prices." Jeans, despite not being manufactured in the USSR, were particularly popular with the Soviet youth.[88] In America, during the 1920s, facing the legal ramifications of the 18th amendment, liquor distributors resorted to hiding alcohol in their boots, earning them the name

[86]Cook, Tim. "A Message to Our Customers." *Apple*, February 2016. Accessed November 25, 2020. https://www.apple.com/customer-letter/
[87] Schneier, *Data,* Chapter 7.
[88]Gindler, Allen. "Black Markets Reveal the Power of Economic Laws." *Foundation for Economic Education*, June 2019. Accessed November 25, 2020. https://fee.org/articles/black-markets-reveal-the-power-of-economic-laws/

bootleggers.[89] Entrepreneurs find solutions to problems. If that problem is government-generated regulation, then so be it.

Privacy-conscious individuals have, for quite some time, been drawn to the power of encryption technology. In the 1990s a group of tech enthusiasts began meeting and discussing the future of the internet.[90] Their principal goal was to secure privacy and anonymity online, both of which they (correctly) guessed would soon be threatened by the U.S. government. Encryption technology was, in their minds, the way to circumvent government restrictions and regulations.

Cryptography is defined as "secret messaging, the enciphering and deciphering of messages in secret code or cipher. Also: the computerized encoding and decoding of information."[91] Encryption has been used to securely browse, communicate, and protect data. Most recently, entrepreneurs have used it to develop decentralized private currencies, called cryptocurrencies.

One of the primary ways, perhaps the primary way, cypherpunk entrepreneurs sought to thwart government encroachment and provide themselves and other individuals with privacy was by hamstringing state control over the currency. Besides state inflation, which is too broad a topic to discuss here, the state had used its monopoly on printing money and financial regulation to block transactions, and track individuals extensively.[92] Mathematician and cypherpunk Eric Hughes, in "A Cypherpunk's Manifesto", wrote, "Privacy is necessary for an open society in the

---

[89]Thornton, Mark. "Prohibition Caused the Greatness of Gatsby." *The Ludwig Von Mises Institute*, May 2013, Accessed November 25, 2020, https://mises.org/library/prohibition-caused-greatness-gatsby

[90]Qureshi, Haseedb. "The Cypherpunks" *Nakamoto Institute*, December 2019. Accessed November 24 , 2020. https://nakamoto.com/the-cypherpunks/

[91]*Merriam Webster.* "Cryptography." Accessed November 24, 2020, https://www.merriam-webster.com/dictionary/cryptography

[92] Schneier, *Data,* Chapter 5.

electronic age … privacy in an open society requires anonymous transaction systems … we are defending our privacy with cryptography … with anonymous money."[93]

It took years and countless failures before Hughes and the other cypherpunk's vision materialized. But eventually, a digitally native private currency was developed. In late 2008, early 2009, the first successful attempt at a cryptocurrency was born – bitcoin. Bitcoin uses encryption technology, decentralized surveys, built-in economic incentives, and open-source code to allow people to send transactions "peer-to-peer" electronically.[94]

Much like the early internet, Bitcoin's network infrastructure is still being built out so it is too early to judge how significant a technology it is.[95] However, as evidenced by its price action, it has a growing list of users and supporters, proving individuals and institutions on some level demand private currency. Realized bitcoin market capitalization and per-unit value hit an all-time high on December 1st, 2020. That price action is not just old users bidding the price higher – the number of bitcoin addresses with a balance of $10 or more has steadily increased since bitcoin was released.[96]

Bitcoin has proven to be valuable, but it is not perfect – it only provides pseudo-anonymity, not full anonymity. The U.S. government has successfully used bitcoin's open ledger, The Blockchain, to identity and track both transactions and individuals. When bitcoin was first in its infancy, state actors feared its potential to shield individuals' identities and transactions. But after blockchain companies found ways to track and link transactions and addresses to specific people, law enforcement began to view bitcoin as a tool for prosecuting

---

[93]Hughes, Eric. "A Cypherpunks Manifesto." *The Satoshi Nakamoto Institute*, March 1993. Accessed November 24 , 2020. https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt

[94]Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *The Satoshi Nakamoto Institute.* Accessed December 1, 2020. https://nakamotoinstitute.org/bitcoin/: 1.

[95]Rozmajal, Anthony. "The True Economic Impacts of Blockchain." Grove City College, February 2018. Accessed November 10, 2020. https://austrianstudentconference.com/archives-2018-schedule/

[96]Carter, Nic. "Nine Bitcoin Charts Already At All-Time Highs." *Medium*, November 2017. Accessed November 30, 2020. https://medium.com/@nic__carter/nine-bitcoin-charts-already-at-all-time-highs-78abbfe82804

crimes.[97] This in turn led some of the more privacy-conscious crypto-entrepreneurs back to the drawing board.

Enter Zcash

Zcash is a "privacy-preserving cryptocurrency" that was conceived from the observation that bitcoin could not offer strong privacy guarantees." Zcash uses "zero-knowledge proofs" which block outsiders from observing transactional amounts or "the parties involved."[98]

Currently, Zcash is not widely used. Nor is it widely known about. Bitcoin, in all respects, dwarfs it. And bitcoin itself is dwarfed by national currencies. But these technologies are still of value. They would not exist, at least in their present form, if states had not encroached on citizen privacy or if individuals had not developed and demanded them. Moreover, the relative valuations and small size of bitcoin and zcash are indicative of consumer preferences; as referenced above, bitcoin, in fact, all cryptocurrencies, are new technologies with infrastructures not fully developed. There are costs to transacting in bitcoin or zcash, such as the cost of searching for merchants who accept it. But there are also costs to using national currencies, such as the U.S. dollar. This cost consists of having transactions tracked by, and ultimately done at the discretion of the state.

In 2019, total bitcoin transaction volume equaled less than 3% of U.S. Gross Domestic Product. Zcash's market capitalization is less than 0.5% of bitcoins. That does not mean these technologies are insignificant or have failed. Rather, this shows most people in most transactions do not have privacy concerns or if they do they do not outweigh their desire for convenience, which is consistent with the economic literature detailed above.

---

[97]Bohannon, John. "Why Criminals Can't Hide Behind Bitcoin." *Science Magazine*, May 2016. Accesses November 30 2020. https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

[98]Messari. "Zcash." Accessed November 30, 2020. https://messari.io/asset/zcash/profile

What is proven by the development of these currencies and their, albeit not widespread, use, is that when government regulation encroached on privacy, entrepreneurs developed alternate, private means of payment. They reacted initially with bitcoin, a decentralized pseudonymous currency that offered individuals an alternative to fiat. Then, once states undermined some of the privacy features behind bitcoin, entrepreneurs again reacted, producing a more fully anonymous currency that provides more privacy than both bitcoin and state-issued fiat money.

Encryption Under Attack

The U.S. government, despite using encryption itself, has continually sought ways to subvert it, both legally and computationally. In 2013, *The Guardian* reported that the FBI tried to force the founder of the encrypted email service provider Lavabit, a man named Ladar Levison, to give them access to the "encryption keys to his system."[99] Lavabit had close to half a million users at the time Levison received the NSL ordering him what amounts to decrypt his user's data. Facing a "Gag" order, search warrants, subpoenas, and fines of up to $5,000 a day, Levison opted to shut down Lavabit instead of exposing his users to state oversight. In his own words, Levison did not want to be "complicit in crimes against the American people."[100] The only reason anyone knows about this case, which was conducted behind in a closed court, is because Levison refused the state's order and requested the court records be unsealed. Other companies and entrepreneurs have similarly been bullied into granting the state access to private, encrypted data – Schneier notes in *Data and Goliath* that Skype and Yahoo were respectively bribed and coerced into granting the State access to its systems.[101] But because the vast majority of these

[99]Rushe, Dominic. "Lavabit founder refused FBI order to hand over email encryption keys." *The Guardian*, October 2013. Accessed November 30, 2020. https://www.theguardian.com/world/2013/oct/03/lavabit-ladar-levison-fbi-encryption-keys-snowden
[100]Ibid.
[101]Schneier, Data, Chapter 5.

deals or state extortions happen in the dark, behind court locked doors, the American public will seldom, if ever, hear about them.

Today, seven years after the Levison case, the U.S. government is still working to make privacy-enhancing technology, specifically encryption, susceptible to state surveillance. In June of 2020 three Republican senators introduced a bill that would "require tech companies to assist law enforcement to access their encrypted devices and services when officials obtain a court-issued warrant based on probable cause that a crime has occurred."[102] Essentially this bill would create a backdoor to encryption for state agencies to walk through. Some members of private enterprise have pushed back on this bill arguing that the bill would ruin encryption and thus privacy for all users.[103] The government crackdown on encryption extends beyond communication and tech companies.

President Donald Trump is reported to have told Treasury Secretary Mnuchin to "go after" bitcoin.[104] The President's disdain for bitcoin and encrypted digital currencies is clear – he tweeted in July of 2019 that he was "not a fan of Bitcoin and other Cryptocurrencies … Unregulated Crypto Assets can facilitate unlawful behavior."[105] The Trump administration has even hired private contractors via a bounty program, offering $625,000 to coders able to break privacy coin Monero's encryption or hackers able to track transactions on one of bitcoin's side networks.[106]

---

[102]Feiner, Lauren. "GOP Senators Introduce Bill that Would Create a Backdoor for Encryption." *CNBC*, June 2020. Accessed November 30, 2020. https://www.cnbc.com/2020/06/24/gop-senators-introduce-bill-that-would-create-a-backdoor-for-encryption.html

[103]Ibid.

[104]Baker, Paddy. "Trump Told Treasury Secretary to "Go after Bitcoin." *Coindesk*, June 2020. Accessed November 3, 2020. https://www.coindesk.com/trump-told-treasury-secretary-to-go-after-bitcoin-bolton-book-reportedly-claims

[105]Trump, Donald. Twitter Post. July 11, 2019. Accessed November 30, 2020. https://twitter.com/realdonaldtrump/status/1149472282584072192?lang=en

[106]Mapperson, Joshua. "The IRS offers a $650,00 bounty to anyone who can break Monero and Lightning." *Cointelegraph*, September 2020. Accessed November 30, 2020. https://cointelegraph.com/news/the-irs-offers-a-625-000-bounty-to-anyone-who-can-break-monero-and-lightning

Encryption, which secures information between sender and receiver, is a privacy-enhancing technology embedded in goods and services by entrepreneurs. The state, having no incentive to meet consumer demand, has continually pushed for more surveillance and more data. Since the creation of bitcoin, the U.S. government has indirectly and directly targeted encrypted currencies; eventually, the U.S. government learned to survey its citizens via bitcoin's digital ledger. This surveillance has in turn generated more investment in PETs and observation technology, as seen in the subsequent creation of fully anonymous cryptocurrency Zcash. As such, since this sequence of events and investment was caused by state intervention, the creation of private digital currencies cannot be understood as anything other than an entrepreneurial effort to provide more privacy in the face of unprecedented state observation.

Conclusion:

Economist Friedrich Hayek demonstrated the importance of decentralized decision for productive markets in his "The Use of Knowledge in Society":

> If we can agree that the economic problem of society is mainly one of rapid adaptation to changes in the particular circumstances of time and place, it would seem to follow that the ultimate decisions must be left to the people who are familiar with these circumstances … We need decentralization because only thus can we ensure that the knowledge of the particular circumstances of time and place will be promptly used.[107]

Letting individuals make decentralized decisions produces more prosperity because entrepreneurs in markets have incentives to meet consumer demand. This is true in all markets and is true in information and privacy markets.

---

[107]Friedrich A. Hayek, "The Use of Knowledge in Society," American Economic Review 35, no. 4 (September 1945): Accessed December 12, 2017, http://www.econlib.org/library/Essays/hykKnw1.html.

The U.S. government has failed to protect individual privacy, in fact, this paper has detailed how the U.S. government is the biggest violator of that privacy and the cause of the public-private surveillance partnership. Entrepreneurs, reacting to this violation, have resisted this partnership outright and stepped in to provide privacy solutions. They've shone a light on state action in the media, fought them in courts, and most importantly met the public demand for privacy by embedding encryption technology into goods, birthing a new generation of currencies that offer users varying levels of privacy via encryption technology.

Bibliography

Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The Economics of Privacy." *Journal of Economic Literature* 54, no. 2 (2016): 442-92. Accessed November 7, 2020. http://www.jstor.org/stable/43966740.

Auxier, Brook Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner. "Americans and Privacy: Concerned, Confused and Feeling a Lack of Control Over Their Personal Information." *Pew Research Center*, November 2019. Accessed November 30, 2020. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Baker, Paddy. "Trump Told Treasury Secretary to "Go after Bitcoin." *Coindesk*, June 2020. Accessed November 3, 2020. https://www.coindesk.com/trump-told-treasury-secretary-to-go-after-bitcoin-bolton-book-reportedly-claims

Bankston, Kevin "Surveillance Shocker: Spring Received 8 million law requests for GPS Data." *Electronics Frontier Foundation*, December 2009. Accessed November 30, 2020. https://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law

Bennet, Corry. "Advocates Accuse Facebook of Secretly Lobbying for Cyber Bill." The Hill, November 2015. Accessed November 30, 2020. https://thehill.com/policy/cybersecurity/258060-advocate-acuses-facebook-of-secretly-lobbying-for-cyber-bill

Bohannon, John. "Why Criminals Can't Hide Behind Bitcoin." *Science Magazine*, May 2016. Accesses November 30 2020. https://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

Carter, Nic. "Nine Bitcoin Charts Already At All-Time Highs." *Medium*, November 2017. Accessed November 30, 2020. https://medium.com/@nic__carter/nine-bitcoin-charts-already-at-all-time-highs-78abbfe82804

Clement, J. "Cumulative Number of Monthly Facebook Users, as of 3rd Quarter 2020." *Statista*, November 2020. Accessed November 20, 2020.https://www.statista.com/statistics/947869/facebook-product-mau/

Cook, Tim. "A Message to Our Customers." *Apple*, February 2016. Accessed November 25 , 2020. https://www.apple.com/customer-letter/

Feiner, Lauren. "GOP Senators Introduce Bill that Would Create a Backdoor for Encryption." *CNBC*, June 2020. Accessed November 30, 2020.

https://www.cnbc.com/2020/06/24/gop-senators-introduce-bill-that-would-create-a-backdoor-for-encryption.html

Foer, Franklin. “What Big Tech Wants Out of the Pandemic.” *The Atlantic*, July 2020. Accessed November 3, 2020. https://www.theatlantic.com/magazine/archive/2020/07/big-tech-pandemic-power-grab/612238/

Friedrich A. Hayek, "The Use of Knowledge in Society," American Economic Review 35, no. 4 (September 1945): Accessed December 12, 2017, http://www.econlib.org/library/Essays/hykKnw1.html.

“FTC imposes 5 billion penalty sweeping new privacy restrictions.” *FTC.gov*, June 2019. Accessed November 30, 2020. https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions

Gindler, Allen. “Black Markets Reveal the Power of Economic Laws.” *Foundation for Economic Education*, June 2019. Accessed November 25, 2020. https://fee.org/articles/black-markets-reveal-the-power-of-economic-laws/

Glasner, April. “Thousand of Contracts Highlight Quiet Ties Between Big Tech and .” *NBC*, July 2020 . Accessed November 30, 2020. https://www.nbcnews.com/tech/tech-news/thousands-contracts-highlight-quiet-ties-between-big-tech-u-s-n1233171

Gulian, Neema. “The FBI Has Access to Over 640 Million Photos of US Through its Facial Recognition Technology.” *ACLU*, June 2019. Accessed November 30, 2020. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/fbi-has-access-over-640-million-photos-us-through

Hazlitt, Henry. Economics in One Lesson. Auburn, Alabama: Ludwig von Mises Institute, 2019. https://mises.org/library/economics-one-lesson

Hughes, Eric. “A Cypherpunks Manifesto.” *The Satoshi Nakamoto Institute*, March 1993. Accessed November 24 , 2020. https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt

Klein, Peter. “The Economics of Data Privacy.” Mises Institute. Lecture. Accessed November 10, 2020. https://mises.org/library/economics-data-privacy-1.

Kruth, Rebecca. “ACLU: Michigan State Police have been tracking cell phones for years.” *Michigan Radio*, October 2015. Accessed November 30, 2020. https://www.michiganradio.org/post/aclu-michigan-state-police-have-been-tracking-cell-phones-years

Laudon, Kenneth C. "Markets and Privacy." Communications of the ACM 39 (9) (1996).: 92-10 Accessed November, 7 2020. https://dl.acm.org/doi/pdf/10.1145/234215.234476.

_____. "Markets and Privacy." Working Paper. NYU Faculty Digital Archives. Stern School of Business, New York University, July 1993. https://archive.nyu.edu/handle/2451/14257.

Macias, Amanda. "Facebook CEO Zuckerber Calls for More Government Regulation." *CNBC*, February 2020. Accessed November 30, 2020. https://www.cnbc.com/2020/02/15/facebook-ceo-zuckerberg-calls-for-more-government-regulation-online-content.html

Mapperson, Joshua. "The IRS offers a $650,00 bounty to anyone who can break Monero and Lightning." *Cointelegraph*, September 2020. Accessed November 30, 2020. https://cointelegraph.com/news/the-irs-offers-a-625-000-bounty-to-anyone-who-can-break-monero-and-lightning

McMaken, Ryan. "Don't Regulate Facebook – That's What Zuckerberg Wants." *Ludwig Von Mises Institute*, April, 2018. Accessed November 30, 2020. https://mises.org/wire/dont-regulate-facebook-thats-what-zuckerberg-wants

Menger, Carl. *Principles Of Economics*, Auburn, Alabama: The Ludwig Von Mises Institute, 2007. https://cdn.mises.org/Principles%20of%20Economics_5.pdf

Messari. "Zcash." Accessed November 30, 2020. https://messari.io/asset/zcash/profile

Miller, Claire. "Tech Companies Concede to Surveillance Program." *The New York Times* June 2013. Accessed November 30, 2020. https://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html?ref=global-home&_r=1&&pagewanted=all

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System." *The Satoshi Nakamoto Institute.* Accessed December 1, 2020. https://nakamotoinstitute.org/bitcoin/

Noam, Eli M. 1997. "Privacy and Self-Regulation: Markets for Electronic Privacy." *In Privacy and Self- Regulation in the Information Age.* Washington, DC: US Department of Commerce, National Tele-communications and Information Administration. Accessed November 24, 2020. https://www.ntia.doc.gov/page/chapter-1-theory-markets-and-privacy.

Ovide, Shira. "Congress Agrees: Big Tech is Broken." *The New York Times*, October 2020. Accessed November 1, 2020. https://www.nytimes.com/2020/10/07/technology/congress-big-tech.html

Pew Research. “Mobile Fact Sheet” *Pew Research Center*. Accessed November 30, 2020. https://www.pewresearch.org/internet/fact-sheet/mobile/

Qureshi, Haseedb. “The Cypherpunks.” *Nakamoto Institute*, December 2019. Accessed November 24 , 2020. https://nakamoto.com/the-cypherpunks/

Rothbard, Murray N. *A History of Money and Banking in the United States: the Colonial Era to World War II.* Auburn, Alabama: Ludwig von Mises Institute, 2005. https://mises.org/library/history-money-and-banking-united-states-colonial-era-world-war-ii

_____. *Anatomy of the State*. Auburn, Alabama: Ludwig Von Mises Institute, 2009.

Rushe, Dominic. “Lavabit founder refused FBI order to hand over email encryption keys.” *The Guardian*, October 2013. Accessed November 30, 2020. https://www.theguardian.com/world/2013/oct/03/lavabit-ladar-levison-fbi-encryption-keys-snowden

Schneier, Bruce. *Data and Goliath: the Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton & Company, 2016. Digital.

Section 215 of the Patriot Act.” *Electronics Frontier Foundation.* Accessed November 30, 2020. https://www.eff.org/files/2018/11/25/215_one_pager_-_2018.11.pdf

Stigler, George J. "An Introduction to Privacy in Economics and Politics." The Journal of Legal Studies 9, no. 4 (1980): 623-44. Accessed November 9, 2020. http://www.jstor.org/stable/724174.

Thornton, Mark. “Prohibition Caused the Greatness of Gatsby.” *The Ludwig Von Mises Institute*, May 2013, Accessed November 25, 2020 https://mises.org/library/prohibition-caused-greatness-gatsby

Trump, Donald. Twitter Post. July 11, 2019. Accessed November 30, 2020. https://twitter.com/realdonaldtrump/status/1149472282584072192?lang=en