Word Count: 18,452

David Chaum and Ecash:

Privacy Technology's Negotiations of Political, Cultural, and Techno-Social Contingencies in the mid-1990s

Michael J. Christie

Undergraduate Senior Thesis, Department of History

Columbia University in the City of New York

Professor Mae Ngai, Faculty Advisor

Professor Matthew Jones, Second Reader

April 3, 2015

Table of Contents

Introduction……..3

Chapter 1: Building an Invasive World Wide Web Infrastructure……..10

Chapter 2: David Chaum and Ecash……..21

Chapter 3: “The Future of Money” and Media Portrayals of Ecash……..28

Chapter 4: Congressional Rhetoric as an Extension of the New Right and Market Populism…….46

Chapter 5: The Nature of Free Market Politics and Social Movement……..57

Conclusion……..70

Appendix……..73

Bibliography……..74

Introduction

Since the first computers were created in the 1940s, government and corporate demand for data on private individuals has grown immensely. As computer technology bolstered commercial interests' capabilities to collect more data in more sophisticated ways, trends in the flow of advertising dollars to the Web fed a thriving industry of data compilers. This development, along with conservative republican government's agenda of deregulation, set a trajectory that shaped the structure of ecommerce and created the free-internet model based on advertising that we know today. Starting in the 1980s, changes in the structure of the advertising industry placed a premium on the ability to track the movements of individuals through the Web in order to measure the effectiveness of advertisements and justify advertising budgets. Consequently, technology innovators, programmers, and web publishers, who relied on advertising dollars, were inclined, if not compelled to create an infrastructure that would facilitate surveillance of individual transactions on the Web. The restructuring and budgeting of the advertising industry and the growing value of information to commercial interests caused an emerging Web infrastructure that was subservient to the surveillance interests of those who funded its creation. By the early 1990s privacy tech innovators and civil libertarians had become disturbed by this ominous downside of the emerging Web, more specifically, its growing propensity to infringe on individual privacy rights.

On July 25, 1995 the first of four Congressional hearings convened to discuss "The Future of Money." The hearing before the Subcommittee on Domestic and International Monetary Policy of the House Committee on Banking and Financial Services included numerous

senators and members of the House of Representatives, executive members of Visa and Mastercard, and various independent tech innovators, including one central to this thesis, David Chaum. The hearings were aimed at reaching a consensus about how the most effective, secure online payment system for the nascent, but rapidly growing ecommerce terrain would be fabricated. The Committee heard testimonies on the various advantages and disadvantages of emerging privacy technology, utilizing the latest cryptographic techniques, all of which needed to be considered by government as a viable alternative to credit cards, which were not created to be used in online transactions. Visa and Mastercard were laying the basis for a more cumbersome system with many security issues. Perhaps more importantly, credit cards were open to government and industrial surveillance, and credit card companies were already engaged in the practice of making their customer data available to outside commercial interests, especially to private commercial data compilers.

The purpose of this thesis is to investigate a critical juncture situated in the privacy debates surrounding ecommerce in the mid-1990s. It is an investigation into privacy technology that, if adopted, would have created a very different Internet model than that of the invasive free advertising model that we have come to know today. In the past, the government has enacted privacy legislation, but in this case it failed to support substantive, structurally effective, and most importantly, tangible privacy technologies that would protect the privacy of Americans as the country led the charge into the digital information age. There are three major reasons for this incongruity. First, most elected representation did not grasp the magnitude of the impending ecommerce movement or the implications of third party interests in control of large stores of personal consumer data. Second, corporate lobbying against more transparent,

functional privacy legislation that would protect individuals from industrial scrutiny proved overwhelming. And third, with Republicans gaining control of both the House and the Senate in the early 1990s, and laissez-faire market policy and deregulation of industry becoming predominant trends, emerging markets were left to regulate themselves through competition. Laissez-faire rhetoric became the crux of a policy of inaction by a new right Congress towards supporting newer and more comprehensive privacy technology. With little support, privacy innovators were left to compete against credit card companies and data brokers for market share. In her testimony on July 25, 1995 Visa executive Rosalind Fisher said "Visa itself processes more than $630 billion in transactions annually."[1] This figure alone was exponentially larger than any competitor. Without substantial popular and government support, privacy technology emerging in the early to mid-1990s failed to take root at a time when the infrastructure of the Web was being created and its implementation was most important, despite its technological viability. This thesis argues that the failure was not a foregone conclusion dictated by technology limitations or other conditions, but was the result of political, cultural, and techno-social contingencies.

In 1995, during and shortly after "The Future of Money hearings," the United States government had an opportunity to shape the Web's infrastructure, and in doing so, build privacy protections into the very nuts and bolts of part of the system. It failed to do so. Government failure to adequately invest in and promote a secure and anonymous payment system to handle ecommerce transactions that *intrinsically* contained the same privacy benefits

[1] Fisher, Rosalind. Statement to the House, Committee on Banking and Financial Services, Subcommittee on Domestic and International Monetary Policy. *The Future of Money,* Hearing, July 25, 1995 (Serial 104-27). Appendix p. 147. Available at: http://www.archive.org/stream/futureofmoneyhea01unit/futureofmoneyhea01unit_djvu.txt

as cash in an open marketplace was a failure on the part of elected representation to protect individual privacy rights from corporate America's—and by extension, government's—ability to surveil. David Chaum's innovation, Ecash, was that intrinsically private technology. By virtue of its everyday function, privacy was an inherent effect; as such, its very use would perpetuate privacy. In other words, individuals who used electronic cash would be protecting valuable pieces of information about their spending habits and personal interests from third party interests, without adding any steps to the purchase process. As more people decided to spend their money directly over the Web using Ecash technology, an online marketplace would develop naturally just as a physical marketplace in a town square, in which consumers buy directly from merchants without being surveiled by third party interests. In this marketplace, disclosure of personal information by the payer is not necessary—whereas with a credit card it would be.[2] This was Chaum's analogy and vision. At this point in the digital age, privacy legislation only protected the possibility of privacy. It was only partially available to an individual if he or she knew enough to adjust his or her browser settings correctly, something the vast majority of Americans did not and still do not know to do.

As a framework for understanding these contingencies, this thesis connects historical analysis with sociological study applied to technology. Communications professor David Phillips makes use of technological framing elements to add analytical clarity to the sociological implications of digital payment systems, and that work is critical to understanding how historical trends impacted social mobilization in support of privacy technology in the mid-

[2] Chaum, David. Statement to the House, Committee on Banking and Financial Services, Subcommittee on Domestic and International Market Policy, *The Future of Money,* Hearing, July 25, 1995 (Serial 104-27). Appendix p. 135. Available at: http://www.archive.org/stream/futureofmoneyhea01unit/futureofmoneyhea01unit_djvu.txt

1990's. He says "technological artifacts are interpretively flexible.[3] Their purpose and the social contexts in which they are situated are inherently malleable. Social actors' interpretations guide and incite action which incorporates the artifacts into social practice. In attempting to manipulate the social understanding of artifacts, actors can essentially sway the action propelling an artifact.[4]

Credit cards, and payment system privacy technology, for example, do not solely transfer value from consumer to vendor. Credit cards, while performing their primary function, gather vast quantities of consumer transaction information and privacy technology protects against such gathering. These databases are extremely valuable to both commercial interests and law enforcement. Whether consumers fully grasp the capacities of a payment system, and how they comprehend the role of surveillance in society, influences how they will fabricate, augment, and interact with the socio-technical structures which constitute that system.

Wiebe Bijker uses the term "'technological frame' to signal those 'elements that influence the interaction within relevant social groups and lead to the attribution of meanings to technological artifacts.'"[5] Elements of these frames may include key obstacles, goals, tacit knowledge, and users' practice. "Entman describes framing as 'select[ing] some aspects of a perceived reality and mak[ing] them more salient in communicating text, in such a way as to promote a particular problem definition, causal interpretation, moral evaluation, and/or

[3] Pinch and Bijker, In. Phillips, David J. "Digital Cash and the Surveillance Society." Diss. U of Pennsylvania, 1998. P.42
[4] Phillips, 42.
[5] Ibid. p. 207.

treatment recommendation.'"[6] Accordingly, these frames are generated by the presence or absence of certain "keywords, stock phrases, stereotyped images, sources of information, and sentences that provide thematically reinforcing clusters of facts or judgements."[7] In Gamson's model, activists promote "packages" for advancing discourse of a certain issue in particular sites. These packages consist of devices which use frames for viewing the issue, and thus, dictate choices for action.[8] [9]

Framing activity such as that mentioned above, can occur in many types of discursive sites. For this thesis I draw attention to a study conducted by Phillips in which he analyzes the Ecash delivery package and its deployment into mass media. The effectiveness of the package is contingent upon both its structural fit with the institutional practices of the discursive site and its "cultural conductiveness" and "resonance" within that site.[10]

While situating Chaum's testimony at the dawn of electronic commerce, and placing the relevant debates around privacy within the conservative upsurge of the late 20th century explains much about the non-adoption of privacy technology, further examination is necessary. The sociology of digital payment technology—specifically, employing frame alignment and social mobilization theory—offers a more robust and analytical explanation into the contingencies that caused the failure of privacy technology in ecommerce.

Phillips' research includes examination of public discourse in order to uncover the processes by which issues of surveillance, identification, and privacy are subsumed into public

[6] Entman in Phillips, 61.
[7] Ibid.
[8] Devices can refer to metaphors, exemplars, consequences and appeals to principle
[9] Gamson In Phillips, "Digital Cash and the Surveillance Society." p. 209.
[10] Gamson In Phillips, "Digital Cash and the Surveillance Society." p. 210.

understandings of consumer payment systems. By coupling Phillips' research—the issue package deployed by Chaum which follows its reverberation (or lack thereof) through the media—with my own analysis, this thesis investigates different levels of acceptance by different actors and situates that analysis within the broader themes of globalization and free market politics in the 1990s.

Chapter 1: Building an Invasive World Wide Web Infrastructure

The Data Compiling Industry:

Collecting, combining, and layering information about individuals for commercial gain is nothing new. Throughout the twentieth century lenders, investigators, retailers, marketers, insurers and a host of others have been engaged the practice of collecting and organizing information in new ways to create value for commercial interests.[11] For marketers, the need to collect information was a matter of finding people who might be most interested in their products. Banks needed to find borrowers. Political motivation dictated list building for others. For example during World War I the government surveiled labor activists and war critics.[12] Similar efforts pervaded the 1950s and 1960s, when the FBI and the Army created databases about tens of thousands of students, anti-war activists, social crusaders, and others deemed undesirable. Information compilers' efforts were almost never regulated and they were limited only by the physical capacity of their offices. In the 1940s the first computers created a boon for data collectors. Their functioning was limited, but they sparked a new way of thinking about information. It was not long before businesses, bureaucrats, scientists, and others realized that the old information storage boundaries no longer existed, and with the increase in capability, would come a concurrent surge in benefits of data compiling.[13]

[11] O'Harrow, Robert. *No Place to Hide*. New York: Free, 2005. P. 39.
[12] O'Harrow, p. 39.
[13] Ibid.

During the 1960s, roughly 250 businesses began specializing in brokering data, right down to the smallest details of personal information.[14] This nascent industry was fueled by magazine publishers, hoteliers, car dealerships and other businesspeople who all realized that they could profit by selling the names addresses, and preferences of their customers.[15] Dunhill International List Company was at the forefront of this surge. In 1964, Dunhill sold personal information to magazine publishers and others. For fourteen dollars, "you could acquire the names of a thousand women who bought a 'bust developer' product. If you wanted to find 'men and women of large means,' the list cost fifteen dollars. A few dollars more would get you the names and addresses of newlyweds, 500, 000 in all."[16] Government agencies soon followed and across the country, government employees started to sell lists of births, marriages, new families, and tax rolls to companies like Dunhill. The Rueben H. Donnelley Corporation started regularly buying information about the cars people registered and it soon was selling access to lists of 400,000 car owners.[17] Information brokering was becoming big business.

The muckraking journalist Vance Packard estimated that "by 1964 business, charities, and political groups were spending $400 million annually to buy information about individuals."[18] While selling details about marriage licenses, one clerk earned nearly $60,000. "There is no question about it," Packard wrote in his book, *The Naked Society,* "In bulk we are very attractive."[19] With computer power on the rise, the data compiling industry was able to expand greatly. O'Harrow said that the credit bureaus were some of the leaders of this charge.

---

[14] Ibid, p. 40.
[15] Ibid. p. 40.
[16] Ibid. p. 40.
[17] Ibid.
[18] Packard, Vance. *The Naked Society*. New York: D. McKay, 1964. P. 183.
[19] Ibid. p. 183.

Hundreds of their operations conducted background investigations of individuals on their behalf for credit card issuers and other lenders. The initial application for credit already provided the bureaus with substantial information. The bureaus then added the data they had already collected from other public sources. Often, the information collected was inadequate and the bureaus sent private investigators to individual's homes and in the process would question landlords, friends, neighbors, and coworkers.[20] According to O'harrow, "the bureaus insisted they handled such reports with care, making the same promises they make now: no one gets access to the information unless they have signed contracts limiting the use of the reports to credit granting."[21] More true, even today, is that for a small fee or even in some cases for free, credit information can be obtained on almost anybody.

The spike in information collecting created much that we now take for granted: instant credit cards, cheaper mortgages, endless shopping options, even phone books. However, "it was also a huge step down the slippery slope of privacy encroachment for commercial gain," said O'Harrow.[22] In 1971, a Michigan University academic named Arthur R. Miller joined pundits when he described the computer-driven changes as a "cybernetic revolution." His book was called *The Assault on Privacy.*[23]

The advent of the Internet and then the World Wide Web drastically changed the terrain of the information industry by networking previously disconnected business interests. It allowed for new ways for data compilers to service different industries. In 1994, in an interview

[20] O'Harrow, Robert. *No Place to Hide*. New York: Free, 2005. P. 41.
[21] Ibid. p. 41.
[22] Ibid.
[23] Ibid.

with the Arkansas Business Journal, Senior Vice President and Chief Information Officer Alex Dietz of Acxiom Corp explained how his company serviced commercial interests as a data compiler by saying "[we] provide a data processing infrastructure where we can basically say, 'Let us help you with your information management technology and let us take this data that you've got and see if we can put it into a framework that will help you be more competitive.'"[24] In doing so, Acxiom and other data compilers were able to layer their existing information on individuals with information from the databases of other companies they were servicing. The net effects of an interlinked network of data compilers, each with their own commercial interests, were twofold. First, they made an already invasive practice even more invasive by deepening the level of detail in the dossiers collected on individuals. And second, they exponentially raised the level of effectiveness of advertising measured by profits.

Acxiom remains the most illustrative example of networked data compiler. "Acxiom alone had almost one million times the capacity for information in 2004 than it had in 1983," a figure that mirrors the advertising and ecommerce boon that happened concurrently with the growing sophistication of data collecting entities.[25] Helping businesses make sense of all their data stores became one of Acxiom's main goals in the 1990s. Simple lists were not as effective anymore. The stakes had been raised. Effective profiling—"getting inside their heads"—

[24] Walters, D. (1994). Blazing an international technology trail: Impressive developments continue with acxiom, arkansas systems, systematics. *Arkansas Business, 11*(35), 18. Retrieved from http://ezproxy.cul.columbia.edu/login?url=http://search.proquest.com/docview/220372108?accountid=10226
[25] O'Harrow, Robert. *No Place to Hide*. P. 43.

precipitated an increased need to acquire even more information about individuals.[26] Data compilers began to make more and more deals with one another, even competitors.

In the early 1990s, the Internet was cumbersome to use and served mainly government and large commercial interests. 1991 saw the advent of the World Wide Web and its proliferation made the Internet more accessible to smaller entities, even to individuals with personal computers. Combined with the growing popularity of the Web, particularly ecommerce, the effectiveness of target marketing fueled by more comprehensive data from new coalitions of data compilers generated enormous profits for private industry. Along with Acxiom, Visa and MasterCard were at the forefront of the data compiling industry.

Shifts in Advertising Shape a New Surveillance Model of the Web: Towards the Free Advertising Model

According to a definition supplied by Joseph Turow in *The Daily You,* "many commonly consider the concept of advertising as mostly entailing the creation of content compelling one to purchase goods or services."[27] However, giving too much credit to what the advertising industry calls the "creative" side of the business neglects important components of advertising's social role. Essentially, advertising is a persuasion technique aimed at convincing people to purchase or support a product. This implies two other practices outside of creating persuasive messages. The first, known in the industry as media planning and buying, is centered

[26] O'Harrow, p. 44.
[27] Turow, Joseph. *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your worth*. New Haven: Yale UP, 2011. p. 19

on providing funds for where the ad is going to be situated.[28] The other, marketing research, is evaluative; as such, it is concerned with the effectiveness and measurability of ads.[29] Both of these practices have changed immensely within the last hundred years, in addition to the creative side. According to traditional advertising protocol, practitioners from both media buying and creative sides of the business should be synergizing for maximum effectiveness, and they often do. Nevertheless, shifts in the industry's balance have propelled the media buying and planning function to the forefront.[30]

While these shifts are associated with the rise of digital media, they are rooted in the pre-Web era. During the eighties and early nineties, many advertising companies chose to reconfigure media planning and buying into stand-alone entities within the industry.[31] Retrospectively viewing the slow rise to media buying's current stature, Turow says "we can see a growing desire to measure and label consumer responses as part of the new media agencies' need to justify the expectations and expenditures of their parent companies."[32] These parent companies were compelling major advertisers to infuse unprecedented amounts of capital into their new, stand-alone buying subsidiaries. In an effort to set themselves apart from other firms, media agency executives bragged about their ever-growing quantitative audience knowledge and about their agencies' "abilities to measure their advertising clients' audience responses."[33] They also claimed to be able to measure return on investment. To garner more clients, executives strongly urged their new subsidiaries to develop proprietary technologies

[28] Turow, p.20.
[29] Ibid.
[30] Ibid.
[31] Ibid.
[32] Ibid.
[33] Turow, p.21.

and models that predicted audience behavior in television, radio, newspapers, and magazines. These traditional forms of media had never been evaluated in these new ways. Turow said "when the internet came along, media buyers saw its interactive environment as a terrific terrain for expanding their numerical understanding of audiences—and for using the measures and labels to directly sell products."[34] Although the results left something to be desired in the early stages, the logic of quantification that these new practices were rooted in took on a life of its own.

The pressure to present data to help advertisers account for costs associated with Web advertising greatly increased as major advertising agencies became involved. In 1996 advertisers spent $300 million to advertise online, according to Jupiter Communications.[35] This demand greatly affected the developing infrastructure of the Web; the growth of which depended almost entirely on advertising dollars. As such, tech innovators were compelled to design in a manner which would fuel the engine that provided capital to fund the Web's expansion. In this system, the very impetus for the Web's expansion demanded that the Web's infrastructure be created in such a way that web users could be surveiled and any data relevant to the Web user be collected and analyzed. Essentially, the more information about Web users' behavior and identities that could be provided to media buying companies, the more revenue early Web engineers and innovators would receive to design and create.

These early stages of the Web were unfolding in ways that consciously overlooked the privacy of individual users. In the early to mid-1990s the free advertising model of the Web did

[34] Turow, p. 20.
[35] Petracca, Laura. "Interactive Agencies Rev Up Separate Online Buying Units," *Advertising Age,* March 17, 1997, p.30.

not exist. People paid monthly for America Online, Compuserve, or Prodigy. For a relatively low monthly rate, one of these companies would bring the Web to you in what we refer to today as a dashboard—mail, shopping, music, games, etc., all highly curated by the provider upon connecting to the Web. However, as invasive information gathering became inextricably tied with generating revenue, and an infrastructure emerged that was predicated on surveillance, the product started to change. Free email that compelled vastly larger numbers of people to divulge their information by signing up was far more valuable than a small membership that paid monthly. At the time, an overwhelming majority of people did not grasp this, especially politicians, policy makers, and the everyday Web user.

An example of an infrastructure component created to track individual Web user movement, the cookie, was discussed at length by Turow. He said "The 'cookie' marked the beginning of a shift. Ultimately, it would do more to shape the advertising—and social attention—on the Web than any other invention apart from the browser itself."[36] Lou Montulli created the cookie while working for Netscape Communications in 1994 to solve a marketing problem, although, at the time, its significance eluded many. Montulli was tasked with improving the "shopping cart," which enabled websites to track various items that customers selected for purchase.[37] There was, however, no way to identify individual customers. Every item selected for purchase and placed in the shopping cart appeared to the vendor with no association to an individual. At this point, online shoppers were only able to purchase single items. Montulli's idea, which came to fruition with the aid of John Giannadrea, another

[36] Turow, Joseph. *The Daily You.* p. 47-48.
[37] Turow, p. 47-48.

Netscape employee, was a small text file called a "cookie."[38] Websites would place cookies on a visitor's computer. These files had identification codes for each visitor along with other codes containing information about the user's clicks during each visit. When the same computer next accessed the website, browser tags would immediately remember the cookie. By decoding its information, the site was made privy to all of that user's previous clicks, what the customer had purchased, and even what had been placed in the user's shopping cart, regardless of whether the customer had clicked far enough and completed the purchase.

I am not suggesting that Montulli invented the cookie with the intent to collect individuals' data for any other reason than to make their shopping experience more streamlined, but the demand to sell products as efficiently as possible paid little concern to individual privacy. The Web that was evolving created enormous stores of data that were controlled by private capitalist corporations whose discretionary use of such data was entirely unregulated. It is worth noting again that the value of such information was, at the time, scantly realized -- especially by politicians. As the already lucrative practice of brokering information became exponentially more valuable with the creation of the Web, a full scale assault by corporate America on individual Web user privacy began.

Alone the cookie could not distinguish between different people using the same computer. Montulli decided to have the cookie implement its protocol without asking the person using the computer to accept it, its various functions, or the implications of those functions.[39] Consequently, Turow says, "this seamless approach had an ominous downside: by

[38] Ibid.
[39] Ibid.

not requiring the computer user's permission to accept the cookie, the two programmers were legitimating the trend toward lack of openness and inserting it into the center of the consumer's digital transactions with marketers."[40]

Netscape installed cookie-placement capability into its Navigator browser in late 1994. Microsoft incorporated it into its first Internet Explorer browser, released in 1995. The head of Microsoft's browser efforts, Michael Wallent, suggested that "to compete with Netscape Navigator, [which owned roughly a 70% market share] his company needed Web publishers and advertisers to conform to Internet Explorer's specifications;" otherwise large numbers of internet users would not adopt this browser.[41] If online companies were to support Explorer, he recalled in 2001, Explorer needed to support cookies: "I don't think that anyone ever thought that cookies were anything that could be excluded in the browser and have that browser become a success in the marketplace."[42]

The implication of Wallent's words supports a view that the very fabric of the World Wide Web was created in a way that surveillance of individual users was fundamental to its survival and expansion. Flowing from media buying demand to justify advertising expenditures in the 1980s and early 1990s, and affecting innovation in such a way that the very success of the Web's infrastructure was determined by its ability to effectively surveil, came awareness on the part of some innovators that we were at a dangerous crossroads.

[40] Ibid.
[41] Wallent, Michael In. Turow. *The Daily You* p. 48.
[42] Wallent in Turow, p. 48.

Some people realized that it simply did not have to be this way. There were very prescient individuals who—even before the mid-1990s—saw these trends developing. Although at times working at cross-purposes, both civil libertarian-minded tech innovators and privacy activists were conscious of the ominous downside to the free model of the Web that was evolving. They were also aware of just how invasive the data compiling industry was at that time. Most importantly, they were aware of the effects of the convergence of the free-advertising model of the Web and the data compiling industry. The emerging ecommerce terrain became for some of these privacy rights-minded individuals and other commercial interests the next and most important developing area of the Web. There would either be a continuance of the surveillance oriented Web infrastructure, or innovations that would oppose the growing trends and develop in a way that would place individual rights before profits.

Chapter 2: David Chaum and Ecash

One of these innovators was David Chaum. In the late Seventies, Chaum was already thinking about information technology and its future. At the time, he was pursuing his doctorate in computer science at the University of California, Berkeley, and he was devising "cryptographic protocols for establishing trust between mutually untrusting parties."[43] Chaum intuitively understood the aforementioned trends created by advertising demands and the consequential subservience of innovation that was beginning to build the nascent Web. His mission became to develop in such a way that that his technology would intrinsically protect its users' privacy, and he righty identified electronic commerce as an emerging structure to which his innovations could have a positive impact. That positive impact in his mind was protecting the privacy of individuals within a system, the growth of which was entirely predicated on its ability to surveil individual users.

Chaum's entire creative life was spent confronting this issue. He spent time teaching at New York University and the University of California, then, in 1990, Chaum founded Digicash. He sought to create a space in which ideas contrary to the notion that surveillance was a necessary condition for growth, could flourish. Digicash's first major innovation was a "system for automatic toll collection in which automobiles carry a card that responds to radioed requests for payment even as they are traveling at highway speeds."[44] It included a smart card installed in the dashboard. The card transmitted payment as the vehicle drove by, without ever slowing down or identifying the vehicle. This is unlike EZpass which requires the registration of

[43] Chaum, David. "Blind Signatures for Untraceable Payments." *Advances in Cryptology Proceedings of Crypto* 82.3 (1983): p. 199-203.
[44] Chaum, David. "Achieving Electronic Privacy." *Scientific American* 267.2 (1992): p. 98.

enormous amounts of personal information and the use of credit cards. From this innovation, Digicash went on to create its solution to the incipient demand for a payment system to handle the transfer of funds electronically over the Web, Ecash.

Ecash as Currency

All forms of money circulating in the United States are types of credit that also function as a medium of exchange. In effect, money is merely a subset of credit. For example, currency is a credit instrument because it is a liability of its issuer, the federal government. According to Bert Ely, "technically, a piece of currency is simply a small denomination, non-interest-bearing bearer bond of no fixed maturity that governments issue for just one reason—it provides interest-free debt financing."[45] Specie (i.e. gold and silver coins) is the only form of money that is not a form of credit, but such coins no longer circulate in market economies.

Checks are also a form of credit—they are liabilities of a bank—as well as a medium of exchange. Unlike currency, though, checking account balances finance bank assets, principally loans and investments. Travelers checks, such as those issued by American Express, likewise are credit instruments that are used to finance the issuer's debt. Debit cards, Ely said, "are not money; instead they are 'keys' that provide electronic access to checkable bank deposits."[46] As such, they can be used to issue electronic checks – they are "value transfer instruments" that *transfer* deposits from payer to payee.[47]

[45] Ely, Bert. "Electronic Money and Monetary Policy: Separating Fact from Fiction." In Dorn, James A. *The Future of Money in the Information Age*. Washington, D.C.: Cato Institute, 1997. P.101-102
[46] Ely, *The Future of Money in the Information Age*. p.101-102
[47] Ely, p. 102.

Ecash functioned in a similar fashion, as a value transfer instrument. It served as a currency when an existing fiat currency's value was transferred to it by a bank or financial institution. Essentially, when a person's bank account was debited and that money was transferred to a digitally implemented note within the Ecash system, that digital note could have been said to have all of the attributes of a currency. It was durable in the sense that unless the entire Web and its backup systems were all entirely lost it had utility in the same way cash did. It was divisible in the sense that it could be reduced to smaller denominations and it was convenient in that it all happened at the push of a button.

So why not just use a credit card? They seemed to accomplish the same thing: one can purchase goods on the Web – it is a way to transfer value. The difference was in the security, privacy, and anonymity that Ecash maintained and perhaps even enhanced over cash and credit cards. By enabling vendors to collect billing information for credit card use, individuals surrendered information about their spending patterns and personal tastes. This provided third party interests with the means to compile powerful stores of information on individuals in order to more effectively sell products.

How Ecash Works (See diagram in appendix)

In 1992, Chaum wrote an article for *The Scientific American.* In it, he discussed Ecash, his latest innovation in cryptography, and how that system functioned. Ecash implements digital notes, unique digital messages that a consumer withdraws from a bank. The notes are then transferred to a merchant, at which point the merchant can redeem them at the issuing bank.

Ecash enables this to be done in a way that the consumer is not identified to either the merchant or bank when the transaction takes place.[48]

Ecash employs blind signature cryptography based on digital signatures.[49] These signatures use two keys—a public and a private—to encrypt and decrypt messages. Private keys sign messages by encrypting them and public keys decrypt and verify those messages. Messages signed with private keys need the associated public key to be verified. Private keys are usually kept on private, personal computing systems and are presumed to be secure. The signer's public key is widely disseminated. So, "if Alice wants to send a signed message to Bob, she encodes it using her private key."[50] When Bob receives her signed message he applies her widely disseminated public key to verify that Alice in fact sent the message.[51]

These same digital signatures are used in the Ecash system to create digital bank notes. Denominations are simply messages signed by the bank using one of the bank's private keys. "All messages bearing one key might be worth a dollar, all those bearing a different key five dollars, and so on… These electronic bank notes [can] be authenticated using the corresponding public key, which the bank has made a matter of record."[52]

Say Alice wants to withdraw one dollar, she generates a random 100-digit number.[53] This serves as the note and it is signed with her private key. Once the bank has verified her signature, it utilizes a private key that is associated with the same denomination that Alice has

[48] Chaum, David. "Achieving Electronic Privacy." Scientific American 267.2 (1992): p. 96.
[49] Chaum, P. 96-97.
[50] Ibid.
[51] Ibid.
[52] Ibid.
[53] Ibid.

requested, in this case, one dollar, and it signs the note with that corresponding key. The note is then returned to Alice and her accounts are debited by one dollar. When purchasing goods with digital notes, Alice transfers a note to Bob, and in turn he forwards that note to the bank where the note's signature is verified. Bob's account is then credited for the amount associated with the note and a digitally signed "deposit slip" is returned to Bob by the bank. At this point, with proof of funds, Bob can confidently ship the purchased goods to Alice.[54]

In this system, one party cannot cheat another. In that sense, the system is said to have provided security to Alice, Bob, and the bank, but the system still lacks privacy.[55] By keeping track of the information associated with depositing and withdrawing individual notes, the bank can still link buyers and sellers. To remedy this Ecash employs blind signatures that Chaum analogizes with embossed envelopes. In this analogy the bank note created by Alice is hidden in a "digital envelope."[56]

When the bank receives the note it embosses the note within the digital envelope. The embossment is equivalent to a worth-one-dollar stamp. The bank then debits Alice's account and the embossed envelope is returned to her. At this point, Alice can remove the note and spend it. Since the bank never saw the note within the envelope—or the digital message with a blind signature—Alice can spend her money as if it were cash, with not only anonymity, but greater privacy.[57]

[54] Chaum, p. 96-97.
[55] Ibid.
[56] Ibid.
[57] Ibid.

The privacy effect of blind signatures is implemented mathematically – through a reversible cryptographic protocol.[58] The note is essentially a random number which is generated by the wallet software being run by Alice's computer. However, before the note (random number) is sent to the bank, the software multiplies it by a "random blinding factor." Upon receiving the note back from the bank with an authenticated value, Alice's wallet software divides the blinding factor back out which leaves her with the original generated number only. The bank's signature remains on the note and empowers Alice to spend her money. All this is done so that when Bob receives the note as payment from Alice, and forwards it to the bank to be verified, the bank recognizes its own signature, but does not recognize the note itself. To a third party, the entire process leaves no apparent connection between Alice and Bob.[59]

Digital notes, however, can be copied easily; as such, Ecash devised a system that ensures a note can only be spent once.[60] Though this may sound impractical, each bank involved in the Ecash system maintained a digital record of every spent note. Each and every note that is sent by a payee to the bank to be redeemed is checked against this digital record of spent notes before it is authenticated and sent back. If it has already been spent, the bank will inform the payee that the note has no value and the payee can cancel the transaction. If the note has not been spent it is authenticated and sent back, but not before it is added to the

[58] Chaum, p. 98.
[59] Ibid.
[60] Ibid.

digital record. At this point, the payee can either have his or her account credited or have new notes sent back to him or her.[61]

There is also some transparency to the system. Ecash offers anonymity, but it is "one-way."[62] During the transaction clearing process, and through the public and private key system, the payee is always identified to the bank, making all of the individual amounts received by payees available for all accounts. This may seem like a flaw in Chaum's privacy model, but he defended it as a measure that prevents crime. If the payer wishes, he or she can "reveal the original note and the blinding factor to the bank, and so permit the bank to link the note they signed for her to the note they redeemed for the seller, producing an irrefutable receipt."[63] In this way, those conducting illicit business transactions would become vulnerable to surveillance by law enforcement. Furthermore, if a digital note is stolen it cannot be used. If someone refuses to give you a receipt there is still proof that they deposited it. If it is lost, you can get your money and records back. The cryptographic challenges posed to counterfeiters rival those posed to those trying to break "the most sophisticated codes used to protect nuclear materials, military secrets, and other large-value wire transfers."[64] Perhaps you may be asking why this is so complex. "To compete with greenbacks," says Chaum. "The reason [hard] currency is so popular is that it combines verifiable authenticity with anonymity."[65]

---

[61] Ibid.
[62] Chaum, p. 99.
[63] Chaum, p. 101.
[64] Chaum, David. Statement to the House, Committee on Banking and Financial Services, Subcommittee on Domestic and International Market Policy, *The Future of Money,* Hearing, July 25, 1995 (Serial 104-27). Appendix p. 135. Available at: http://www.archive.org/stream/futureofmoneyhea01unit/futureofmoneyhea01unit_djvu.txt
[65] Pitta, Julie. David Chaum: The Cybermint, Forbes magazine, July 7, 1997, p.320

Chapter 3: "The Future of Money" and Media Portrayals of Ecash

With Chaum and Digicash firmly pushing Ecash to financial institutions, Visa and Mastercard looking to quash them and the like, and the US government ready to take a position on the new electronic marketplace, Chairman Castle convened the first "The Future of Money" hearing on July 25, 1995. The testimony offers varying perspectives and proposals that grapple with key issues associated with the impending ecommerce revolution. Among those whose testimonies are most relevant to this thesis are David Chaum, Rosalind Fisher, Executive Vice President of Delivery Systems for Visa U.S.A., Heidi Goff of Mastercard International Incorporated, David Van Lear, CEO of Electronic Payment Services Inc, and various House committee members including Carolyn Maloney, Sue Kelly, Edward Royce, and Chairman Michael Castle.

Republican Michael Castle hailed from the small state of Delaware which was known for its support of the technology sector via lawmaking, and encouragement of the financial services industry. He was governor there from 1985 until 1992 at which time he was elected to the House of Representatives. Castle took office January 3, 1993 and retained his seat until January 3, 2011.

The 104rd Congress saw the Republican Party take control of both the Senate and House of Representatives for the first time since 1950. The next four Congresses—with both houses under Republican control—were responsible for massive legislation aimed at deregulation, reaching their pinnacle in 1999 with the passing of the Gramm—Leach—Bliley Act also known as the Financial Services Modernization Act. In 1993, with an eye towards deregulation,

Michael Castle was made Chairman of the Subcommittee on Domestic and International Monetary Policy, and he began to focus the committee's efforts on electronic money, or e-money.

In the first "Future of Money" hearing before the Subcommittee on Domestic and International Monetary Policy, July 25, 1995 Ecash was presented by Chaum as a "privacy technology" which "allow[ed] people to protect their own information and other interests."[66] By "information and other interests" Chaum was referring to what has become popularly known today as data compiling which made possible targeted marketing campaigns. This allowed third party payment systems without sufficient privacy features to collect transactional information associated with the purchase of goods and share that information other interests. An example of this happens when Alice buys a crib for her unborn child and weeks later Alice receives promotions for other baby products in the mail from companies that were made privy to the transactional information associated with the purchase of Alice's crib. While this collected information was necessary to companies like Visa and Mastercard to prevent fraud and minimize risk, buyers became vulnerable to oppressive institutional scrutiny.

Chaum's opening statement described the moment as a decision in which "the core values we as a nation have fought for and continue to stand for are at stake."[67] In doing so, Chaum was implying that the decision between which technology the government should support was not merely a decision about choosing the most effective and secure means to

[66] Chaum, David. Statement to the House, Committee on Banking and Financial Services, Subcommittee on Domestic and International Market Policy, *The Future of Money,* Hearing, July 25, 1995 (Serial 104-27). Appendix p. 135. Available at: http://www.archive.org/stream/futureofmoneyhea01unit/futureofmoneyhea01unit_djvu.txt
[67] Chaum. *The Future of Money,* p. 134.

transfer money electronically. The decision was about protecting an individual's rights to privacy. Chaum's rhetoric—at a time when ecommerce was a tiny fraction of what it is today—may have seemed overstated in 1995. However, given what we know now about net security and third party digital surveillance capability, Chaum's testimony was particularly prescient. While the right to privacy is not explicit in the constitution, he not only fathomed the ensuing surge in digital, commercial transactions, but, in Ecash, accounted for the risks to individual privacy which he rightly equated with a constitutional threat by linking those risks to the "core values we as a nation had fought for."

At every turn in his testimony, Chaum diligently unpacked the implications and responsibilities associated with the necessary features of an online payment system. He defined security "simply [as] the protection of interests."[68] People had to protect their money and the banks needed to protect their exposure. He continued to impart that role of government was to maintain the integrity and confidence of the system. This view of security was common to all testifying about their innovative solutions to support monetized transactions within the rapidly growing ecommerce system; however, Chaum added a subtle twist. He said that with electronic cash it is the responsibility of government "to protect against systemic risk" and followed that the responsibility "cannot be left to the micro-economic interests of commercial organizations."[69] Chaum was acutely aware of the impetus provided by the advertising dollar – that the success of Web innovations was often inextricably linked with surveillance (i.e. cookies) and that surveillance could be the crux of the micro-economic interests of commercial

[68] Chaum. *The Future of Money,* p. 134.
[69] Chaum. *The Future of Money,* p. 134.

organizations. Protection against systemic risk was not unique to Ecash. All those testifying about their epayment solutions believed it to be necessary, but the shared definition only included technical flaws to the structure of the system such as tamper resistance. To Chaum, the system did not just include the electronic payment infrastructure, it included the Web and its commercial forces, which just so happened—by virtue of their function—to obliterate privacy. Chaum said, "In my view a sound architecture must, one, include…security…Two, prevent vulnerability…and three, address privacy concerns, effectively. Today, Digicash systems are alone in having these three attributes."[70] And above all, he believed that "protection" entailed an active role by government in supporting privacy technology.

Chaum's testimony then shifted to privacy concerns. He offered a robust vision of how privacy technology should function and what it should protect against. He said:

> Privacy technology allows people to protect their own information and other interests while, at the same time, maintains very high security for organizations. Essentially, it is the difference between, on the one hand, a centralized system with disenfranchised participants, like electronically tagged animals in feedlots, and, on the other hand, a system where each participant is able to protect its own interests, like buyers and sellers on a town market square[71]

The dystopian metaphor that Chaum employed referred to an ecommerce payment system in which credit cards like Visa and Mastercard conduct the transactions. The system was centralized in that a third party was necessary to complete every transaction between a buyer and seller. Every time an individual wanted to purchase an item, he or she must have handed all of their personal information over to Visa or Mastercard so that they in turn could pay the seller of the item; in that sense, they were electronically tagged and the system was

[70] Chaum. *The Future of Money,* p. 134.
[71] Chaum. *The Future of Money,* p. 134.

centralized. Ecash allowed buyers to send digital notes directly to sellers. They could in turn send those digital notes directly to the bank and have their accounts credited. Essentially, money has been exchanged just "like buyers and sellers on a town market square." Chaum chose to call buyers using credit cards online "disenfranchised" because they were denied the right to keep their online purchasing habits private. He had a full grasp on the extent to which purchase-related information, collected and shared among private industry with commercial interests, could infringe on individual rights to privacy.

Chaum's testimony continued with the purpose of alleviating other areas of government security concerns like lost or stolen Ecash, counterfeiting, and black market transacting. Ecash is superior to paper cash, he argued, because if it is stolen it cannot be used; if you are refused a receipt, you have proof of deposit; and if lost, your money and records can be retrieved.[72] "Counterfeiting poses the same cryptographic challenge as breaking the most sophisticated codes used to protect nuclear materials and military secrets," said Chaum.[73] And since anonymity is one-way, an extortionist is vulnerable to being revealed to law enforcement by his or her payee.

Chaum cited to the Committee a poll in which 82% of Americans expressed concern over privacy of computerized data. This was following the advent of computer-generated mailers with people's names printed on them, concerning products or services related to previous purchases regarding health issues. He not only believed in the right to privacy, but he

[72] Chaum. *The Future of Money,* p. 134.
[73] Chaum. *The Future of Money,* p. 134.

also believed that the vast majority of Americans wanted it, and would choose a system that was slightly more cumbersome in order to protect their privacy.

According to Chaum's testimony, Ecash, by the time of the Subcommittee's hearing, had received substantial media coverage. He said "the public is beginning to realize that the coming of electronic payments need not mean obliteration of privacy," and that such awareness coupled with growing concern over the privacy of computerized data is stimulating Ecash's success.[74] As the World Wide Web grew, so did consumer awareness of choices affecting the emerging infrastructure of a new global terrain – one that was linking the globe in ways never before known. In this climate, Chaum believed that government had two responsibilities. The first was to encourage and protect developments in privacy technology. The second called on government to further establish public confidence in these new technologies in order to protect against systemic risk; in this case, the risk was in control of individual privacy becoming subservient to "the micro-economic interests of commercial organizations." He suggested that if government succeeded in promoting and protecting privacy technologies they would see "economic growth and market leadership," and if they failed, global competition would surpass them.[75]

Digicash delivered a remarkably compelling technological solution. Its delivery system accounted for the interests of individuals, central banks, and law enforcement, as well as commercial businesses. Publically disseminated material at the time of the congressional hearings constructed Ecash as a technology that empowered the individual with respect to

[74] Chaum. The Future of Money, p. 134.
[75] Chaum. The Future of Money, p. 134.

organizations in the face of ever more fine-grained surveillance techniques, all while leaving intact the existing police and regulatory controls over the monetary system that protected society's interests.

There are two essential attributes to the cogency of this construction: anonymity and traceability, both discussed at length by Chaum. Ecash provided anonymity to the payer which would, preserve the level of privacy that people enjoy now by using cash. This level of privacy was not only "traditional, expected, and desired," said Chaum, but essential for the maintenance of the "core values of democratic participation and free markets."[76] At the same time, the system permitted the payee's identification to always be known. This, according to Chaum, in conjunction with nontransferability, will "maintain or improve the current level of protection of society's interests'."[77]

Chaum believed that because Ecash empowered individuals vis-à-vis organizations, its adoption would be driven by public demand. He believed many individuals wanted their privacy protected. As a technological innovator, he understood the risks inherent in commercial control of private, individual interests and that, in the electronic marketplace, those people should be afforded the same privacy features provided by hard currency, as they are in the traditional marketplace. However, most importantly, he grasped the magnitude of the impending ecommerce marketplace and process, the increasing volume of cyber-transactions, and growing capabilities of commercial and institutional scrutiny. Rep. Michael N. Castle, chairman of the Subcommittee hearings said "the intersection of technology and commerce has

[76] Chaum. The Future of Money, p. 136.
[77] Chaum. *The Future of Money,* p. 135.

been predicted to fall on almost every point along the continuum ranging from an over-hyped fad to change with implications as profound as the industrial revolution."[78] Chaum knew popular adoption might avail his company handsome profits and a place in the ecommerce market, and he certainly was in business to make money, but he also realized that not everyone had the same grasp on the depth of what was happening to the marketplace as people in 1995 knew it.

However, without the full support of government in the system's implementation and the traction from a government campaign to protect the privacy rights of citizens, Chaum's more substantial goal of empowering individuals fell short. To Chaum, then, the goal in participating in the "The Future of Money" hearings became his plea to government to support and protect the interests of individuals by embracing privacy technology, and further, openly supporting its implementation and continued use.

Visa – Rosalind Fisher

Rosalind Fisher and Heidi Goff, of Visa and Mastercard, respectively, gave very similar testimonies in which they discussed epayment solutions that had not yet been fabricated. Their testimonies relied on their deeply rooted market presence as companies that provided consumers credit access at brick and mortar vendors in order to give them authority over the emerging ecommerce terrain. This authority sets credit card companies with commercial interests as the central figures enabling electronic transactions – a position that made them the

[78] Castle, Michael. Chairman's opening remarks, Committee on Banking and Financial Services, Subcommittee on Domestic and International Market Policy, *The Future of Money,* Hearing, October 11, 1995 (Serial 104-27). Appendix. p. 1

gatekeepers of consumer and transactional data. Fisher and Goff also relied on promoting an open relationship with regulators and law enforcement in which they promised to offer access to consumer data through their member institutions, mainly banks that offer their credit cards. Another reference that was made often was that consideration to electronic payment services other than to credit cards or "regulated financial institutions" would result in loss of public confidence in the system.[79] Repeatedly Fisher alluded to the negative impacts from a loss in public confidence and she ascribed the effects of this loss to technological solutions other than those that are not currently regulated by government; by default, she implicated Chaum and Ecash. When they mentioned privacy and related concerns, there was little to no mention of consumer data, let alone anything about their current practices with such information. Most of their testimony to congressional members of the hearing opined their technology for "providing payment systems that offer consumers and merchants convenience..."[80] What little attention that was paid to privacy left the concept ill-defined.

Privacy innovators and especially Chaum had a clear vision of what privacy should look like. To Chaum, it was critical for the electronic payment system servicing the web to evolve as closely as possible to a natural marketplace in which consumers purchase products from vendors with hard currency. Privacy, then, for Chaum meant that there need not be any disclosure of personal or transactional information to a third party. The system lacked centrality in that a third party would not be made privy to consumer data. It was imperative for the electronic marketplace to evolve in this manner. The crucial component to Chaum's solution,

[79] Fisher, Rosalind. Statement to the House, Committee on Banking and Financial Services, Subcommittee on Domestic and International Monetary Policy. *The Future of Money,* Hearing, July 25, 1995 (Serial 104-27). Appendix p. 148. Available at: http://www.archive.org/stream/futureofmoneyhea01unit/futureofmoneyhea01unit_djvu.txt
[80] Fisher. *The Future of Money,* p. 149.

Ecash, prevented third party commercial interests from gaining access to such data. Banks would still affix digital notes with value by debiting consumer accounts, but with the blind signature technology employed by Ecash, banks would not be privy to the transactional information associated with purchases. A bank customer using Ecash technology to withdraw money from his or her account was similar in the bank's eyes to him or her withdrawing cash from an ATM. Chaum had created technology that achieved a clear depiction of privacy, and he made a cogent delivery to Congress of how his technology worked.

In in her testimony Fisher mentioned the word privacy very rarely. She said, "questions of security, risk and privacy are all crucial factors in the development of payment products and services" and later she mentioned it in the form of a question: "Does [our product] offer protection of data and privacy for its users? All of these questions must be answered and addressed before you have a business solution. And all of these factors are the crux of the goals of Visa…"[81] By failing to clearly define a vision of privacy, Fisher—and by extension, Visa—avoided any discussion of privacy concerns entailing their practices with consumer data. Fisher also admitted to Visa not having already fabricated any technological solution to the problem and merely stated that privacy—among other features—was the "crux" of their goals.

Similarly, Heidi Goff of Mastercard also avoided giving a clearly defined concept of privacy. She said "last year, we joined with Yankelovich Partners to assess the privacy concerns of today's consumers."[82] While Goff recognized that consumer data practices by credit card

[81] Fisher. *The Future of Money,* p. 149-150.
[82] Goff, Heidi. Statement to the House, Committee on Banking and Financial Services, Subcommittee on Domestic and International Monetary Policy. *The Future of Money,* Hearing, July 25, 1995 (Serial 104-27). Appendix p. 167. Available at: http://www.archive.org/stream/futureofmoneyhea01unit/futureofmoneyhea01unit_djvu.txt

companies were of concern to customers, she concluded her testimony merely by saying "we're currently working with our members to develop effective privacy guidelines."[83] Other than the recognition of the term "privacy" as a concern to consumers, Mastercard, like Visa, had not fabricated any technological solution to address a concern that was left ill-defined, privacy.

What is even more troubling about Visa and Mastercard's vague conception of privacy is that the context of their remarks left open other interpretations. Often, their usage seemed to conflate security issues with privacy issues, relating privacy to the prevention of unauthorized data interception or modification. From the hearings, the most blatant example of this came from David Van Lear who was the president of a credit card processing service, owned by five bank holding companies. He said "as to privacy, [when] all [transaction] information is within a single bank [and therefore protected from interception]…there is no major issue."[84] The most viable threat to the conception of privacy described here was from anonymous hackers and pirates who could steal proprietary information. This was contrary to Chaum's delivery of privacy which set the issue as a power struggle between individuals and organizations.

Fisher and Goff described an epayment system to support electronic transactions that functioned with a third-party commercial interest as a central figure necessary to complete transactions. To this point Fisher said "the integrity of the payment system, and the public confidence in it, could be at risk if so called 'electronic money' becomes nothing more than

[83] Goff. *The Future of Money.* p. 149-150.

[84] Van Lear, David. Statement to the House, Committee on Banking and Financial Services, Subcommittee on Domestic and International Monetary Policy. *The Future of Money,* Hearing, July 25, 1995 (Serial 104-27). Appendix p. 58. Available at: http://www.archive.org/stream/futureofmoneyhea01unit/futureofmoneyhea01unit_djvu.txt

zeroes and ones—digital signals—without the backing and central involvement of regulated financial institutions."[85] Fisher suggested that public confidence in the system depended on the regulation of financial institutions. Fisher was right to suggest that public confidence was important, but it should be questioned whether the only way to maintain public confidence was through government regulation of banks. In that system, where credit card companies and banks were the central figures, payment for good or services was rendered only after all of the information associated with each individual transaction was collected by the credit issuer (in this case, Visa or Mastercard). This left the customer vulnerable to having his or her information exchanged with data compilers. "Furthermore," said Fisher, "policymakers must be cognizant of the potential economic consequences that would result from a loss of public confidence in major unregulated, uninsured issuers."[86] While the potential economic consequences were never made clear by Fisher, to a body of lawmakers whom were relatively uncertain about the future of ecommerce, Fisher's testimony acted as a major deterrent to government support of unregulated privacy technology.

The other implication was that as member financial institutions and banks, subject to federal banking regulation, the government, including law enforcement, would also have access to consumer data. In fact, Fisher says "if it becomes necessary, working with law enforcement officials to trace something, we can do that with our system, and that is an important contrast, if you will, to what Dr. Chaum was talking about."[87] While this might have sounded agreeable as a protective measure to consumers, Ecash technology allowed for similar access to consumer

[85] Fisher. *The Future of Money,* p. 147.
[86] Fisher. *The Future of Money,* p. 155.
[87] Fisher. *The Future of Money*. p. 32.

data by government and law enforcement, but only at the behest of the consumer. The right to privacy according to Chaum should empower the consumer to choose to make transactional data available by sharing access to the encrypted transaction. In event the individual consumer made that choice, government and law enforcement would have gained access to the same information that they would have had the transaction been conducted with a credit card. The absence of choice in the Visa and Mastercard payment system left consumers to become passive actors in Chaums' metaphor of "a centralized system—with disenfranchised participants like electronically tagged animals in feedlots."

Fisher then said "while we must ensure such involvement, we caution that premature government regulation—or the failure to modify existing regulations to accommodate evolving technologies—could chill or halt the delivery of new financial products to consumers."[88] This spoke directly to Chaum's earlier point that it was the responsibility of government to protect against systemic risk and that this cannot be left to the micro-economic interests of commercial organizations. With Visa and Mastercard as the central figures of the payment system, consumers became vulnerable to systemic risk. By constructing an electronic payment system that was achieved through third party commercial centrality, and not clearly defining privacy and how privacy concerns would be alleviated in a technological solution, Fisher glossed over the concerns of commercial interests in control of consumer data. In the mid-1990s ordinary citizens and politicians were scarcely aware of the invasive practices of credit card companies with regard to collecting and exchanging personal and transactional data from consumers. The data compiling industry's activities were largely hidden from public scrutiny and they remain so

[88] Fisher. *The Future of Money,* p. 148.

today. Chaum stood alone in trying to impart to Congress the dangers in commercial interests as the sole facilitators of a new ecommerce system. Given the brief nature of each participant's testimony, avoiding a subject that was scantly realized in the first place was just enough to not induce action by government that would have addressed privacy concerns as they related to protecting consumer data from being abused by commercial interests.

Both Chaum and Fisher warned that overregulation would stifle innovation. Chaum said that "governments who stifle the new technology while it is still in its infancy…will be left behind in global competition."[89] However, Chaum's warning had one caveat: that government had to "proactively support needed infrastructure" that would protect individual privacy rights. He said "countries who take clear positions based on understanding of the technology, however, and encourage needed developments stand to gain enormous growth and market leadership."[90] In saying so, Chaum posited a payment system that would "harmonize with existing financial institutions," and create a boon for the American economy.[91] Fisher said "products and services such as those described here are in nascent stages and could be adversely impacted by overregulation…subjecting many of these products to government regulation could result in their premature death."[92] However, Fisher's caveat was that product development, "if shaped by regulation other than by market forces, would be stunted."[93] Her implication was that the existing market which was dominated by credit card companies should be allowed to work itself out. By both insisting that centrality was necessary and warning

[89] Chaum. *The Future of Money,* p. 136.
[90] Ibid
[91] Ibid
[92] Fisher. *The Future of Money,* p. 156.
[93] Ibid

Congress that overregulation would stifle innovation, Visa and Mastercard effectively posited themselves as the only viable, central figures to facilitate the system. Were that scenario to play out—and essentially it did—credit card companies would remain in control of the increasingly valuable flow of consumer data that they already monopolized, to the detriment of consumer privacy rights.

Fisher's comment regarding law enforcement is worth further discussion: she said "if it becomes necessary, working with law enforcement officials to trace something, we can do that with our system." Already in full force was an effort by the US government and law enforcement agencies to defend their traditional ability to intercept domestic and international communications in the form of Key Escrow, which was first presented by government in 1993. Their strategy was to assert an "Escrowed Encryption Standard" that employed a classified algorithm that was to be implemented on tamper-resistant chips ("Clipper Chips") with escrowed encryption keys.[94] This proposal was to provide a standard for confidential electronic communication, but also a set of "spare keys" (held in escrow) that could be accessed by law enforcement agencies "with the proper legal authorization."[95] Clipper Chips were forced onto the telecommunications industry and their use was not revoked until the Security and Freedom through Encryption Act was passed in 1997. With government already fighting a costly battle over encryption framed as a national security issue, Fisher was playing right to government interests. Access to consumer data for law enforcement was, and still is, a major priority of the state.

[94] Diffie, Whitfield, and Susan Eva. Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT, 1998. P. 216.
[95] Diffie and Landau. P. 216.

Ecash Portrayals in Mass Media

In an effort to add a more analytical focus to events concerning the non-adoption of privacy technology, this section considers Philips' research into mass media portrayals of Ecash, in order to establish the prevalence of Chaum's package elements. In doing so, a sense of the effectiveness of Chaum's delivery can be ascertained with the goal of drawing larger conclusions about the implications of privacy technology within free market politics. Chaum's issue package can be thought of as synonymous with "privacy and security through one-way anonymity."

Phillips generated a corpus of articles by the Nexis database with the criteria "HLEAD (Digicash) AND DATE>2/28/95 AND DATE <4/1/96".[96] Seventy one articles were returned. Of those, only certain publishers were used, among them were: the American Bankers Association, The American Banker, Lafferty, Faulkner and Grey, and the Financial Times. The publications were chosen because interviewees in the study had said that their coverage was "important, good, or influential."[97] The study also used national and international press reports, including articles from: *Popular Science, The Mail, PC-Computing, Newsweek, Business Week, The Times,* and *The New York Times.* The final corpus consisted of twenty three articles.

Phillips examined each article to determine whether or not it included the theme of "privacy and security through one-way anonymity," and how these anonymity features were conceptually linked to problems of privacy and security.[98] Only one article, an interview with

[96] Phillips, David J. "Digital Cash and the Surveillance Society." p. 109
[97] Phillips, 109.
[98] Phillips, p. 112.

David Chaum, reverberated a complete, integrated delivery of Chaum's package—that privacy issues set organizational surveillance opposed to individual autonomy, and Ecash technology solved this problem by providing payer anonymity, all while offering sound organizational security through payee identification. The remaining articles offered only fractured representations of the complete package. Seven articles suggested that an individual's right to privacy was solved by Ecash within a sociological context, but they did not address security issues.[99] Seven other articles briefly mentioned anonymity with regard to Ecash, but did not place it in any social context involving individual privacy. Eight articles failed to mention anonymity, privacy, or security, and depicted Ecash as either a tool or hurdle in various business strategies.[100]

Further analysis of the context in which the articles were situated revealed mostly fractured framing elements: several of the articles centered on the commercial use of payment systems, that is, their business function and the stratagems of innovators in their development.[101] The only social issue that the payment systems engaged was the need for a secure network payment mechanism. Of those articles that sought to place Ecash in a wider social context, the broader context was usually one of banks and government on the brink of ruin in the face of digital anarchy. Posing historically stable and foundational social institutions at risk of collapse surely inhibited a broader sense of acceptance for privacy technology.[102] For example, *Newsweek's* title asks "The End of Money? Probably not." *Business Week* was less ambivalent in this regard, recapitulating social change on par with that of the Industrial

[99] Phillips, p. 114.
[100] Ibid.
[101] Ibid.
[102] Phillips. P. 117.

Revolution. Each of the articles discussed privacy rights as a social issue, and each posed Ecash as a possible remedy, but in each, fear of currency collapse, counterfeiting, and institutional pandemonium overshadowed issues of individual privacy.

A summary of Phillips' analysis showed that although portions of Chaum's official package were located in media portrayals, the fractured nature of its representation severely diminished its rhetorical power. Ecash was likely to be addressed in the context of business strategies rather than within the realm of social problems, and even at times, the potential for catastrophic social reorganization was suggested by the authors.[103]

[103] Phillips. p. 117-118.

Chapter 4: Congressional Rhetoric as an Extension of the New Right and Market Populism

With memories of the Great Depression fading by the late 1970s and early 1980s, both liberals and conservatives increased support for economic deregulation. New financial institutions—including a burgeoning credit card industry—were gaining traction in the business community while existing financial institutions, especially the Wall Street investment banking industry became more sophisticated. In this climate, investment opportunities for middle-class consumers were on the rise, which precipitated federal banking agencies to allow greater freedoms to regulated financial institutions that were managing consumers' money. Among those institutions were Visa and Mastercard.

Banking regulation came under siege mid-way through the Carter Administration. His economic advisors urged Carter to consider banking deregulation as a category of "economic" regulatory reform. In doing so, *increased competition* became the crux of laissez faire rhetoric purportedly meant to benefit consumers.[104] However, the risks to consumers became lost in the growing movement towards deregulation. Among those risks, although hardly known at the time, were the effects of credit card companies exchanging consumer data, especially Visa and Mastercard. Credit card companies from the late 1970s to present day were among the leading proponents of deregulation. More important than deregulation being veiled by talk of increased competition, though, was how laissez faire or deregulatory rhetoric became entwined with politicians' and industry's newly forming conception of the Internet. As the World Wide Web and its future were being widely celebrated, its capabilities and purpose were

[104] McGarity, Thomas O. *Freedom to Harm: The Lasting Legacy of the Laissez Faire Revival*. London: Yale UP, 2013. p. 165.

being manipulated by politicians and industry leaders to form rhetorical devices for supporting the new right's deregulatory agenda. In 1995 this manifested in duplicity from Congressional members overseeing "The Future of Money" hearings along with Heidi Goff and Rosalind Fisher—each coopted laissez-faire rhetoric to carry out a larger agenda. In this case, towards and end in which emerging privacy technology would fizzle away, and Visa and Mastercard would be left to decide the fate of ecommerce.

Within the larger movement towards deregulation, the technology sector, mainly the manufacturing industry for computer technology experienced a transformation. According to Stanford communications professor Fred Turner, "by March of 1993, desktop computers had become common features of homes and offices nationwide, [and] the cost of computing was plummeting."[105] American economist Robert Gordon estimated that the price of computing power was decreasing roughly fifteen percent each year from 1987 to 1995, and from 1996 to 1999, that percentage decrease rose to roughly 31 percent. Microsoft and Intel were supplying software and hardware for a growing sector of computer manufacturers that included Dell, Compaq, and Gateway, and by 1995, "the Microsoft Windows operating system had become a global standard."[106]

As new powerful personal computers increased in availability, the privatization of the Internet backbone—a cluster of commercial networks—was occurring, along with a substantial increase in public computer networking.[107] According to Turner, in the early 1980s the Internet

[105] Turner, Fred. From *Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism.* Chicago: U of Chicago, 2006. P. 212
[106] Gordon, Robert. "Does the 'New Economy' Measure Up?" p.50
[107] Turner, Fred. *From Counterculture to Cyberculture* p. 213

backbone was government owned. The late 1980s saw a dramatic increase in academic utilization of the Internet which laid the groundwork for a transfer of ownership away from government and towards private interests.[108] Almost immediately, a series of commercial and alternative networks—aside from government sponsored academic work—had sprung, such that by the end of the 1980s, "millions of Americans were e-mailing one another, participating in online discussions, and posting information."[109] By April 1995, the government's National Science Fund Foundation "relinquished control of the Internet backbone," which facilitated the interlinking of commercial, alternative, and government-sponsored networks, and the mixing of for-profit and not-for-profit uses across the system.[110]

By the time this happened, another anomaly had grown in popularity on the Internet: the World Wide Web. In 1990, Tim Berners-Lee and colleagues of his at the Centre Europeenne pour la Recherche Nucleaire (CERN) created the Web. Turner said "the Web took advantage of the Internet's information transfer protocols to create a new system of information exchange."[111] With the use of hyperlinks and the new Universal Resource Locator (URL) system, Web users could maneuver data in ways they were not capable of doing before. Until now, the primary use of the Internet had been as a text messaging system. However, the World Wide Web changed that. Publishing information, incorporating multimedia formats, and quickly and

[108] Turner. p. 213.
[109] Ibid.
[110] Abbate, Janet. *Inventing the Internet*. Cambridge, Mass: MIT, 1999. P. 181.
[111] Turner, Fred. *From Counterculture to Cyberculture* p. 213

purposefully connecting spurious groupings of information were now primary modes of the Internet.[112]

In the beginning, Web use saw little growth and distribution of CERN Web software went primarily to the scientific community. However, in 1993, Mark Andreesen, a staffer at the National Center for Supercomputer Applications (NCSA) at the University of Illinois, and a small team, created a new Web browser called Mosaic. This new browser empowered users with the ability to embed hyperlinks in images and for the posting of those images to be in color; this was a first. Mosaic was made available to download publicly in November 1993 and in that first month 40,000 copies were had by Web users. By the spring of 1994, more than a million copies were improving Web user experiences around the country. The effect of Mosaic's proliferation was growth of the Web itself. "In April 1993, the Web featured only 62 servers; by May 1994, that number had ballooned to 1,248," according to Gordon.[113] In 1994 Andreesen left the University of Illinois and founded Netscape. The commercial browser manufacturing company had a product that improved on existing browsers in several categories: speed, security, and user-friendliness, all of which drove the ecommerce boon.[114]

During the ensuing five years, Internet and Web use grew immensely. This prompted speculators to drive up share values of Internet- and Web-related stocks to never-before-seen levels. Between 1995 and 1999, companies that generated little or no revenue experienced

[112] Turner. p. 213.
[113] Gordon, Robert J. "Does the "New Economy" Measure up to the Great Inventions of the Past?" *Journal of Economic Perspectives* 14.4 (2000): 49-74. p. 50.
[114] Turner, Fred. *From Counterculture to Cyberculture,* p.213-214

stock value increases topping out at nearly 3000 percent.[115] By the year 2000, the largest speculative bubble in American economic history had appeared. In its beginning, Americans had just cause for optimism: the Internet and World Wide Web were beginning to surge and the economy was expanding.[116]

However, computers and their use, in the business or home, did not drive the leap in growth and productivity. Most of it was achieved from increases in manufacturing durable goods which made up roughly twelve percent of the economy. Turner said "the use of computers—as distinct from the manufacture of computer hardware—had very little measurable effect on productivity."[117]

Regardless of where the economic growth originated, throughout the mid to late the 1990s, personal computers and especially the Internet had captivated the public's minds. It has been suggested many that this public sentiment evolved naturally, as part of the novelty of the Internet. However, British academic Nigel Thrift suggests "that by the end of the 1990s an entire circuit of stock analysts, journalists, publicists, and pundits had also emerged," which flooded the waves with self-prognostications that reinforced what analysts and investors were starting to agree on: computers were creating a "New Economy."[118] Turner added that now "more entrepreneurial forms of corporate organization, rapid investment in high technology, and the ability to corral the intangible knowledge and skills of employees—all seemingly made possible by the suddenly ubiquitous computer and communications networks—were

[115] Turner. p.214.
[116] Ibid.
[117] Ibid.
[118] Thrift in Turner. *From Counterculture to Cyberculture.* p.214.

transforming America and perhaps even bringing to an end the business cycle itself."[119] In 1999 even chairman of the Federal Reserve, Alan Greenspan, started to agree. With his unique phraseology, he explained that "a perceptible quickening of the pace at which technology innovations are applied argues for the hypothesis for the recent acceleration in labor productivity is not just a cyclical phenomenon or a statistical aberration, but reflects at least in part, a more deep-seated, still developing, shift in our economic landscape."[120]

The perception of a "New Economy" grew concurrently with a swing to the right in American politics and business.[121] Even though centrist democrat Bill Clinton controlled the presidency from 1993 to 2001, his time in office continued a long train of deregulatory legislation in industry and the scaling back of government. The 104th Congress wielded the first Republican majority in both the House and the Senate for forty years. With Newt Gingrich leading, the House of Representatives brought about government rollbacks and heavily deregulated the telecommunications sector. Gingrich and pundits argued that America was beginning a new era. Technology was about to make bureaucratic oversight in politics and industry, obsolete. According to Turner, "as Gingrich and others saw it, deregulation would free markets to become the engines of political and social change that they were meant to be."[122]

---

[119] Turner. p. 214-215.
[120] Greenspan, Alan. "The American Economy in a World Context," at the 35th Annual Conference on Bank Structure and Competition, Federal Reserve Bank of Chicago, May 6, 1999, available at http://www.federalreserve.gov/board-docs/speeches/1999/19990506.htm
[121] Turner. P. 215.
[122] Gingrich in Turner, *From Counterculture to Cyberculture.* p.214.

"Market populism," was the name that Thomas Frank gave to this futuristic mode of governance. In the 1990s it depended on how one saw the Internet. "If the market was to be a deregulated mechanism of political as well as economic exchange, the recently privatized circuits of the Internet, with their free-flowing streams of commercial and non-commercial bits, made a perfect rhetorical prototype of the market populist ideal," Turner said of market populism.[123] As the 1990s concluded, this libertarian, utopian, populist construct of the Internet had spread from Congress to individual Americans sitting in their kitchens, and from the Federal Reserve all the way to retail financial planners. But in the mid-1990s at the time of "The Future of Money" hearings it was just beginning.[124]

In August 1996, Gene Koprowski of Forbes Magazine wrote an article entitled "Rep. Mike Castle on E-Money: Let the Market Decide." In that article and about the chairman of "The Future of Money" hearings, Castle, Koprowski says he "has a deregulatory bent on finance. He believes the market should settle most questions before government gets involved…[and about the hearings] is not considering legislation…and prefers to let companies like Digicash and American Express work out the market through competition."[125] This was the general consensus in the media following the hearings in which Congress consistently vocalized a hands-off approach towards anything related to ecommerce.

After Chaum, Fisher, and Goff all gave statements, a question and answer portion of the hearing commenced. The format allowed for Congressional members to voice their concerns and clarify previous testimony. One of the very first concerns was brought about by republican

[123] Turner. p. 215.
[124] Ibid.
[125] Koprowski, Gene. "Rep. Mike Castle on E-Money: Let the Market Decide."*Forbes* 26 Sept. 1996: 72. Print.

House of Representatives member Hon. Edward Royce, who said, "there are two slightly contradictory observations that you have made here today," referring to both Chaum's and Fisher's testimony:

> One is that e-cash or digital money would best be shaped by market forces rather than regulation, that we should have as little regulatory burden as possible. At the same time, each of you have said that we need safety and soundness and a high degree of trust, and therefore a high degree of government control over this emerging process, with the exception of Ms. Fisher, who has suggested that we could use backing of regulated financial institutions in place of that evolution.[126]

At no point in Chaum's testimony did he mention or closely echo that "digital money would best be shaped by market forces." However, one of his most critical points was that government needed to play and active role in supporting privacy technology so that they would not be left alone to face market forces, and the "systemic risk" inherent to those forces which were driven by commercial interests—in this case the interests of Visa and Mastercard. Fisher's suggestion was more surreptitious. By using the backing of regulated financial institutions namely their member banks, to offer "safety, soundness, and a high degree of trust," Visa and Mastercard would accomplish two things. One, they would position themselves as a central figure in the new payment system allowing them to continue to log transactional data related to consumers. Second, Visa and Mastercard would become regulatory figures in the ecommerce terrain, deeming their services necessary in order for consumers to transact over the Internet. As such, Visa and Mastercard (along with other credit card companies) essentially would become the sole "market force," eliminating any possible competition from privacy

[126] Royce, Edward. Question and answer portion, Committee on Banking and Financial Services, Subcommittee on Domestic and International Monetary Policy. *The Future of Money,* Hearing, July 25, 1995 (Serial 104-27). Appendix p. 28. Available at: http://www.archive.org/stream/futureofmoneyhea01unit/futureofmoneyhea01unit_djvu.txt

technology innovators. Royce's analysis continued with a warning about government oversight, he said:

> So the basic assessment here is that it is government control of the emerging system that you are going to rely upon for that measure of safety and soundness. What I would argue, for you to think about, is that in the Western world, governments routinely debase their currency. Governments do a very bad job of managing the value of the currency. [127]

More to the point of Web innovations and their purposes being manipulated by politicians to support an agenda of deregulation, Royce then said:

> I was looking at it from the opposite perspective. I was in the hope that the evolution of digital money might bring pressure to bear on the existing monetary system to encourage an end to this debasement of the currency and that somehow the evolution of a new system would encourage and leverage for a stable unit of exchange. [128]

This was Turner's point: if the market was to be a deregulated mechanism of political as well as economic exchange, the recently privatized circuits of the Internet, with their free-flowing streams of commercial and non-commercial bits, made a perfect rhetorical prototype of the market populist ideal. In that sense, Royce was suggesting what Gingrich and pundits were simultaneously arguing, that America was beginning a new era. Technology, in this case, electronic cash, would, if Royce's rhetoric played out, bring pressure to bear on the existing monetary system to encourage better—or less—government oversight. As was said earlier, to Gingrich and others, deregulation would free markets to become the engines of political and social change that they were meant to be. Particularly troubling to Chaum and other privacy

[127] Royce. *The Future of Money.* p. 28.
[128] Royce. *The Future of Money.* p. 28.

innovators, and likely to the delight of Fisher and Goff, though, was the implication that Ecash and other privacy technology would be left to battle Visa and Mastercard for market share in the emerging electronic payment industry without support from government. One of the great failures of these proceedings and the way the electronic commerce system developed as a result of "free market" dynamics was that privacy came to be seen as an external issue to commerce, not as a critical component to its successful implementation.

Republican House of Representatives member Sue Kelly shared similar sentiments. She said "I am not so sure [this] is an appropriate place for government, because with the government regulations in place we may be micro-managing something that the market forces will micro-manage on their own."[129] To which chairman Castle replied "Absolutely. This whole hearing is not pursuant to legislation we are pursuing. It is basically to educate this Congress about what is happening, and I think…it is an evolving market and we should leave it alone."[130] Both Castle and Kelly reinforced a deregulatory agenda throughout the rest of the hearing, but Castle's proclamation about the goal of the hearings, that they were not pursuant to legislation and that their purpose was merely to educate, only further stymied Chaum's reasons for participating—to gain government support for privacy technology. While the delivery of Chaum's testimony was seemingly well-received, Castle's vocalization of inaction all but guaranteed that privacy technology was merely a novel fascination of a new right congress, and that in the new era of market populism, privacy rights would become subservient to market

[129] Kelly, Sue. Question and answer portion, Committee on Banking and Financial Services, Subcommittee on Domestic and International Monetary Policy. *The Future of Money,* Hearing, July 25, 1995 (Serial 104-27). Appendix p. 35. Available at: http://www.archive.org/stream/futureofmoneyhea01unit/futureofmoneyhea01unit_djvu.txt
[130] Castle. *The Future of Money,* p. 36.

forces. Nothing supported this view with more zeal than some of Chairman Castle's final words to Fisher and Goff:

> You picked, by the way, the right Congress. This is the most anti-regulatory Congress that has been around in years. In fact, we just got rid of one regulation on the floor about 10 minutes ago. We are more into deregulating than we are into putting in new regulations, so when you make a plea that this is a nascent industry just being born, just trying to get off the ground and regulation could hinder it, I think you probably will find that falls on ears that will listen well to it.[131]

The Future of Money hearings presented a problematic and clichéd solution by credit card companies for supporting electronic commerce. What Visa and Mastercard ended up accomplishing was a successful cooptation of the new right's push for deregulation of markets—both their rhetoric and agenda. In that sense, the argument for the transformation of credit cards—which were not devised to be used over the Internet—into a viable, secure mechanism for hosting electronic transactions was veiled by an argument that saw their emergence as leaders of the electronic terrain being owed to the naturalness of market competition. By invoking market populist rhetoric, and appeasing government concerns over security and surveillance, Visa and Mastercard created a situation where privacy innovators with superior products, but miniscule financing, were left to compete against industry giants, without the support of government institutions. In this case, American privacy concerns lost out to the new right's agenda of deregulation.

[131] Castle. *The Future of Money,* p. 36.

Chapter 5: The Nature of Free Market Politics and Social Movement

In the larger spectrum, regulatory debates framed in terms of "more" and "less" is not only specious, but it also tilts the argument toward conservative positions by positing intrusive structures of regulation as the free market.[132] In the finance industry over the past twenty years, pushes for deregulation have been shrouds for enacting rules and cover stories for decisions not to act, all starkly favoring corporate interests. According to Dean Baker, "in the US economy, there is no free market. It is just that structures that heavily regulate the economy are taken as inevitable."[133] Deregulation can be a principled position held by those who truly believe in a free market. However, it is not often that either position argues against regulation as such. The real issue is the structure of regulation, and how that affects economic outcomes.[134]

This provides insight as to why Visa and Mastercard pushed Congress for regulation of the new electronic payment system to be subsumed within the purview of existing financial institutions, mainly their member banks who issued credit cards to consumers. While simultaneously arguing for an unregulated market, but suggesting their own gain centrality, they were structuring the market to favor their own commercial interests—maintaining access to consumer data. Baker uses the example of Wall Streeters wanting one-sided regulation that provided them with government security blankets— he calls it the too-big-to-fail principle or TBTF—without any costs or conditions.[135] None of the Citigroup, Goldman Sachs, or J.P. Morgan

[132] Baker, Dean. *Taking Economics Seriously*. Cambridge, MA: MIT, 2010. p. 2.
[133] Baker. p. 3.
[134] Baker. p. 11.
[135] Baker. p. 12.

corps ever lobbied Congress for an explicit repeal of TBTF legislations. They were selective in lobbying for deregulation, and pushed when it was in their own commercial interests. While many on Wall Street were left unemployed as a result of the recession in the late 2000s, the hundreds of millions of dollars that were earned by bankers in the preceding years, especially by executives, were theirs to keep.

Why are regulatory debates so often miscast in terms extent when their structuring is the real issue? For conservatives, the answer lies in a popular American belief in the idea of free markets set against an old and deep-seeded aversion to government.[136] Since the early Sixties when covert, unlawful government operations first started to come to light, faith in government has been in constant flux. Knowing this, then, it will almost always be to one's advantage, to align political positions with support of the free market. For Visa and Mastercard, identifying the importance of providing the payment platform for electronic commerce necessitated a strategy that would eliminate competition in order to maintain their free-flowing streams of consumer data. "The Future of Money" hearings became a pivotal moment in their existence, one in which they could "structure" an emerging marketplace. Veiling their goals by aligning them with the dominant political current that championed free market ideology, allowed Visa and Mastercard to coopt political power to achieve their own ends.

The exceptional appeal of free-market doctrine, despite all its striking harms, is "that it still endures beyond all expectations. Its extraordinary powers, [Fred Block and Margaret Somers] believe, are rooted in its promise of a world without politics, a world of almost

[136] Baker. p. 12.

complete individual freedom where the role of government—so often feared as coercive and threatening to our rights—would be kept to an absolute minimum."[137]

Karl Polanyi believed that the market was imposed by government, and was not facilitated by the retreat of political power, nor was it something "natural."[138] Accordingly, although the new digital space and ecommerce were certainly never-before-seen, new markets, they always existed within the confines of financial and political institutions, and those institutions' regulations. More importantly, they were always being shaped by political and commercial interests, and by the socio-technical relationship constructs associated with the innovation of their infrastructures. Well before ecommerce became a viable way to purchase goods online, the advertising industry's demand to quantify successful advertising provided impetus for an invasive surveillance infrastructure, and well before the Internet ever powered up, data collecting proved extremely valuable.

Thus, this thesis speaks more broadly to the processes by which information has, over latter half of the twentieth century become increasingly subjected to commodity form. A commodity is something exchanged in a marketplace. According to Yovitz, two attributes enable things—including information— to become objects of trade, appropriability and valuability. "Appropriability is the capacity of being owned and valuability is the capacity of being assigned a market value in some standard unit."[139] The two criteria give rise to an unambiguous definition of commodity. In particular, the criteria can be used to determine if

[137] Block, Fred L., and Margaret R. Somers. *The Power of Market Fundamentalism: Karl Polanyi's Critique*. N.p.: n.p., n.d. p. 219.
[138] Block and Somers. p. 6.
[139] Yovits, M. C. *Advances in Computers*. Boston: Academic, 1994. P. 38.

something is an information commodity. The lack of government regulation over the commercial sector's discretion with consumer data, especially in the mid-1990's, allowed for consumer data to be appropriated in whichever way the commercial entity saw fit. Essentially, possession of data constituted ownership, and to a certain extent it still does today. The logic of quantification that took root in the online advertising industry lead to a series of innovations all aimed at creating value. Innovations like the "cookie," and new ways to measure consumer traffic such as click-through rates, created a new systems of valuation to assess data. From these roots, a new information commodity was developing with its loci residing in the nascent ecommerce industry.

Widening the scope, the effects of free market politics on the electronic marketplace in the latter half of the twentieth century saw a recasting of classical American economic theory into a new rhetorical prototype that featured and new electronic marketplace with endless possibilities, but governed by the same old principles. According to Karl Polanyi, the arrival of the market, specifically the subjection of labor, nature, and money to the commodity form, had an enormously destructive effect on "society" and individual freedom, and the same principles held true as information became increasingly subjected to commodity form.[140] The very idea of a truly free market, fundamental to liberal economic theory was, according to Polanyi, a "utopia" of the worst kind—when its fruition is even attempted, the action inflicts severe, "real" damage on society.[141] The market society, by subjecting social interaction to the contingency of contractual relations, abrades the non-contractual foundations of social order.

[140] Block and Somers. *The Power of Market Fundamentalism.* p. 83.
[141] Block and Somers. p. 101-102.

In this world, Adam Smith's Invisible Hand causes the Social Contract to become expendable.[142] In the developing information economy, more specifically in the realm of ecommerce, the most expendable part of social interaction was an individual's right to privacy.

According professors Fred Block and Margaret Somers, Polanyi thought that market liberal utopianism proceeded by ignoring that the market was in fact created and facilitated by political power.[143] "Getting rid of politics," democratic politics, at that, is the aim of those who prosper in market society.[144] In that sense, the market is always "embedded," not only in the political regime that brings it to fruition, but also embedded in a knowledge regime that shapes market society's intellectual culture and character. The market is a form of social interaction that is imposed and manipulated, politically, as well as cognitively framed as something "normal" and "natural." Polanyi was convinced that from the social devastation caused by market forces would come "protective countermovements."[145] This would result in a democratic socialist domestication of the market without it entirely dissolving, and by which society, as it were, would fight back. But how so, and what are the contingencies?

Globalizing frame alignment strategy: Ecash as a protective countermovement

Free market ideology legitimated the new right's policy of inaction—veiled as restraint in the public's best interest—towards supporting privacy technology that would have protected individual consumers. Allowing regulation of the electronic marketplace to fall under the purview of credit card companies—cloaked in the naturalness of market competition—vis a vis

[142] Block and Somers. p. 101-102.
[143] Ibid.
[144] Block and Somers. p. 31-34
[145] Ibid.

its member financial institutions, structured the emerging market place to benefit commercial interests just as Polanyi suggested. More specifically, transactional data had now become the lifeblood of a new information commodity that would subsist by positioning credit card companies as the facilitator of the new electronic payment system. Understanding privacy technology innovation in the 1990s within Polanyi's context of the free market prompts analysis into the Ecash movement to protect individual privacy rights from commercial interests as a "protective countermovement"-- as one side of what Polanyi presents as a "double movement:" on the one side, "the forces of laissez-faire justify an ever expanding process of commodification by invoking the utopian promise of a fully self-regulating market society free of politics. On the other, multiple social movements mobilize in opposition…by establishing institutional protections."[146] Phillips chronicles how Ecash's delivery fits the mold of a social movement.

The Ecash package delivered to Congress explicitly mentioned a strategy for its adoption. Chaum said will be driven not by institutional interests, but by consumer demand fueled by mobilized individuals. Therefore, according to Phillips, Chaum's delivery should be approached as a social movement organization.

Phillips cites Snow in defining micromobilization as the "range of interactive processes devised and employed by social movement organization and their representative actors to mobilize or influence various target groups with respect to the pursuit of collective or common interests."[147] Phillips partially attributes micromobilization to frame alignment, the "linkage or

[146] Block and Somers. p. 242.
[147] Snow in Phillips. "Digital Cash and The Surveillance Society." p. 207.

conjunction of individual and social movement organization interpretive frameworks."[148] Essentially, frame alignment is an exercise in coordinating the frames of the social movement organization and of its target groups.

Snow described four modes of frame alignment, including frame amplification and frame transformation. Frame amplification is the clarification or invigoration of an existing frame. Phillips says "it may include the identification, idealization, or elevation of one or more values, or the amplification of the importance of presumed structural relationships."[149] For example, amplification strategy may center on, and attempt to make more apparent the gravity of an issue, the placement of blame for a problem, or the possibility of change and the need for action. Frame transformation is a bid to forge and nurture new values, and to redefine already meaningful activities and events. Frame amplification solidifies the frames of a target group, while frame transformation endeavors to modify those frames.

By advocating the frame of "privacy with security through one way anonymity," Chaum used both amplification and transformation. By highlighting problems both of privacy and security, it amplified two formerly segregated and incongruent frames. Through his concept of one-way anonymity, it introduced a new, global, transforming frame through which to understand the relation of privacy and security, and the mediating power of Ecash in that relation. Phillips said "it is thus an attempt to induce social movement – to create a new

[148] Snow in Phillips. p. 207.
[149] Phillips. p. 208.

'cognitive praxis,' to open a new 'cognitive territory,' a new conceptual space that is filled by a dynamic interaction between different groups and organizations."[150]

The new global frame must be compelling enough within each social group to spur mobilization. Oppositional frames are "collective action frames," they "inspire and legitimate social movement activities," they underscore justice, specify blame or causality, and suggest the means of resolution.[151] "In a globalizing tactic, the persuader must convince different groups of almost diametric types of injustice. Yet it must also be temperate and accommodating of the histories and concerns of all of these groups."[152] In the case of Ecash, the ardent "anarcho-capitalist" view and civil libertarian principle, both at the forefront of privacy technology innovation, must be convinced of the injustice of tax evasion and bribery, along with other economic dysfunction and societal ills that could possibly skew from the protective purpose privacy innovation. All the while, ardent "defenders of the State" and new right political agents must be convinced of the injustice of panoptic surveillance.[153] While pieces of the package might be accepted by either group, neither willingly accepts the package in its entirety. Meanwhile, econsumers must be convinced that information imbalance is a social ill worthy of personal corrective action. A social movement in support of Ecash proved difficult to cohere.

Ecash had one, explicit and consistent construction. Phillips said "it is a 'privacy technology' – a mathematical solution to a social problem and" "its necessity sprung directly

[150] Phillips. p. 219.
[151] Phillips. p. 222.
[152] Ibid.
[153] Ibid.

from privacy concerns."[154] Chaum presented it as historically rooted in democratic values and recognized cash as a historical arbiter of those values. In Ecash, he recreated that role in a new and threatening (to some) technological context, supported by an unfamiliar digital medium; only, Ecash had not achieved what Bijker termed "technological closure."[155] This occurs when "consensus among the different relevant social groups about the dominant meaning of an artifact emerges and the 'pluralism of artifacts' decreases."[156] "Closure results in one artifact - that is, one meaning as attributed by one social group - becoming dominant across all relevant social groups."[157] Once closure has occurred and the artifact has become obdurate, it can be used as a model within other technological frames. A model artifact "forms part of the hardened network of practices, theories and social institutions."[158]

Phillips suggests that cash—paper notes and coinage—has become one of these model artifacts. It is stabilized, unreflectively used and completely understood within a wide range of practices. It has a set meaning within the technological frames of multiple social groups involved in payment system negotiations, and its qualities as a model are used by actors to strategically position new systems within existing frames.

The Digicash strategy for adoption relied on patent restrictions to curtail use by institutions that would "not only provide social legitimacy and cachet," but also curtail use to that condoned by Digicash.[159] These patents acted as a stopper on the activities of activist

[154] Phillips. p. 90.
[155] Bijker in Phillips. p. 211.
[156] Ibid.
[157] Ibid.
[158] Ibid.
[159] Phillips. p. 195.

users who comprised social groups. This stopper was an attempt to "mainstream" use, but it also set up tension with other organizations that may have provided impetus for mainstream adoption.[160] This tension grew from simultaneously seeking legitimacy while also striving to compel fringe adopters. These fringe adopters, many of whom aligned with anarcho-capitalist and civil libertarian principles were essential in creating awareness which would have brought more general demand, but the awareness that they generated was often contrary to Digicash's aims. In general, anarcho-capitalists and civil libertarians shied away from tactics of legitimation, some because of anarchic ideology which related law and its enforcement with violence and coercion, and others because of an expectation that technical systems themselves would, in time, render state actions irrelevant by creating a diversion around structures of law and policy.[161] For these actors, technologies formed the groundwork of their resources of control—"cryptography not only provided a certain functionality which participants in the market found attractive enough to pay for, it also provided the means by which applications incorporating that functionality could be protected so that users generated income for the developer."[162] Technical systems, especially decentralized networks like the Internet, also splintered and disrupted the market, essentially discharging that market structure from the control of state structure.[163]

Digicash was not interested in "mobilizing legitimation resources, except to enforce its patents," and to "persuade those who commanded legitimate power" (policy makers, regulators, and law enforcement) that Ecash aligned with their interests within the confines of

[160] Phillips. p. 195
[161] Phillips. p. 204.
[162] Ibid.
[163] Ibid.

democracy.[164] However, that persuasion failed. Only those segments of the argument which presented the erosion of privacy as a social problem were reflected in Congress's concerns. During "The Future of Money" hearings, at no point did any Congressional members show that they accepted Ecash as a solution to those problems, or that they recognized Ecash as viable protection for state power.[165]

Digicash's adoption strategy for Ecash dealt with the economic superiority of large banking interests by believing that its cogent solution would incite consumer demand, and that the Internet would circumvent market barriers which kept smaller banks from filling that demand.[166] At the same time, however, it was "dependent on the signification resources that larger banks brought: the reputation they carried which stimulated trust and use."[167]

Digicash's construction of Ecash was relatively complex. As such, different social groups accepted the parts they favored and ignored the others.[168] According to Phillips, in the press, Ecash was often referred to as anonymous, but the complexities of one-way anonymity were rarely fleshed out. Some Congressional members accepted privacy as a social issue, but their understanding still held privacy and security in tension; this was evident in the hearings. Certain activist users incorporated blind signatures, but dismissed clearing and payee identification. The aggregate of evidence, both from Phillips' research and my own, offers no proof that any group, other than Ecash's developers, understood the Ecash system as an adequate solution to any of the problems facing ecommerce. Moreover, in the press there was correlation of Ecash,

[164] Phillips. p. 196.
[165] Ibid.
[166] Ibid.
[167] Ibid.
[168] Ibid.

anonymity, and social danger.[169] Though "Digicash's tactics required general consumer awareness and demand to prompt institutional adoption, the media chose to disseminate only fragmented versions of the Ecash construction."[170] The perpetuation of fragmented technological frames created barriers to social movement and prevented Ecash from achieving any semblance of technological closure.

Interestingly, while privacy technology was struggling to mobilize support in opposition to commercial interests in ecommerce, another battle was taking place over non-government use of strong cryptography. This was discussed earlier in relation to Fisher's comment about access to consumer data for law enforcement. The end result of that struggle was brought about by significant social movement. The Clipper standard failed under a storm of protest from *both* civil liberty *and* business interests. Diffie and Landau, who wrote extensively on the battle over strong encryption, said "fortunately, the fight for cryptographic freedom, unlike the fight against credit card databases, is a fight in which privacy and commerce are on the same side."[171]

For commercial interests, the desire for strong cryptography manifested from the need to protect valuable data from being transmitted to its relative business interests. For individuals, the need for strong encryption manifested from the desire to protect their right to privacy. In this battle a consensus was reached among the different relevant social groups about the dominant meaning of encryption. For all involved in fighting Key Escrow,

[169] Phillips. p. 196.
[170] Phillips. p. 223.
[171] Diffie and Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*. p. 239.

cryptographic freedom was about self-preservation, and both individuals' and commercial organizations' rights under democracy.

Conclusion

"The Future of Money Hearings" were some of the first public forums in which discourse occurred among policy makers, privacy technology innovators, and commercial interests over the structuring of the payment platform that was to facilitate the digital marketplace. The trajectories that were set by this discourse for implementing the electronic payment system had long lasting, detrimental effects on individual privacy rights. That detriment stemmed from the convergence of free market ideology with commercial interest's assimilation of the virtually endless capabilities that developed from the advent of the Internet.

The decisions made at the time of the hearings firmly entrenched an already rapidly growing, insidious trend in which consumer data was becoming the lifeblood of marketing campaigns by banks and credit card companies, as well as the crux of the data compiling industry's practice of layering information on consumers. Data compilers like Acxiom and their relationship with banks, credit card companies, and other sources of consumer data enabled the creation some of the most detailed and invasive dossiers on individuals ever known—so detailed that commercial interests gained the ability to predict individual consumer purchasing behavior with enough certainty as to exponentially increase their sales, often preying on the individuals who can afford to make those purchases the least.

Compared with more traditional media, the Internet is woven into people's lives in a more intimate way as it connects people with organizations and institutions, and of course, people with people. Gradually, "the applications of new technologies have eroded the distinction between public and private space and comprised the very idea of private space by

establishing long-lived interconnections among formerly separate spaces."[172] As a result, consumers are no longer able to depend on their intuitive sense of space and presence that guides their observable behavior to ensure that they are not surveilled, thus diminishing the privacy barrier even further. As the Internet continues to become more interlinked, these distinctions of space will only continue to become more blurred.

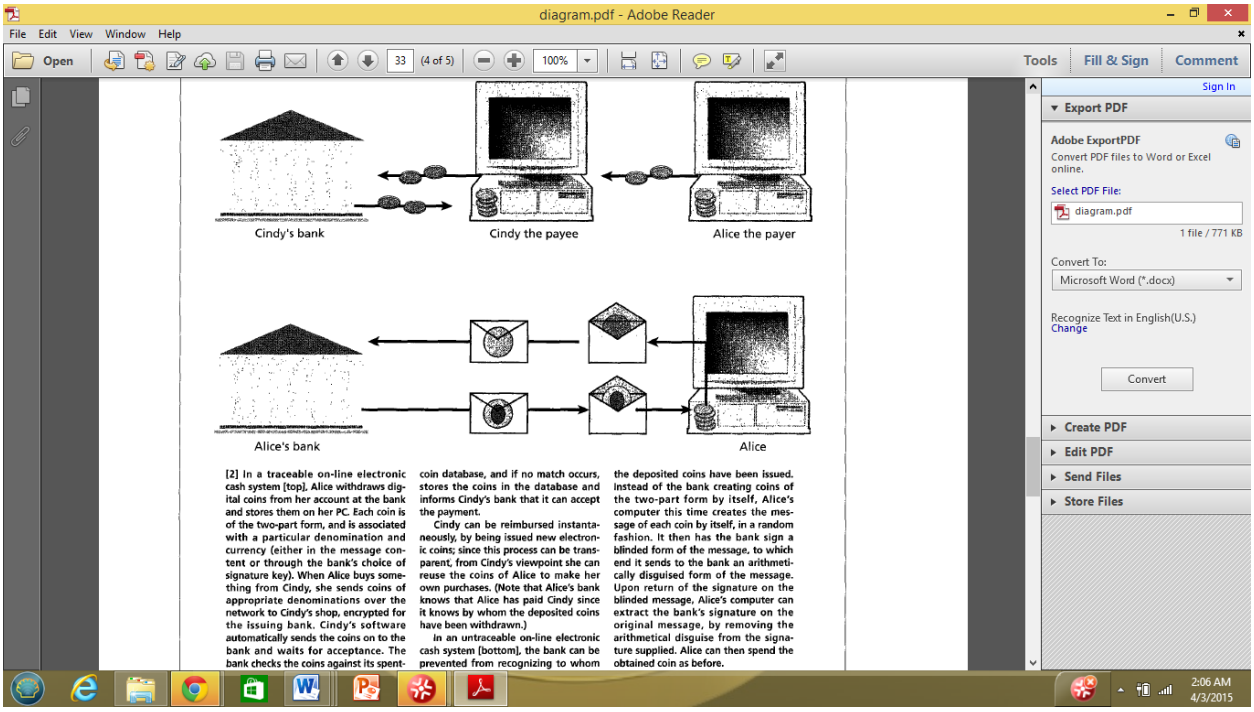
One of the more remarkable findings of this thesis is just how prescient David Chaum's technological innovations were in the late 1980s and 1990s. At a time when the World Wide Web had not yet been subsumed by the free advertising model, the ability to fabricate what could have been a viable, structural counterforce that engaged virtually all of the most invasive practices that plague even today's consumers with regard to privacy, certainly speaks to a deep and sweeping perception by Chaum of the nature of free market politics, and how those forces were going to interact with the new digital medium.

The failure of Ecash and other privacy technologies despite their technological viability speaks to the very nature of political, cultural, techno-social contingencies. They are just that: conditions, uncertainties, and chance events. In some cases, these are failures of framing, and in others, a case of unfortunate timing with regard to the public and political climates in which the technologies were developed and deployed. In other cases, much more troubling ones, direct political forces caused the defeat of widespread privacy technologies in favor of commercial interests, and by extension the interests of the governmental surveillance apparatus that would take advantage of the collation done by various corporations. Free

[172] Bellotti, Victoria. "Design for Privacy in Multimedia Computing and Communications Environments." In Agre, Philip, and Marc Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT, 1997. P.

market ideologues conveniently interpreted the government's long standing mandate to promote trade and commerce as a laissez-faire commandment set in stone, instead of as a responsibility to protect both public and individual interests as aggressively as those of corporations and the government itself. This interpretation became a policy of inaction towards legislative support for privacy technology in the mid-1990s. As civil libertarian principles gain traction, especially on the Web, Ecash-like privacy technologies are becoming more and more appealing as solutions to increasingly invasive and unpopular data collection, and abuse of privacy expectations. How these solutions are implemented, to say nothing of whether they will be, is likely, based on this research, a techno-social question. Will proponents of new-age digital cash be able to deploy the types of universally accepted, global frames necessary to crosscut the many social barriers and encourage a wide enough adoption to make a meaningful market alternative? As more and more privacies erode for the individual, the exigency in resolving the political, cultural, and techno-social contingencies that so often hamper social mobilization has never been stronger.

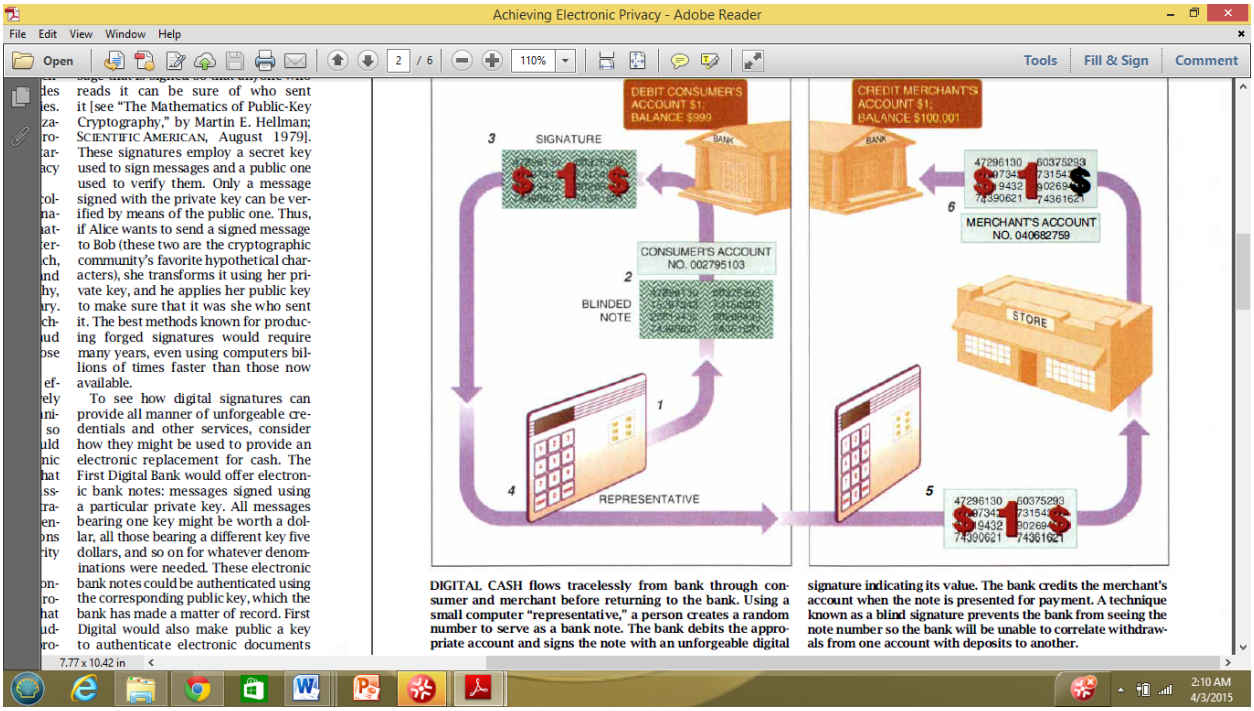
Appendix:



[2] In a traceable on-line electronic cash system [top], Alice withdraws digital coins from her account at the bank and stores them on her PC. Each coin is of the two-part form, and is associated with a particular denomination and currency (either in the message content or through the bank's choice of signature key). When Alice buys something from Cindy, she sends coins of appropriate denominations over the network to Cindy's shop, encrypted for the issuing bank. Cindy's software automatically sends the coins on to the bank and waits for acceptance. The bank checks the coins against its spent-coin database, and if no match occurs, stores the coins in the database and informs Cindy's bank that it can accept the payment.

Cindy can be reimbursed instantaneously, by being issued new electronic coins; since this process can be transparent, from Cindy's viewpoint she can reuse the coins of Alice to make her own purchases. (Note that Alice's bank knows that Alice has paid Cindy since it knows by whom the deposited coins have been withdrawn.)

In an untraceable on-line electronic cash system [bottom], the bank can be prevented from recognizing to whom the deposited coins have been issued. Instead of the bank creating coins of the two-part form by itself, Alice's computer this time creates the message of each coin by itself, in a random fashion. It then has the bank sign a blinded form of the message, to which end it sends to the bank an arithmetically disguised form of the message. Upon return of the signature on the blinded message, Alice's computer can extract the bank's signature on the original message, by removing the arithmetical disguise from the signature supplied. Alice can then spend the obtained coin as before.



reads it can be sure of who sent it [see "The Mathematics of Public-Key Cryptography," by Martin E. Hellman; SCIENTIFIC AMERICAN, August 1979]. These signatures employ a secret key used to sign messages and a public one used to verify them. Only a message signed with the private key can be verified by means of the public one. Thus, if Alice wants to send a signed message to Bob (these two are the cryptographic community's favorite hypothetical characters), she transforms it using her private key, and he applies her public key to make sure that it was she who sent it. The best methods known for producing forged signatures would require many years, even using computers billions of times faster than those now available.

To see how digital signatures can provide all manner of unforgeable credentials and other services, consider how they might be used to provide an electronic replacement for cash. The First Digital Bank would offer electronic bank notes: messages signed using a particular private key. All messages bearing one key might be worth a dollar, all those bearing a different key five dollars, and so on for whatever denominations were needed. These electronic bank notes could be authenticated using the corresponding public key, which the bank has made a matter of record. First Digital would also make public a key to authenticate electronic documents

DIGITAL CASH flows tracelessly from bank through consumer and merchant before returning to the bank. Using a small computer "representative," a person creates a random number to serve as a bank note. The bank debits the appropriate account and signs the note with an unforgeable digital signature indicating its value. The bank credits the merchant's account when the note is presented for payment. A technique known as a blind signature prevents the bank from seeing the note number so the bank will be unable to correlate withdrawals from one account with deposits to another.

Works Cited

Published Government Documents

The Future of Money, 104th Cong. (1995) (testimony of JAMES A. LEACH, Iowa, Chairman BILL McCOLLUM, Florida, Vice Chairman MARGE ROUKEMA, New Jersey DOUG BEREUTER, Nebraska TOBY ROTH, Wisconsin RICHARD H. BAKER, Louisiana RICK LAZIO, New York SPENCER BACHUS, Alabama MICHAEL CASTLE, Delaware PEIER KING, New York EDWARD ROYCE, California FRANK D. LUCAS, Oklahoma JERRY WELLER, Illinois J.D. HAYWORTH, Arizona JACK METCALF. Washington SONNY BONO, California ROBERT NEY, Ohio ROBERT L. EHRLICH, Maryland BOB BARR, Georgia DICK CHRYSLER, Michigan FRANK CREMEANS, Ohio JON FOX, Pennsylvania FREDERICK HEINEMAN, North Carolina STEVE STOCKMAN. Texas FRANK LoBIONDO, New Jersey J.C. WATTS, Oklahoma SUE W. KELLY, New York HENRY B. GONZALEZ, Texas JOHN J. LaFALCE, New York BRUCE F. VENTO, Minnesota CHARLES E. SCHUMER, New York BARNEY FRANK, Massachusetts PAUL E. KANJORSKI, Pennsylvania JOSEPH P. KENNEDY II, Massachusetts FLOYD H. FLAKE, New York KWEISI MFUME, Maryland MAXINE WATERS, California BILL ORTON, Utah CAROLYN B. MALONEY, New York LUIS V. GUTIERREZ, Illinois LUCILLE ROYBAL-ALLARD, California THOMAS M. BARRETT, Wisconsin NYDIA M. VELAZQUEZ, New York ALBERT R. WYNN, Maryland CLEO FIELDS, Louisiana MELVIN WATT, North Carolina MAURICE HINCHEY, New York GARY ACKERMAN, New York KEN BENTSEN, Texas BERNARD SANDERS, Vermont DAVID CHAUM, Digicash, DAVID VAN LEAR, EPS, WILLIAM MELTON, Cybercash, ROSALIND FISHER, Visa USA, HEIDI GOFF, Mastercard, SCOTT COOK, Intuit, Inc). Print.

Primary Source Material

Chaum, David. "Achieving Electronic Privacy." *Scientific American* 267.2 (1992): 96-101. Web.

Chaum, David. "Blind Signatures for Untraceable Payments." *Advances in Cryptology of Crypto* 82.3 (1983): p. 199-203.

Digicash. *World's First Electronic Cash Payment over Computer Networks.* Publications from Digicash, 27 May 1994. Web. 3 Apr. 2015. <http://www.di.unipi.it/~gervasi/ISLP9697/www.cli.di.unipi.it/~pratesil/progetto/bibliogr/D6giCash%20publications%20-%20first%20e>.

Greenspan, Alan. "The American Economy in a World Context," at the 35th Annual Conference on Bank Structure and Competition, Federal Reserve Bank of Chicago, May 6, 1999, available at http://www.federalreserve.gov/board-docs/speeches/1999/19990506.htm

Koprowski, Gene. "Rep. Mike Castle on E-Money: Let the Market Decide."*Forbes* 26 Sept. 1996: 72. Print.

Pitta, Julie. "David Chaum: The Cybermint." *Forbes Magazine* July-Aug. 1997: 32. Web.

Walters, Dixie. "Blazing an International Technology Trail: Impressive Developments Continue with Acxiom, Arkansas Systems, Systematics." *Arkansas Business* 29 Aug. 1994: n. pag. Web.

Secondary Source Material

Abbate, Janet. *Inventing the Internet*. Cambridge, Mass: MIT, 1999. Print.

Agre, Philip, and Marc Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT, 1997. Print.

Baker, Dean. *Taking Economics Seriously*. Cambridge, MA: MIT, 2010. Print.

Bellotti, Victoria. “Design for Privacy in Multimedia Computing and Communications Environments.” In Agre, Philip, and Marc Rotenberg. *Technology and Privacy: The New Landscape*. Cambridge, MA: MIT, 1997. P.

Block, Fred L., and Margaret R. Somers. *The Power of Market Fundamentalism: Karl Polanyi's Critique*. N.p.: n.p., n.d. Print.

Diffie, Whitfield, and Susan Eva. Landau. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: MIT, 1998. Print.

Dorn, James A. *The Future of Money in the Information Age*. Washington, D.C.: Cato Institute, 1997. Print.

Ely, Bert. "Electronic Money and Monetary Policy: Separating Fact from Fiction." *Cato Journal* 13.3 (1994): 413-36. Web.

Gordon, Robert J. "Does the “New Economy” Measure up to the Great Inventions of the Past?" *Journal of Economic Perspectives* 14.4 (2000): 49-74. Web.

McGarity, Thomas O. *Freedom to Harm: The Lasting Legacy of the Laissez Faire Revival*. N.p.: n.p., n.d. Print.

O'Harrow, Robert. *No Place to Hide*. New York: Free, 2005. Print.

Packard, Vance. *The Naked Society*. New York: D. McKay, 1964. Print.

Phillips, David. "Digital Cash and the Surveillance Society." Diss. U of Pennsylvania, 1998. Print.

Turner, Fred. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago: U of Chicago, 2006. Print.

Turow, Joseph. *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your worth*. New Haven: Yale UP, 2011. Print.

Yovits, M. C. *Advances in Computers*. Boston: Academic, 1994. Print.