Journal of International and Comparative Law

Volume 5
Issue 2 *Volume 5, Spring 2015, Issue 2*

Article 4

March 2016

Pick-Pocketing: A Thing of the Past the New Risk of Data Security Breaches and Identity Theft - Content Hoarding in the Digital Age - The Web Does Not Forget

Fatima Arash

PICK-POCKETING: A THING OF THE PAST THE NEW RISK OF DATA SECURITY BREACHES AND IDENTITY THEFT – CONTENT HOARDING IN THE DIGITAL AGE – THE WEB DOES NOT FORGET

Note

Fatima Arash[1]

INTRODUCTION

Hackers have exposed the personal information of 110 million Americans' – roughly half of the nation's adults – in the last twelve months alone.[2] The exact number of affected accounts is hard to pin down because some companies like Target, United Parcel Service, and The Home Depot are unlikely to release information relating to a breach until several weeks, months, or even years later. [3] Popular sites like eBay, Facebook, and Amazon can retain user information indefinitely and sell it to other companies.[4] The law increasingly requires private companies to disclose data breaches for the benefit of consumers.[5] By disclosing the events of a breach consumers are able to take safeguards for identity theft prevention. This Article finds that the current law in the United States is incomplete. Americans' lives are increasingly online. The impact of social

[1] J.D. Candidate, 2015, St. Johns University School of Law; B.S., 2011, St. John's University.

[2] *See* Jose Pagliery, Half of American Adults Hacked this Year, (May 28, 2014 9:25 AM), *http://money.cnn.com/2014/05/28/technology/security/hack-data breach/index.html?iid=SF_T_River. See also* Steven A. Hetcher, *The Emergence of Website Privacy Norms,* 7 MICH. TELECOMM. TECH. L. REV. 97(2001)("[W]ebsites have benefitted through the largely unrestricted collection of personal data while consumers suffered injury due to the degradation of their personal privacy from this data collection. In other words, degradation of consumer privacy resulted as a third-party externality of free-market data-collection norms of the website industry.").

[3] Many breaches are disclosed by third parties, and not by the corporation. The Target breach was first exposed by cyber security blogger Brian Krebs through his site KrebsonSecurity.com. *See* Brian Krebson, Sources: Target Investigating Breach, (December 18, 2013 2:33 PM), *http://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/.* As a result of his efforts, Sony Pictures Entertainment Inc. confirmed that it is working on a movie based on the security blogger. *See id.*

[4] eBay.com Privacy Notice, eBay, http://pages.ebay.com/help/policies/privacy-policy.html (last updated Sep. 15, 2014); Data Use Policy, Facebook, https://www.facebook.com/policy.php (last updated Nov. 15, 2013); Amazon.com Privacy Notice, Amazon, http://www.amazon.com/gp/help/customer/display.html?nodeId=468496 (last updated Mar. 3, 2014).

[5] Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913 (2007). There are many different disclosures required by law. *See id.*

media and new technology has led to our shopping, banking, medication, and even dinner to be ordered online. The days of walking into a retail establishment are coming to an end. Because our lives are increasingly conducted online, consumers are entitled to secure and responsible handling of their personal data. The United States Constitution has long recognized that privacy interests coexist alongside fundamental First Amendment rights to freedom of speech, freedom of the press, and freedom of association. Companies should not be allowed to store private information such as names, addresses, date of birth, social security numbers, and credit card information indefinitely. Limits must be placed on the storage, dissemination, and the transport of such data to other countries. Consumers should have the 'right to be forgotten' online, when the information retained has become inaccurate, inadequate, irrelevant or excessive. A 'right to be forgotten' [6] will allow consumers easier access to their data, more control over their personal data, as well as the right to have data deleted when there are no legitimate grounds for the company to retain it. [7] Additionally, this rule empowers consumers by allowing them to be in control of their information. This rule is not about erasing past events or restricting the freedom of the press. [8]

In 2012, a Spanish citizen brought suit against Google Spain and Google Inc. after he failed to secure the deletion of an auction notice of his repossessed home on Google's search

[6] Frank Pasquale, a law professor at the University of Maryland who is an expert on law and information technology, and the author of the forthcoming book *The Black Box Society: The Secret Algorithms That Control Money and Information* has stated in interviews that the name of the 'right to be forgotten' can be rather misleading to Americans. He states: "I think that the name of the right is misleading. It really might be better understood as the "right not to have one damaging incident or characterization dominate important reports about oneself." *See* Jathan Sandowski, *Lessons From the 'Right to be Forgotten,' available at http://thehill.com/blogs/pundits-blog/technology/207841-lessons-from-the-right-to-be-forgotten.*

[7] *See id.*

[8] *See id.* at 2.

results. [9] The foreclosure proceedings had been fully resolved for a number of years, however they would still appear every time his name was searched on Google. The court held that the search results were irrelevant and should not have been linked to him whenever his name was searched on the search engine. [10] In its May 2014 ruling the European Court held individuals have the right, under certain conditions, to ask search engines to remove links with personal information about them. [11] This 'right to be forgotten' applies when information is inaccurate, inadequate, irrelevant, or excessive.[12] Even if the physical server of a company processing data is located outside of Europe, EU rules apply to search engine operators if they have a branch or subsidiary in a Member State, which promotes the selling of advertising space offered by the search engine.[13] The court reasoned that Google could not escape liability under European law when handling personal data by arguing that it is a search engine. [14] The court held that European Data Protection law applies to search engines and so does the "right to be forgotten." [15]

In theory, the 'right to be forgotten' addresses an urgent problem in the digital age: It is very hard to escape your past on the Internet now that every photo, status update, and tweet lives forever in the cloud. [16] The availability of the Internet to kids and teenagers at a young age has led to teenagers to leave behind statements or digital traces they may later regret. The Vice-President of the European Commission, Viviane Reding has taken the first step in Data

[9] Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González (May 13, 2014), *available at http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&rid=14*.
[10] *See id.*
[11] *See id.*
[12] *See id.*
[13] *See id.*
[14] *See id.*
[15] *See id.*
[16] Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88 (2012).

Protection Reform. [17] In her 2012 speech, she aimed for a comprehensive reform of the European data protection rules. [18] Making Europe the standard setter in this area of the law, Commissioner Reding has implemented the right to be forgotten.[19] She has made it explicit that people hold the right to put out personal information, and have the right to withdraw that information just as easily. [20] The right to be forgotten is not a completely new concept to Europe; the principal underpinnings of the idea were included in the 1995 EU Data Protection Directive: "[a] person can ask for personal data to be deleted once that data is no longer necessary (Article 12 of the Directive)." [21]

Unlike people, the Internet has almost unlimited search, memory, and storage capacity. [22] Consumers should be empowered with the right to protect their identity online, particularly minors, and college students. [23] The United States has been behind in developments in the privacy sector of the law. In 2012, the Obama Administration released a "Privacy Bill of Rights" as a comprehensive blueprint to improve the protections available to consumers online and

[17] Viviane Reding, Vice President, Eur. Comm'n, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age 5 (Jan. 22, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF. Vice President Reding stressed the need for new data protection rules as the current rules date from 1995. Personal data has become one of companies' most valuable assets in the digital market leading to fear and hesitation in consumers to conduct online purchases and accept new services.

[18] *See id.*

[19] *See id.* Reding has aimed to simplify data protection, by implementing a 'one-stop-shop' for businesses for all data protection matters. A company will only have to comply with one universal rule for the entire EU territory. It will only have to deal with one single data protection authority, leading to easier compliance and making data exchanges less burdensome and more secure. *Id.*

[20] *See id.* Reding emphasized that the new rules will provide for data portability and easier access to one's own data. She clarified that people will have the right to withdraw their consent to the processing of their data they have given out themselves. *Id.*

[21] Eur. Comm'n, *Factsheet on the "Right to be Forgotten" ruling (C-131/12)*(Jun. 2, 2014), *http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_en.pdf*. Note that this is not an absolute right. Reding highlighted legitimate and legally justified interests in keeping data under some circumstances such as archives of a newspaper. She continuously stressed throughout her speech that the right to be forgotten would take absolutely no precedence over Freedom of Expression or Freedom of Press. *Id.*

[22] *See id.*

[23] *See id.*

ensure the Internet continues to fuel economic growth. [24] President Obama stressed, "[n]ever has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones. In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information. So, it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times." [25] This proposal does not quite have the strength of the European Data Directive, but is a step towards the recognition of stronger privacy protection. [26] Nonetheless, there is much opposition towards recognition of the 'right to be forgotten' in the United States. Much of this is because of Freedom of Speech concerns. Many Americans are worried that implementation of this right will lead to censorship, and will infringe on other constitutionally protected rights. [27] However, the 'right to be forgotten' does not infringe on constitutionally protected rights, instead, it disallows the retention and dissemination of irrelevant, outdated, excessive, and incorrect information retained on behalf of consumers.

I. THE RIGHT TO BE FORGOTTEN DOES NOT INFRINGE ON CONSTITUTIONALLY PROTECTED RIGHTS SUCH AS FREEDOM OF EXPRESSION AND FREEDOM OF THE PRESS. RATHER, THE RETENTION OF STALE OUTDATED DATA INFRINGES ON OUR CONSTITUTIONAL RIGHTS TO PRIVACY

Personal data is shared knowingly and unknowingly. Many consumers are completely unaware that their every movement is being tracked every time they login to social networking

[24] The Obama Administration recognized American Internet users' right to privacy in its "Consumer Privacy Bill of Rights." Press Release, The White House, *Fact Sheet: Plan to Protect Privacy in the Internet Age by Adopting a Consumer Privacy Bill of Rights* (Feb. 23, 2012), *available at http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protectprivacy-internet-age-adopting-consumer-privacy-b.* The Bill of Rights is based on the premise that "American Internet users should have the right to control personal information about themselves." *Id.*
[25] *See id.* at 5.
[26] *See id.*
[27] *See* U.S.C.A. Const. Amend. 1.

sites such as Facebook, go shopping at Target, or using a loyalty card. [28] By monitoring you, companies are able to learn about your personal finances, religious and political affiliations, ethnic background, health problems, and sexual preferences. Our personal identifying information, our purchases, and websites we visit are scraped and saved for future marketing and business purposes on behalf of these companies. [29] Online shopping is looking better than ever, with estimates of growth of over 4.1% in the 2014 holiday season. [30] Every time you surf the internet, your browser collects bits and pieces of information from sites you visit, either in the form of cache, which stores photos and site data on your hard drive to help speed up page loading, or cookies, which are small files deposited on your computer so websites can remember

[28] Sensitive personal information is also tracked when consumers make purchases on their smartphones using a company's mobile applications ("apps"). The Federal Trade Commission staff studied some of the most popular mobile apps that allow consumers to compare prices across retailers, collect and redeem deals, or pay for purchases while shopping in brick-and-mortar stores. The FTC sought to learn more about how these apps and services operate, primarily by examining information that is available to consumers before they download the software onto their mobile devices. They looked for pre-downloaded information describing how those apps that enable consumers to make purchases, dealt with fraudulent or unauthorized transactions, billing errors, or other payment-related disputes. In addition, because shopping apps can allow multiple parties to gather and consolidate personal and purchase data, the staff looked for information explaining how the apps handled consumer data. Based on its review, the staff found that the apps studied often failed to provide pre-download information on issues that are important to consumers. Prior to download, few of the in-store purchase apps provided any information explaining consumers' liability or describing the app's process for handling payment-related disputes. Additionally, although nearly all of the apps made strong security promises and linked to privacy policies, most privacy policies used vague language that reserved broad rights to collect, use, and share consumer data, making it difficult for readers to understand how the apps actually used consumer data or to compare the apps' data practices. *See What's the Deal? An FTC Study on Mobile Shopping Apps,* FED. TRADE COMM'N, at 8 (Aug. 2014).

[29] *See* Adam Tanner, *What Stays in Vegas: The World of Personal Data—Lifeblood of Big Business—and the End of Privacy as We Know It* 8 (2014). Caesars now provides prepaid cash cards that collect data about where clients shop, eat, and how much they spend. *See id.*

[30] Retailers prepared for a greater surge in online spending for the 2014 holiday season. Currently, the online retail industry's annual sales are $3.2 trillion. *See* Press Release, Kathy Grannis, Treacy Reynolds, *Optimism Shines as National Retail Federation Forecasts Holiday Sales to Increase 4.1%* (Oct. 7, 2014), *https://nrf.com/media/press-releases/optimism-shines-national-retail-federation-forecasts-holiday-sales-increase-41* (last visited Nov. 4, 2014).

certain things about you. [31] Merely knowing a zip code, gender, and a birthdate provides enough information to identify nearly 90 percent of the population. [32]

Adam Tanner, author of *What Stays in Vegas: The World of Personal Data—Lifeblood of Big Business—and the End of Privacy as We Know It,* stresses that no one expected privacy until mass urbanization began over a hundred years ago. [33] In fact, the Constitution never directly addresses consumer privacy and the Internet. [34] In strict contrast to this, the FBI and NSA are not interested in the majority of citizens they monitor.[35] They hold no personal stake, nor do they profit from data. [36] However, these entities are subject to substantial governmental, congressional, and judicial oversight. [37] By contrast, private companies gather, maintain, and indefinitely store detailed individual profiles on millions of people with minimal restrictions. The consumer is not empowered to see what data these companies have about them, nor do they have the power to limit, delete, or rectify any incorrect information.[38] The overwhelmingly diminishing privacy rights Americans face force us to consider the implementation of a 'right to be forgotten.'

Critics have largely criticized Europe's 'right to be forgotten' and have argued that implementation of such a right in the United States infringes on Americans' constitutionally

---

[31] *See* John Herrman, *What are Flash Cookies and How Can You Stop Them?,* (Sept. 23, 2010, 5:20 PM), http://www.popularmechanics.com/technology/how-to/computer-security/what-are-flash-cookies-and-how-can-you-stop-them (extensively explaining the difference between regular cookies and 'flash' cookies which are not deleted when other cookies are. Sites can continue to store and maintain tracking cookies through your Flash plug-in regardless of your browser's privacy settings.).
[32] *See id.* at 14.
[33] Tanner emphasizes that no company knows the value of data collection better than Caesars Entertainment. The secret to the company's success lies in their tracking activities of the overwhelming majority of gamblers. The casinos' data-mining methods are purposely intrusive - they know what games their clients like, who their favorite hostess might be, and exactly how to keep them returning back to the casino. *See supra* note 29.
[34] *See id.*
[35] *See id.*
[36] *See id.*
[37] *See id.*
[38] *See id.*

protected rights, such as freedom of expression, and freedom of the press. [39] Further, critics have incorrectly argued that the European Court decision will create a censored World Wide Web. [40] To the contrary, the European Commission has made it clear that the right of erasure is not absolute and has clear limits which are balanced against other public policy concerns.[41]

At minimum, in order for the 'right to be forgotten' to apply, the information about the individual must be inaccurate, inadequate, irrelevant or excessive. [42] The mere economic interests of companies to compile and use information for marketing purposes, regardless of truth and accuracy, cannot override a person's right to data protection. Europe's right to be forgotten is not absolute, and will always be balanced against other fundamental rights such as freedom of expression and freedom of the media. [43] The court in its judgment did not elevate the right to be forgotten to trump other fundamental rights. The right to be forgotten can be analogized to negative items falling off of a credit report after seven years. [44]

In February 2012, the Obama Administration released a framework for protecting privacy and promoting innovation in the global digital economy. [45] President Obama stressed the importance of privacy protections and the need for growth of these protections in the coming years. President Obama analogized data protection rights to the implementation of the United States Postal Service. After the postal system was set up, laws were passed making it a crime to invade the mails. Proving that the law has always been in constant change due to the circumstances of our time. [46] President Obama stressed that although we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that

[39] *See id.*
[40] *See id.*
[41] *See id.*
[42] *See supra note* 18, at 6.
[43] *See supra note* 18.
[44] *See id.*
[45] *Supra* note 21.
[46] *See id.*

privacy is an outdated value. [47] It has now become more important than ever to continue to apply our timeless privacy values from the time of the Constitution to the new and upcoming technologies and circumstances of our time. [48]

The U.S.' Consumer 'Privacy Bill of Rights' is a step in the direction of Europe's 'right to be forgotten' laws. The rights of Freedom of Speech and Freedom of the Press regarding the collection and use of consumer information must be balanced with the need for transparency to individuals about how data about them is collected, used, disseminated and the opportunity for individuals to access and correct data that has been collected about them. [49] Additionally, just as the EU Commission stressed, the White House believes that consumers have the right to withdraw consent to use personal data just as easily as it is granted. [50] Google dominates online search traffic, controlling about 67% of search traffic in the United States, and almost 90% of it in the European Union. [51] So if it is not on Google, it does not exist. [52]

Allowing one big player like Google to be the effective gatekeeper of all information will distort our collective view of the world and will dampen our right to the free flow of accurate information. [53] Further, allowing companies to control and retain stale outdated information

---

[47] *Supra* note 21, at 3.
[48] *Id.*
[49] *Id.* at 48 para. 5. Other areas of the law are also considering reform in regards to background checks conducted on potential job applicants. Widely known as "Ban the Box" these fair-hiring initiatives remove the question on the job application about an individual's conviction history and delay the background check inquiry until later in the hiring process. Thirteen states have embraced statewide "Ban the Box" fair hiring laws. Some of the states include California, Colorado, Connecticut, Delaware, Illinois, Maryland, and New Jersey. And more than 60 cities and counties – from Indianapolis to Kansas City, Buffalo, and Rochester have adopted similar laws for government employment. Nationwide almost 70 cities and counties – including New York City have taken critical steps in removing unfair barriers in their hiring policies. Similarly, in the Internet sector, Americans should feel secure that irrelevant, excessive, or outdated information will be removed from search engine results. *See* National Employment Law Project, *Ban the Box: Major U.S. Cities and Counties Adopt Fair Hiring Policies to Remove Unfair Barriers to Employment of People with Criminal Records* at 5, (Sep. 2014)
[50] *See id.*
[51] *See id.*
[52] Evan Leatherwood, Why Google's Removal of News Links in the EU Is a Good Thing, (July 9, 2014 6:40 PM), http://www.huffingtonpost.com/evan-leatherwood/why-googles-take-down-of-_b_5572225.html
[53] *Id.*

infringe on our constitutionally protected rights. Even when consumers voluntarily provide personal details to online retailers, social networks, or even their financial institutions, the consumer has little power to control which of those entities will sell the data. Many times the data is sold to affiliates or subsidiaries, regardless of how accurate or outdated that information may be. Consumers suffering from various health diseases may recover from a condition but still receive marketing that has been aimed towards them because of continuous and inaccurate data spreading.[54] Data hoarding has become a trend within many large corporations and enterprises drowning in data, regardless of how relevant that information is. [55] Unfathomable amounts of data are being generated from traditional and modern sources such as social media and cookie tracking methods.[56] A majority of Americans would agree that such useless data, like outdated medical records or other irrelevant, inaccurate private information that is being stored, should be legally and safely disposed of. However, many companies are set on storing as much information, for as long as possible, with little to no regulation. According to the CSC, the volume of data storage is expected to increase exponentially, leading to a 4,300% increase by 2020. [57]

Some 80% of the data is "unstructured" or non-database content, largely email but increasingly documents, images, audio, and video. [58] Further, an estimated 70% of data has

[54] *See id.* Therefore, the European Data Protection Regulation strikes the right balance between the right to the protection of personal data and freedom of protection. *Id.*
[55] *See id.*
[56] *See* Do-Not-Track Online Act of 2011, S. 913, 112th Congress (2011); Do Not Track Me Online Act, H.R. 654, 112th Congress (2011). Hoarding is defined clinically as embodying "a persistent difficulty discarding or parting with possessions because of a perceived need to save them." That accumulation occurs regardless of the actual value associated with the possessions, and often stands in stark contrast to a "normal" person's perception. *See* Judy Selby, James Sherer, *Are you—or someone you love—a content hoarder?*, (Sep. 18, 2014), http://www.dataprivacymonitor.com/information-governance-2/are-you-or-someone-you-love-a-content-hoarder/
[57] More rigorous regulations are necessary to prevent against corporate abuses. *See* CSC, Big Data Beginning to Explode, DIGITAL UNIVERSE STUDY, *http://www.csc.com/big_data/flxwd/83638-big_data_just_beginning_to_explode_interactive_infographic*
[58] *See id.* Companies would not preserve half as many records if they were forced to send those e-mails in paper format. Companies would also be forced to become more efficient if they discarded volumes of useless data. This

absolutely no value, and simply adds to confusion and problems in enterprises, where 42% of managers say they use the wrong information at least once per week. [59]

In light of all the data breaches occurring in 2014, such invasive cyber practices and storage of confidential personal data pose a much larger and dangerous risk to consumers. Therefore, establishing limitations as well as expiration dates for data is a forward-looking idea that will be necessary in the coming years. An increasing numbers of Americans use social media both on and off the job. Recently, some employers have asked employees to turn over their usernames and passwords for their social media accounts. [60] Many states, like New Jersey, have already limited an employer's right to request that an employee or applicant disclose any means for accessing personal social media accounts or services. The same limitations should be placed on companies that indefinitely gather, store, and sell consumer information. [61]

II. SELL IT MAYBE? THE RIGHT TO BE FORGOTTEN EXTENDS TO DATA MINING IN THE PHARMACEUTICAL INDUSTRY.

Hippocrates' ancient oath to keep secrets sacred between physician and patient is having a rough time in the modern age as drug companies, the government, and insurers dip into databases rich with personal medical information.[62] Pharmaceutical data mining is the business of collecting information relating to the prescribing habits of doctors, dentists, and nurse practitioners. [63] This information is then sold to affiliates, or outside companies, that use the

---

would substantially reduce the amount of time that is wasted when searches turn up old and irrelevant information. *Id.*

[59] *Id.*

[60] *Id.*

[61] *See* NAT'L CONF. OF STATE LEGISLATURES, A.B. 2878, *http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2014* (2014). Six states - California, Delaware, Illinois, Maryland, Michigan and New Jersey--enacted legislation in 2012 that prohibits requesting or requiring an employee, student or applicant to disclose a username or password for a personal social media account. *Id.* There is still much pending litigation.

[62] *See* Cal Woodward Data-Mining Case Tests Boundaries of Medical Privacy, available at: *http://www.cmaj.ca/content/183/9/E509.full?ijkey=0347e140a8844f36c5950b20a90530401881d938&keytype2=tf_ipsecsha.*

[63] Michael Heesters, Comment, *An Assault on the Business of Pharmaceutical Data*

information in their business. [64] An example of this practice entails pharmaceutical data mining companies collecting prescribing data from pharmacies. [65] The data mining companies then distill the data to determine the prescribing patterns of individual prescribers. [66] Pharmaceutical companies then buy this information, which allow them to better target their sales force. [67]

IMS Health Holdings Inc. says it pulled in nearly $2 billion in the first nine months of 2013, from sweeping up data from pharmacies and selling it to pharmaceutical and biotech companies. [68] The firm's revenues in 2012 reached $2.4 billion, about 60 percent of which came from selling such private information. [69] Physicians and privacy advocates have argued that prescription records could be used to obtain information about specific patients' conditions without their permission. [70] In addition, physicians have largely argued that they have a right to privacy about their various prescribing habits, why they prefer certain drugs, and the process by which they choose drugs. However, physicians are never consulted before pharmacies sell information about them and their prescribing habits. [71] This is important because many times physicians feel pressured to prescribe certain drugs because marketing companies will cease marketing to the physician if they have not been prescribing their product. Physicians have financial incentives to prescribe certain products. If they are a top prescriber of a particular drug,

---

Mining, 11 U. P.A.J. BUS. L. 789, 796 (2009), *available at http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1337&context=jbl.*

[64] *Id.* Marc Rotenberg, executive director of the Electronic Privacy Information Center, says the cryptographic technique used to protect patient identity is outdated. Therefore, anonymity cannot be assured when the personal information that is retained in prescription records is combined with identifiers in other databases such as a user's online search queries, credit card records, even movie reviews. The industry disputes that. *Id.*

[65] *Id.*

[66] *Id.*

[67] NAT'L CONF. OF STATE LEGISLATURES, 28 STATE HEALTH NOTES: VITAL SIGNS FOR POLICYMAKERS (2007), *available at* http://www.ncsl.org/print/health/shn/shn496.pdf.

[68] Charles Ornstein, Big Data + Big Pharma = Big Money, (Jan. 10, 2014), *http://www.propublica.org/article/big-data-big-pharma-big-money.*

[69] *See id.*

[70] *See id.*

[71] *See id.*

pharmaceutical companies will continue to provide free medication samples, educational and promotional meetings, and even hire the physician for paid promotional talks. [72]

In *Sorrell v. IMS Health Inc.,* a group of Vermont Data Miners and the Association of Pharmaceutical Manufacturers brought an action challenging the constitutionality of Vermont's Prescription Confidentiality Law, which restricted the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors. [73] Vermont's Prescription Confidentiality Law required that records containing doctors prescribing practices not be sold or used for marketing purposes unless the physician consented. Vermont argued that the use of prescriber-identifying information undermines the doctor-patient relationship by allowing detailers to influence treatment decisions. Under Vermont's law, pharmacies may share prescriber-identifying information with anyone for any reason except one: They must not allow the information to be used for marketing.

At issue in *Sorrell v. IMS Health, Inc.* was whether physician prescribers have a right of privacy and whether that right takes precedence over a particular use of information or data speech for commercial purposes. Pharmaceutical companies and data miner companies argued that Vermont's statutory restrictions on selling information for marketing purposes infringed on their opportunities to conduct business with their customers because their business in some part is conducted through data collection. The U.S. District Court ruled for Vermont, but the U.S.

---

[72] *See id.* According to a study by ProPublica, an independent investigative news organization, eight pharmaceutical companies provided more than $220 million in speaker payments to physicians in 2010. The companies often host these events at restaurants and provide meals to physicians who attend. *See Persuading the Prescribers: Pharmaceutical Industry Marketing and its Influence on Physicians and Patients,* Prescription Project, (Nov. 11, 2013).

[73] *See Sorrell v. IMS Health Inc.*, 131 S. Ct. 2653, 180 L. Ed. 2d 544 (2011). Pharmaceutical manufacturers promote their drugs to doctors through a process called "detailing." Pharmacies receive prescriber-identifying information when processing prescriptions and go on to sell that behavior to data miners. In return, data miners produce reports detailing this behavior and go on to lease these reports to pharmaceutical manufacturers. Thereafter, "detailers" who are employed by pharmaceutical manufacturers then use the reports to refine and tailor their marketing tactics towards doctors. *See id.*

Court of Appeals for the Second Circuit overturned the ruling in a 2-1 decision. [74] After the reversal, the State of Vermont sought certiorari by the United States Supreme Court. [75]

The Supreme Court, in an opinion by Justice Kennedy, held that the statute was designed to impose a specific, content and speaker based burden on protected expression warranting a higher standard of judicial scrutiny in determining whether it violated First Amendment free speech protections. [76] The Court struck down the Vermont law that required data mining companies to obtain permission from individual physicians before selling prescription records.[77] The decision was based primarily on constitutional free speech concerns rather than data sharing considerations.

The court failed to take into consideration the privacy concerns of physicians and patients. Under existing laws in the United States, in almost every state pharmacies can sell prescription information to data mining companies as long as the patient information has been "de-identified." [78] As long as the de-identification complies with the standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[79] the data mining companies are then free to aggregate these reports and sell them to prescription drug marketers, pharmaceutical companies, and others. [80]

---

[74] The U.S. Court of Appeals for the First Circuit had previously upheld similar statutes in Maine and New Hampshire. More than 20 states have taken steps to limit the use of prescription information. *See* Cal Woodward, Data-Mining case tests boundaries of medical privacy, (June 14, 2011), *http://www.cmaj.ca/content/183/9/E509.full?ijkey=0347e140a8844f36c5950b20a90530401881d938&keytype2=tf_ipsecsha*

[75] *See id.*

[76] *See id.*

[77] *See id.*

[78] *See id.* De-indentification involves the removal of names and other unique identifiers; however the extent to what information is left is unclear. The prescriptions do however still contain the prescriber's name, the drug they prescribed, their doses, and the frequency that they are prescribed. *See id.*

[79] *See id.*

[80] *See id.*

Sorrell brought to light the enormous industry of data collection. Consumers must be empowered with more rights regarding their private information. The 'right to be forgotten' will not arm citizens with the ability to edit history. Instead it will allow Americans to control information about themselves. It will allow consumers the right to have information that is inaccurate or outdated removed. Privacy is essential to our democratic society and must continue to remain essential.

III. THE 'RIGHT TO BE FORGOTTEN' SHOULD SIMILARLY APPLY LIKE THE FAIR CREDIT REPORTING ACT'S CREDIT STATUTES – ADVERSE, IRRELEVANT, AND OUTDATED INFORMATION SHOULD NOT BE SUBJECT TO RELEASE.

A. Consumer Reporting and the Fair Credit Reporting Act

The role consumer reporting agencies play in Americans lives are endless. Purchasing a home, car, renting an apartment, and many offers for employment all have one thing in common - they require your credit report. Consumer reporting agencies have played an essential role in our economy by providing "those who extend credit or insurance or who offer employment … the facts they need to make sound decisions." [81] A credit reporting agency's main function is to assemble and disseminate volumes upon volumes of information about individuals, thus holding the power to unduly invade individuals' privacy and the ability to cause irreparable harm by negligently or mistakenly disclosing inaccurate or outdated information. [82] Congress enacted the Fair Credit Reporting Act in 1970 [83] to limit abuse on behalf of the credit reporting industry, which had assumed a vital role in "assembling and evaluating consumer credit and other information on consumers." [84] Congress reasoned that the banking system is dependent upon fair and accurate credit reporting. Inaccurate credit reports directly impair the efficiency of the

[81] *See* S. Rep. No. 91-517 at 2 (1969). Since 1970, the FCRA was updated in 2003, broadening its reach to also protect against identity theft by allowing companies to provide fraud alerts, and adding amendments to definitions.
[82] *See id.*
[83] Pub. L. 91-508, § 601, 84 Stat. 1128, 1128 (1970)(*codified at* 15 U.S.C. § 1681(a)(3)).
[84] *See id*.

banking system and in turn undermine public confidence, which is essential to the continued functioning of the banking system. [85]

Under some circumstances Congress has the power to prohibit the reporting of true commercial speech.[86] A provision of the Fair Credit Reporting Act, 15 U.S.C. § 1681c, limits the length of time that credit bureaus may report accurate information. [87] Subsections (a)(2)[88] and (a)(5)[89] of the statute generally prohibit consumer reporting agencies from disclosing public information regarding an individual's non-conviction history such as civil suits, civil judgments, and records of arrest that are more than seven years old. [90]

The stated purpose of the Fair Credit Reporting Act is "to require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce ... in a manner which is fair and equitable to the consumer." [91] In other words, Congress' interest is two-fold: allow businesses to engage in commerce and meet the needs of business while at the same time protecting consumer privacy. [92] Congress achieves such a balance between these competing yet equally important interests through a variety of provisions in the Fair Credit Reporting Act. [93] These provisions simultaneously make consumer report information available to businesses, but limit the type of information being reported and the circumstances in which it may be reported. [94] In striking the most appropriate balance between business needs and consumer privacy, Congress

[85] 15 U.S.C.A. § 1681 (a)(1).
[86] *See id.*
[87] 15 U.S.C. § 1681c. *See also* Pamela Nevata, Paul Kehoe, Is FCRA's Prohibition on CRAs from Disclosing Truthful Public Information Constitutional? The Government to Defend Its Position, (Feb. 4, 2014), *http://www.laborandemploymentlawcounsel.com/2014/02/is-fcras-prohibition-on-cras-from-disclosing-truthful-public-information-constitutional-the-government-to-defend-its-position/.*
[88] 15 U.S.C.A. § 1681c(a)(2).
[89] 15 U.S.C.A. § 1681c(a)(5).
[90] *Id.* at (a)(2).
[91] 15 U.S.C. § 1681(a)(4).
[92] *Id.*
[93] *Id.*
[94] *Id.*

must weigh the significance of "confidentiality, relevancy, and proper utilization of such information." [95]

B. King v. General Information Services Inc.

In November 12, 2012 the Eastern District of Pennsylvania ruled that 15 U.S.C. § 1681c, a provision of the Fair Credit Reporting Act ("FCRA") is constitutional. [96] *King v. General Information Services, Inc.* stems from a class action complaint filed on behalf of a plaintiff and others similarly situated, alleging that General Information Services provided conviction information over seven years old in a report sold to potential employers. [97] General Information Services, Inc. ("GIS") is a consumer-reporting agency, as defined by section 1681a(f) of the FCRA. [98] The company investigates and reviews public record databases and maintains consumer files, which contain public record information concerning, among other things, the criminal history of individuals. [99] From its files, GIS sells consumer reports to potential employers wishing to investigate the criminal record history, or lack thereof, of various job applicants. [100]

Around early 2010, Shamara King applied for a job with the United States Postal Service. [101] In connection with Ms. King's application, the Postal Service ordered a background check from GIS services. [102] The background report on Ms. King included ten nolle prossed charges

[95] 15 U.S.C. § 1681(b).
[96] Section 1681a (c) of the FCRA defines the seven year period, "shall begin, with respect to any delinquent account that is placed for collection (internally or by referral to a third party, whichever is earlier), charged to profit and loss, or subjected to any similar action, upon the expiration of the 180-day period beginning on the date of the commencement of the delinquency which immediately preceded the collection activity, charge to profit and loss, or similar action." 15 U.S.C. 1681a(c).
[97] 903 F. Supp. 2d 305 (E.D. Pa. 2012).
[98] *See id.*
[99] *See id.*
[100] *See id.*
[101] *See id.*
[102] *See id.*

she received in July 2000 after an arrest for a criminal incident.[103] Ms. King's consumer report also disclosed an inaccurate charge date and arrest date for the offense. [104] On or about March 4, 2010, GIS mailed Ms. King a copy of the consumer report that was earlier sent to the Postal Service. [105] Shortly afterwards, Ms. King, on behalf of herself and others similarly situated, brought suit against GIS for its alleged failure to comply with § 1681(c) of the FCRA by maintaining a practice of willfully reporting outdated adverse public information, including records of arrest, that is required to be excluded from the consumer reports that it sells. [106] Ms. King specifically alleged that GIS violated § 1681(c) when disclosing her 10-year-old nolle prossed charges to the Postal Service. GIS challenged the constitutionality of the FCRA's § 1681(c) on the ground that the it violated the First Amendment under the Supreme Court's recent decision in *Sorrell v. IMS Health Inc.* [107] The main provision at issue: 1681(c) – a provision that, with narrow exceptions, prevents consumer reporting agencies from disclosing arrest records and other adverse information that are more than seven years old. [108]

The court in *King* held that information disseminated by consumer reporting agencies in a consumer report concerned purely private matters, therefore warranting reduced First Amendment protection, subject to intermediate scrutiny, under the commercial speech doctrine. [109] The Supreme Court has made clear that consumer report information is "speech" under the

[103] *See id.*
[104] *See Id.*
[105] *See id.*
[106] *See id.*
[107] Determining, under a First Amendment commercial speech inquiry, whether a law directly advances an interest in a way that is no more extensive than necessary essentially involves a consideration of the fit between the legislature's "ends and the means" chosen to accomplish those ends; that fit between a legislature's goal and the means chosen to accomplish that goal does not necessarily have to be perfect, but just reasonable, and the law's scope must be in proportion to the interest served. U.S.C.A. Const. Amend. 1.
[108] *See id.*
[109] *See id.*

First Amendment. [110] However, the degree of First Amendment protection accorded to consumer report information turns on whether the particular information is of public or private concern. [111] In *Dun & Bradstreet*, the Supreme Court reasoned that such a determination "depends on whether the report's content, form, and context indicate that it concerns a public matter." [112] Where the information is "solely in the interest of the speaker and its specific business audience" and made available only to a limited number of subscribers and the credit report information concerns no public issue, that form of speech warrants a reduced First Amendment protection. [113] Therefore, like here, private agencies that compile consumer reporting information for the purpose of making a profit are entitled to reduced First Amendment Protection because its business customers purchased reports to make business decisions, and reports were only made available to paying subscribers.[114] GIS attempted to invalidate this longstanding FCRA protection by arguing that *Sorrell* changed the First Amendment standards relating to commercial speech. [115] However, the Supreme Court established the *Central Hudson* test over thirty years ago and it still applies to statutes such as 1681(c) that restricts commercial speech. The FCRA's 1681(c) would similarly pass this test and nothing in *Sorrell* suggests otherwise. [116]

III. SIMILARLY, THE 'RIGHT TO BE FORGOTTEN' IS ANALOGOUS TO THE SAFEGUARDS CONGRESS HAS PUT IN PLACE BY IMPLEMENTING THE FAIR CREDIT REPORTING ACT, GRAMM LEACH BLILEY ACT, AND OTHER CONSUMER SAFEGUARDS.

[110] *See Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.,* 472 U.S. 749, 105 S.Ct. 2939, 86 L.Ed.2d 593 (1985); *Trans Union Corp. v. F.T.C.*, 245 F.3d 809 (D.C.Cir.2001), *cert. denied,* 536 U.S. 915, 122 S.Ct. 2386, 153 L.Ed.2d 199 (2002).
[111] 472 U.S. at 762 n. 8, 105 S.Ct. 2946.
[112] *See id.* at 2942.
[113] *See id.* at 2959.
[114] *See supra* note 81. U.S.C.A. Const. Amend. 1.
[115] *See supra* note 81.
[116] *See supra* note 81.

Courts have confirmed that restrictions on the sale of data should be analyzed under the *Central Hudson* commercial speech test. [117] In a commercial speech case, under the Central Hudson Commercial Speech test, the court must first determine whether the expression is protected by the First Amendment and must next ask whether the asserted governmental interest is substantial. [118] If both answers are yes, the court must determine whether the regulation directly advances a governmental interest and whether the regulation is more extensive than is necessary to serve that interest. The Ninth Circuit has held that selling information about recent arrestees to attorneys and others seeking new clients qualified as commercial speech protected under *Central Hudson*. [119]

Personal harms do emerge from inappropriate data storage and predictive analysis of an individual's personal data without their knowledge or express consent. For example, in 2012, a well-publicized *New York Times* article revealed that the popular American retailer Target had used data mining techniques to predict which female customers were pregnant, even if they had not yet announced it publicly. [120] This activity resulted in the unauthorized disclosure of personal information to marketers, who in turn "guessed" or knew that the customer was

[117] U.S.C.A. Const. Amends. 1, 14. *See Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York*, 447 U.S. 557, 100 S. Ct. 2343, 65 L. Ed. 2d 341 (1980).
[118] *Id.*
[119] *See King v. General Information Services, Inc*., 2:10-cv-06850-PBT. *See also United Reporting Publ'g Corp v. Cal. Highway Patrol,* 146 F.3d 1133, 1135-37 (9th Circ. 1998), *rev'd on other grounds sub nom. L.A. Police Dep't v. United Reporting Publ'g Corp,* 528 U.S. 32 (1999).

[120] Andrew Pole had just started working as a statistician for Target in 2002, when two colleagues from the marketing department stopped by his desk to ask an odd question: "If we wanted to figure out if a customer is pregnant, even if she didn't want us to know, can you do that?" *See* Charles Duhigg, *How Companies Learn Your Secrets,* N.Y. TIMES, Feb. 16, 2012, *available at http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewanted=all&_r=0* (last visited Oct. 10, 2014). *See also* Charles Duhigg, *Psst. You in Aisle 5,* N.Y. TIMES, Feb. 19, 2012, § 6 (Magazine), at 30.

pregnant and released her information to their marketing department who then shortly afterwards sent pregnancy related marketing ads to her home. [121] [122]

Further, the "right to be forgotten" will not lead to the 'slippery slope' issue critics are largely worried about. The fear critics have is a censored world wide web, much like that of China. Google announced that over 58% of 'right to be forgotten' requests were rejected. [123] Google stated that it had received 144,954 requests involving 497,695 URLs. [124] Of that total, it has removed only 42%, keeping 58% in its results.[125] In evaluating its requests, Google stated that they look at whether their search results include outdated or inaccurate information about the person. [126] Their determination is based on whether or not there is a public interest in maintaining that information in Google search results.[127] For example, if the information relates to financial scams, professional malpractice, criminal convictions, or public conduct as a public official, this information will not be removed. [128] One example of a request Google has approved was received from a rape victim in Germany. [129] The victim asked Google to remove a link to a newspaper article about the crime when inputting her name into the search engine. [130] In contrast, a request by a Switzerland professional who asked Google to remove more than ten

[121] *See id.* At the time of this article, Charles Duhigg's wife was seven months pregnant. As a shopper at Target he had given the company his address so he could start receiving offers and coupons in the mail. As his wife's pregnancy progressed, he noticed a subtle increase in the number of advertisements for diapers and baby clothes arriving at his house. One day he stopped at a Target to pick up some deodorant, and then also bought some T-shirts and some fancy hair gel. On a whim, he threw in some pacifiers, to see how Target's data collecting computers would react. When he paid, he didn't receive any sudden deals on diapers or baby formula. It made sense, though: he was shopping in a city he never previously visited, at 9:45 p.m. on a weeknight, buying a random assortment of items and was using a corporate credit card. It was clear to Target's data collecting computers that he was in fact on a business trip. *See id* at 12.

[123] James O'Toole, *Google Rejects 58% of 'right to be forgotten' requests*, http://money.cnn.com/2014/10/10/technology/google-forgotten/index.html?iid=HP_River.
[124] *See id.*
[125] *See id.*
[126] *See id.*
[127] *See id.*
[128] *See id.*
[129] *See id.*
[130] *See id.*

links regarding his arrest and convictions for financial crimes he had committed over the years was denied. [131] Thus, Europe's 'right to be forgotten' is not a mechanism to rewrite history; rather it is a mechanism to allow the public to remove outdated information. [132]

A. The Gramm- Leach Bliley Act

In a speech made on the day the Gramm-Leach-Bliley Act (GLBA) [133] was signed, Senator Phil Gramm stated, "the world changes, and we have to change with it." [134] The reality of online banking is that it is growing quickly and exponentially, without an end in sight.

Congress enacted the GLBA, [135] and declared it to be the policy of Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic, personal information.[136] To further this goal, Congress enacted broad privacy protective provisions. [137]

Enactment of the GLBA, also known as the Financial Services Modernization Act of 1999, [138] was a profound event in the world of Financial Services. For the financial industry, the GLBA marked the end of defects that caused the Great Depression and an opportunity to restructure the U.S. Financial Services Industry. [139] For consumers, the GLBA marked

---

[131] *See id.*
[132] *See id.*
[133] Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338-1481 (1999) (codified in scattered sections of 12 U.S.C. & 15 U.S.C.). For an overview of the main provisions of GLBA, see Scott A. Cammarn & Paul J. Polking, *Overview of the Gramm-Leach-Bliley Act*, 4 N.C. Banking Inst. 1 (2000).
[134] Over a decade later the GLBA is still going strong. Senator Grimm was positive about the GLBA's future stating: "although this bill will be changed many times, and changed dramatically as we expand freedom and opportunity, I do not believe it will be repealed. It sets the foundation for the future, and that will be the test." He analogized with a quote Abraham Lincolns once said: "it would be unreasonable to expect a man to wear the same clothes he wore as a boy." *See* Press Release, Senate Banking Committee, Gramm Closing Floor Statement on Gramm-Leach-Bliley Act of 1999 (Nov. 4, 1999), *available at http://banking.senate.gov/prel99/1104sta.htm* (last visited Nov. 4, 2014).
[135] 9 C.J.S. Banks and Banking § 270. *See also* 15 U.S.C.A. § 6801. Under Federal Law, each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic, personal, information. *See id.*
[136] *Id.*
[137] *See id.*
[138] *See id.* The GLBA repeals sections 20 and 32 of the Glass-Steagall Act. Pub. L. No. 106-102, § 101, 113 Stat. 1338, 1341 (1999).
[139] *See id.*

Congress' attempt to ensure that financial institutions safeguarded their customers' sensitive financial information. [140]

Compliance with the GLBA is mandatory on behalf of all financial institutions. [141] Title V applies to any entity that is a "financial institution" within the definition of GLBA. [142] This definition, in turn, includes "any institution the business of which is engaging in financial activities" within the meaning of subsection 4(k) of the Bank Holding Company Act of 1956, [52] as amended by Title I of GLBA. The term "nonpublic personal information" [143] means personally identifiable financial information provided by a consumer to a financial institution;[144] resulting from any transaction with the consumer or any service performed for the consumer; [145] otherwise obtained by the financial institution. [146] The GLBA defines a consumer as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an individual." [147]

The regulations clarify primarily through examples the distinction between "consumers" and "customers." [148] A "consumer" is an individual who obtains financial products or services from a financial institution that is to be used mainly for personal, family or household

---

[140] *See id.*
[141] *See id.* The term "financial institution" is defined as: (a) to be financial in nature or incidental to such financial activity or; (b) is complementary to a financial activity and does not pose a substantial risk to the safety or soundness of depository institutions or the financial system generally. 12 U.S.C.A. § 1843(k) (West). *See also* Charles M. Horn*, Financial Services Privacy at the Start of the 21st Century: A Conceptual Perspective*, 5 N.C. BANKING INST. 89, 104 (2001).
[142] *See id.*
[143] 15 U.S.C. § 6809(4)(a)(i), (ii), (iii).
[144] 15 U.S.C. § 6809(4)(a)(i).
[145] 15 U.S.C. § 6809(4)(a)(ii).
[146] 15 U.S.C. § 6809(4)(a)(iii).
[147] 15 U.S.C. § 6809(9).
[148]. *See FDIC Compliance Manual,* Title VIII, (January 2014) *available at https://www.fdic.gov/regulations/compliance/manual/pdf/VIII-1.1.pdf.*

purposes,[149] whereas a "customer" of a financial institution is a consumer that has established a "continuing relationship" with a financial institution.[150] The distinction between consumers and customers is significant because financial institutions have additional disclosure duties with respect to customers. All customers covered under the regulation are consumers, but not all consumers are customers. [151] Therefore, a consumer who engages in an isolated ATM transaction or having a check cashed at a check-cash establishment is a "consumer" who has the right to know whether their information will be shared with a third party. That "consumer" must be given the right to "opt-out" of having that information shared, whereas a "customer" is entitled to more protection. In contrast, a "customer" is a consumer who has a "customer relationship" with a financial institution. [152] A "customer relationship" is a continuing relationship between a consumer and a financial institution under which the institution provides one or more financial products or services to the consumer that are to be used primarily for personal, family, or household purposes. [153] For example, a customer relationship may be established when a consumer engages in one of the following activities with a financial institution: maintains a deposit or investment account; obtains a loan; opens a credit card with a financial institution; enters into a lease of personal property; or obtains financial, investment, or economic advisory services for a fee. [154]

Under the GLBA, financial institutions must provide their customers a privacy notice that explains what information the company stores, gathers, disseminates about the customer, where

[149] *See id.*
[150] *See id.*
[151] *See id.*
[152] The distinction between consumers and customers is significant because financial institutions have additional disclosure duties with respect to customers. All customers covered under the regulation are consumers, but not all consumers are customers. *See also FDIC Compliance Manual,* Title VIII, (January 2014) *available at https://www.fdic.gov/regulations/compliance/manual/pdf/VIII-1.1.pdf.*
[153] *See* Privacy of Consumer Financial Information, 65 FR 35162-01 §3 (h)(i). *See also* Horn, *supra* note 133.
[154] *See id.*

and with who the information is shared, and how or what safeguards are implemented to protect that sensitive information. [155] The privacy notice must be given to the customer prior to entering into an agreement to do business. [156] The privacy notice also must explain to customers their right to "opt-out." [157] Opting out means clients can refuse to allow their information to be shared with "non-affiliated partners." [158] The Fair Credit Reporting Act ("FCRA") is responsible for this opt-out opportunity, but the GLBA must also inform the customer of this protected right under the GLBA. [159]

Even after these safeguards, the GLBA does not create a strong privacy right of protection because there is a tradeoff between efficiency and privacy. Under the GLBA, financial institutions can more easily correlate consumer information and foster more efficient business decisions. Congress could have provided stronger privacy protection under the GLBA. For example, like Europe, the GLBA could have provided that customers must "opt-in" instead of "opt-out." [160] Additionally, the GLBA could have included time limitations that financial institutions could have complied with in regards to storage of sensitive customer information. However, even with its shortcomings, the GLBA is still a crucial part of protecting sensitive consumer information in the banking industry. Just as the GLBA is limited in the collection, storage, and dissemination of private, sensitive consumer financial information, the same should

---

[155] *See id.*
[156] *See id.*
[157] *See id.*
[158] *See id.*
[159] *See id.* The Committee bill expands the ability of consumer reporting agencies to use consumer report information for prescreening and direct marketing. At the same time, however, the bill mandates that consumer-reporting agencies create and maintain a system to allow consumers to "opt out" of the prescreening and direct marketing processes. By opting out, consumers can prohibit consumer-reporting agencies from releasing their names or other information from their reports for prescreening and direct marketing. The consumer's choice to opt out will be effective for 2 years following the consumer's notification of the consumer reporting agency, or permanently, if the consumer specifies so in writing. S. REP. 103-209, 13.
[160] *See* Steve Jarvis, *Opt-In Can't be Stressed Enough Online*, MARKETING NEWS, May 21, 2001, at 6 (discussing the effects of opt-in privacy policies and procedures employed on behalf of research firms); Donna Gillin, *Opt in or Opt Out?* MARKETING RESEARCH, July 1, 2001, at 6.

be applicable to consumer online information. In the same light, retailers, and corporations maintain excessive amounts of outdated consumer information, but do so with very little to no regulation. Further, just as the damaging information retained under the FCRA is subject to stringent limitations and regulation, the same must be done in the data industry. Many of these data companies rely on self-regulation, which is conducted in ways most profitable to the company. After all, data is gold and retention and reselling that data ensures profitable gains to companies.

CONCLUSION

All in all, much has to be done in the United States to safeguard consumer information. In an era of rapid and continuing technological change, consumer information has become easier to collect, maintain, and use for profitable gain. The United States is in desperate need of implementing more stringent methods of collection regarding sensitive consumer information, and time limits in retention of that information. Europe's continuing advancement in the protection of consumer information by implementing the 'right to be forgotten' and disallowing companies from using pre-checked [161] boxes for the collection of personal data, is a step in the right direction. The United States is also slowly but surely heading in the same direction.

Implementing a 'right to be forgotten' in the United States is necessary now that Americans' lives are increasingly moving online. From shopping, to banking, and filling prescriptions at the pharmacy, less is done manually, and more is done electronically. Just as times change, laws

[161] Businesses will not be able to use pre-ticked boxes to gain user consent for the processing of their data under changes proposed by the European Parliament to new EU data protection laws. *See* Eur. Parliament, General Data Protection Regulation (Dec. 12, 2012), *available at http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf.*

must change to continue to safeguard consumers in the marketplace. [162] For businesses, consumer privacy must be a priority, just as keeping track of costs, revenues, and strategic planning are. [163] Allowing companies to indefinitely store no longer accurate, excessive, or irrelevant consumer information and not granting the consumer the right to monitor or rectify that information must come to an end in the United States. Further, more has to be done in the United States to disallow data from following a consumer indefinitely. Just as the FCRA prevents credit reporting agencies from indefinitely storing any negative information on a credit report, the same must be done in the data industry.

The Obama Administration has recognized American Internet users' right to privacy when it unveiled a "Consumer Privacy Bill of Rights" in 2012. [164] The Bill of Rights is based on the premise that "[A]merican [i]nternet users should have the right to control personal information about themselves." [165] President Obama reiterated "consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate." [166] Thus, stressing that consumers do in fact have the right to access and correct inaccurate personal data. The 'right to

---

[162] *See* FTC, *Protecting Consumer Privacy in an Era of Rapid Change, A Proposed Framework for Businesses and Policymakers, Preliminary FTC Staff Report* (Dec. 2010), *available at http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.*

[163] *See id* at 5.

[164] "Americans have always cherished our privacy. From the birth of our republic, we assured ourselves protection against unlawful intrusion into our homes and our personal papers. At the same time, we set up a postal system to enable citizens all over the new nation to engage in commerce and political discourse. Soon after, Congress made it a crime to invade the privacy of the mails. And later we extended privacy protections to new modes of communications such as the telephone, the computer, and eventually email." The White House, *supra* note 25.

[165] *See* White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 2012), *available at* http:// www.whitehouse.gov/sites/default/files/privacy-final.pdf. The FIPPs as articulated in the Administration paper are: Transparency, Individual Control, Respect for Context, Security, Access and Accuracy, Focused Collection, and Accountability.

[166] *Id.* The Consumer Privacy Bill of Rights is not law. Rather, it's a document that sets forth rights in the Obama Administrations view that provide a baseline of clear protections for consumers and creates certainty for companies. *See id* at 1.

be forgotten' should be enacted through the Consumer Privacy Bill of Rights through Federal legislation. [167] This would increase legal certainty for companies, strengthen consumer trust, and bolster the United States' ability to lead consumer data privacy engagements with our international counterparts. [168] Even if Congress does not pass legislation, the Consumer Privacy Bill of Rights will serve as a template for privacy protections that increase consumer trust on the Internet and continue to promote innovation.[169]

[167] Currently, the Consumer Privacy Bill of Rights reads, "Companies should use reasonable measures to ensure they maintain accurate personal data. Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to collect inaccurate data or request its deletion or use limitation. Companies that handle personal data should construe this principle in a manner consistent with freedom of expression and freedom of the press." *See id.* at 19.
[168] *See id.* at 2.
[169] *See id.*