WAKE FOREST JOURNAL OF BUSINESS AND INTELLECTUAL PROPERTY LAW

VOLUME 15 WINTER 2015 NUMBER 2

SHY GODIVA: DIGITAL LIKENESS AND THE PERSONAL DATA PROTECTION AND BREACH ACCOUNTABILITY ACT

Austin Griffin[†]

[†] J.D. candidate, May 2015, Wake Forest University School of Law. Staff Member 2014-15, *Wake Forest Journal of Business and Intellectual Property Law*. The author would like to thank the Journal staff and editors for their help on this article, Professor Simone Rose for her guidance on the topic, and his friends and family for their constant love and encouragement throughout his law school career.

I. INTRODUCTION

In early September 2014 Apple joined the ranks of the compromised data giants as the nude photos of some one hundred celebrities were stolen from its iCloud.[1] The result of this breach was the posting of hundreds of nude photographs on websites[2] around the Internet, violating their creators' and subjects' privacy interests. However, these "Shy Godivas"[3] were not alone in their sudden exposure. This breach was one of several[4] in recent history,[5] all of which had a similar focus: the theft of personal information and digital property of the average Internet user.[6] In the past few years these pieces of personal information and digital property have arguably become a new form of intellectual property—the "digital likeness."[7] Due to its novelty, this form is without the meaningful protections given to other types of intellectual property.

---

[1] Alyson Shontell, *APPLE STATEMENT ON CELEBRITY HACKING: Our Systems Weren't Breached*, BUSINESS INSIDER (Sept. 2, 2014, 2:36 PM), http://www.businessinsider.com/apple-statement-on-celebrity-hacking-2014-9.

[2] Madeline Grant, *Hundreds of Intimate Celebrity Pictures Leaked Online Following Alleged iCloud Breach*, NEWSWEEK (Sept. 1, 2014, 1:27 PM), http://www.newsweek.com/hundreds-intimate-celebrity-pictures-leaked-online-following-suspected-icloud-267851 (stating that the photos were uploaded to the websites 4chan and Twitter).

[3] The term "Shy Godiva" is meant to recall the old English folktale of Lady Godiva, riding her horse naked through the streets of Coventry. In cases like the Apple iCloud breach, the nude photos of several celebrities "ran through the public square" of the Internet in a similar fashion. *See An Anglo-Saxon Tale: Lady Godiva*, BBC, http://www.bbc.co.uk/history/ancient/anglo_saxons/godiva_01.shtml (last visited Jan. 25, 2015).

[4] *See, e.g., Data breach at Home Depot leads to fraud*, FORTUNE.COM (Sept. 23, 2014, 7:35 PM), http://fortune.com/2014/09/23/data-breach-at-home-depot-leads-to-fraud/.

[5] *See, e.g., data breach FAQ*, TARGET.COM, https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ (last visited Jan. 25, 2015).

[6] *See* Noah Rayman, *Breaches of Your Personal Data Are Up 20%,* TIME (July 3, 2014), http://time.com/2953428/data-breaches-identity-theft/ (stating that more than 10 million personal records had been stolen in 381 breaches by July 2014).

[7] The term "digital likeness" has been coined for the purposes of this comment. The basis of the term is the common law concept of likeness comprising anything that represents or resembles in some way a particular person, and has been applied here to include digital data, images, and video. *See generally right of publicity*, BLACK'S LAW DICTIONARY 1521 (10th ed. 2014) (defining right of publicity as "the right to control the use of one's own . . . likeness and to prevent another from using it for commercial benefit without one's consent."); Merriam-Webster, *likeness*, M-W.COM, http://www.merriam-webster.com/dictionary/likeness (last visited Jan. 25, 2015).

The appropriation and use of this digital likeness for commercial benefit, which occurred in these recent breaches, tracks the common law right of publicity,[8] but the scale of these thefts, the scope of geography, and the masses of people involved likely bar recovery on a personal level. Even in suit, the number of plaintiffs likely to bring claims in these data breaches would create large class actions with multiple conflicts of law and uncertain remedies.[9] Without uniform federal laws, a set number of defendants, or a grasp of the information's economic nature, these actions could continue *ad infinitem*, or be dismissed just as easily.

Apart from a suit under state law, there is very little legal protection[10] for the average Internet user when these thefts occur. Even the chances of preventing the further spread of stolen information from the original hacking party are incredibly slim.[11] Although the Federal Trade Commission has acted, its actions have stemmed from the misrepresentations of the breached companies' security, rather than from the failed digital defenses that allowed the breach.[12] A recently proposed law, the Personal Data Protection and Breach Accountability Act ("PDPBAA"), now in committee, could help protect the average user's digital likeness from these breaches and provide a federal cause of action against the companies that allow them to occur.[13] However, this law requires some textual changes to

[8] *See* 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 1:3 (2d ed. 2000) ("The right of publicity is a state-law created intellectual property right whose infringement is a commercial tort of unfair competition.").

[9] *See* Linda Silberman, *The Role of Choice of Law in National Class Actions*, 156 U. PA. L. REV. 2001, 2011 (2008) (noting the difficulties of applying the laws of multiple states to class action lawsuits).

[10] *See* FEDERAL TRADE COMMISSION, PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION ON DATA BREACH ON THE RISE PROTECTING PERSONAL INFORMATION FROM HARM BEFORE THE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, UNITED STATES SENATE, 2–3 (2014), *available at* http://www.ftc.gov/system/files/documents/public_statements/296011/140402datasecurity.pdf (providing that the FTC's actions against data security breaches have been limited to the federal laws in place, unfair and deceptive trade prosecution, policy initiatives, consumer education, and "supporting" new federal security laws).

[11] *See* Robert Hackett, *Online, a bazaar bursting with stolen credit card information*, FORTUNE.COM (Sept. 21, 2014, 11:37 AM), http://fortune.com/2014/09/21/home-depot-stolen-card-information-market/ (describing a system of personal data hackers and online markets that quickly sell stolen information around the world after an attack).

[12] *See* FEDERAL TRADE COMMISSION, *supra* note 10, at 3 ("[T]he [FTC] has settled more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice.").

[13] Personal Data Protection and Breach Accountability Act of 2014, S. 1995, 113th Cong. (2014).

clearly protect what was stolen in an iCloud breach—private photos and videos.

This comment will give an overview of the common law right of publicity historically, demonstrate how it has been applied to Internet property in the concept of a digital likeness, suggest a solution to the problems faced by this right of publicity in the PDPBAA, and provide a backing in Constitutional law to this new solution, assuming the statute is faced with opposition upon its passing. Beginning with the Background in Part II, Section II-A will discuss the history of the common law right to publicity and how it relates to the advent of the Internet. Section II-B will give the current state of the right of publicity and the growth of the new digital likeness as well as problems with its protection. In Part III, Analysis, Section III-A will provide an overview of the PDPBAA while Section III-B will posit a textual change to better encompass the emerging digital likeness. Finally, Section III-C will demonstrate the constitutionality of this new law, based on previous Supreme Court cases and the Constitution itself.

II. BACKGROUND

A. The Right of Publicity at Common Law

The common law right to publicity originated as a practical expansion of the right of privacy.[14] The mention of a right to privacy in scholarship began in 1890 with an article[15] by Samuel D. Warren and Louis Brandeis that proposed a "right to be let alone" stemming from "[r]ecent inventions and [new] business methods."[16] These business methods were, at the time, the advent of "instantaneous photographs and newspaper enterprise."[17] Though originally found baseless in contemporary jurisprudence,[18] the continued expansion of technology and communication eventually led courts to accept the

[14] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[15] *Id.* at 193.

[16] *Id.* at 195.

[17] *Id.*

[18] Roberson v. Rochester Folding Box Co., 64 N.E. 442, 447 (N.Y. 1902) (holding that "the so-called 'right of privacy' has not as yet found an abiding place in [the court's] jurisprudence").

right to publicity.[19] Even the Supreme Court now considers this right to privacy as an assumptive right under the Constitution.[20]

In the wake of the right to privacy's expansion, the right to publicity was coined by the United States Court of Appeals for the Second Circuit in *Haelan Labs, Inc. v. Topps Chewing Gum, Inc.* to protect a baseball player's likeness from being used in an advertisement without his acquiescence or benefit.[21] In assuming this newly minted right, the court made clear that this was "in addition to and independent of that right of privacy" and that a person "has a right in the publicity value of [his or her] photograph."[22] Over time, the right was to be clarified to protect an accepted facet of the right of privacy—"appropriation of plaintiff's name or likeness for defendant's benefit."[23] This matured right and its attendant likeness protected everything from a person's signature, their photograph, and even their voice.[24] However, the full expansion of this right did not occur until after the Supreme Court case *Zacchini v. Scripps-Howard Broad. Co.*[25]

In 1977, the Supreme Court of the United States chose to review the right of publicity in *Zacchini v. Scripps-Howard Broad. Co*.[26] The controversy centered around a "human cannonball," whose act was was filmed at an Ohio fair and then broadcasted on the local news without his permission.[27] Though the defendant television station claimed constitutional freedom of the press, the Court found that the right of publicity did not run afoul of the First or Fourteenth

[19] Pavesich v. New England Life Ins. Co., 50 S.E. 68, 70 (Ga. 1905) ("A right of privacy in matters purely private is . . . derived from natural law.").

[20] *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (showing that there is a "zone of privacy created by several fundamental constitutional guarantees.").

[21] Haelan Labs., Inc. v. Topps Chewing Gum, Inc., 202 F.2d 866, 868 (2d Cir. 1953).

[22] *Id.*

[23] Factors Etc., Inc. v. Pro Arts, Inc., 579 F.2d 215, 220 (2d Cir. 1978), *rev'd on other grounds*, 652 F.2d 278 (2d Cir. 1981) (quoting W. PROSSER, TORTS 804, 804 (4th ed. 1971).

[24] *See* Prima v. Darden Restaurants, Inc., 78 F. Supp. 2d 337, 345-46 (D.N.J. 2000) ("There is a right of publicity in the name, voice, signature, photograph or likeness of every person.") (quoting NEV. REV. STAT. § 597.790(1) (2013)); CAL. CIV. CODE § 3344 (2014) (requiring consent on basis of right of publicity for "a use of a name, voice, signature, photograph, or likeness"); *and* RESTATEMENT (THIRD) OF UNFAIR COMPETITION, § 46 cmt. d (1995) (stating that "the use of other identifying characteristics or attributes may also infringe the right of publicity" including voice or performance style).

[25] Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 566–68 (1977).

[26] *Id.*

[27] *Id.* at 563–64.

Amendment Rights of the appropriator.[28] With the Constitutional sign-off by the Supreme Court, the right to publicity continued to grow, and was mainly utilized to protect a public figure from another party's unjust enrichment through the use of their likeness.[29] Several states even enacted statutes that recognized this right to publicity.[30] However, many courts,[31] including the Supreme Court, made sure to keep the right in a commercial context, asserting that that it had "little to do with protecting feelings or reputation."[32]

Just as changes in communications and technology spurred the original idea for the right of privacy, the invention of the personal computer and the Internet created an unprecedented need to expand the right of publicity to electronic media.[33] This form of publicity, however, has had to face the realities of digital information itself, including its intangibility and short commercial shelf life.[34]

The digital likeness is meant to protect a right of publicity in digital information. Unlike physical photographs, signatures, and

[28] *Id.* at 574–75 (stating that the court was "quite sure that the First and Fourteenth Amendments do not immunize the media when they broadcast a performer's entire act without his consent.").

[29] *See* Carson v. Here's Johnny Portable Toilets, Inc., 698 F.2d 831, 835 (6th Cir. 1983) ("The right of publicity. . . is that a celebrity has a protected pecuniary interest in the commercial exploitation of his identity."); *and* Memphis Dev. Found. v. Factors Etc., Inc., 616 F.2d 956, 957 (6th Cir. 1980) ("The famous have *an exclusive legal right* during life to control and profit from the commercial use of their name and personality.") (emphasis added).

[30] *See* CAL. CIV. CODE § 3344 (2014) ("Any person who knowingly uses another's . . . likeness . . . for purposes of advertising or selling"); MASS. GEN. LAWS ANN. ch. 214, § 3A (West 2014) (Massachusetts's right of publicity statute); OHIO REV. CODE ANN. §2741.06 (West 2014) (Ohio's statute); 765 ILL. COMP. STAT. ANN. 1075/30 (LexisNexis 2014) (Illinois's statute); *and see generally Statutes*, RIGHTOFPUBLICITY.COM, http://rightofpublicity.com/statutes (last visited Oct. 31, 2014).

[31] *See* Rosemont Enters., Inc. v. Random House, Inc., 294 N.Y.S.2d 122, 129 (Sup. Ct. 1968) (holding that "[the] requirement of commercial use which limits the New York right of privacy inheres in the 'right of publicity.'"); Blair v. Nev. Landing P'ship, 859 N.E.2d 1188, 1191–92 (Ill. App. Ct. 2006) (listing the elements of a right of publicity case, including "for another's commercial benefit"); *and* General Star Indemnity Co. v. Travelers Indemnity Co., No. CV0840233383S, 2013 WL 1849285, *11 (Conn. Super. Ct. Apr. 9, 2013) (explaining that under Missouri law, "misappropriation of a person's name as a symbol of his identity for commercial exploitation" violates the right of publicity).

[32] Zacchini, 433 U.S. at 573.

[33] Cristina Fernandez, Article, *The Right of Publicity on the Internet*, 8 MARQ. SPORTS L.J. 289, 292 (1998) (positing that "[t]he current law . . . needs to be adapted in order to take into consideration the special nature of the Internet.").

[34] *Id.* at 355–56 (discussing how the "digital revolution is changing some of the traditional concepts and a very important one is the value of information.").

other forms of likeness, digital information cannot be "owned," but merely experienced.[35] Even then, that information is perishable.[36] With each passing reproduction, it loses its value of novelty and its commercial value for the appropriator.[37] Therefore, the information being misappropriated through events like the Apple iCloud breach must fit a changed definition of publicity: one balancing a greater emphasis on the act of appropriation with a less direct resulting commercial benefit. This shift is at the heart of the law's current changes.

B. The Digital Age and the Right of Publicity

1. Introduction to the digital likeness

The right of publicity is currently available in a majority of states, whether in statutory or common law form.[38] Its modern incarnation includes two elements that must be met, in order to have a cause of action for violation of the right of publicity: (1) misappropriation of a person's likeness; [39] and (2) the commercial benefit from misappropriation to the detriment of the person.[40] The emphasis now, as it was historically, is on the commercial benefit to the appropriating party. An example of this modern emphasis can be seen in *C.B.C. Distrib. & Mktg. v. Major League Baseball Advanced Media, L.P.* which was an action to protect a Major League Baseball player's identity which was being used on an unauthorized website.[41] In the resulting opinion, the U.S. District Court for the Eastern District of Missouri granted summary judgment against the petitioner's suit because there was no obvious "intent to gain a commercial advantage" by using the likeness of a baseball player on a fantasy baseball website.[42] The court in *C.B.C.* stated clearly the rule: "[t]o prove a violation of one's right of publicity[,] a plaintiff must establish that the defendant *commercially* exploited the plaintiff's identity without the

[35] *Id*. at 304–05.

[36] *Id.* at 305.

[37] *Id.*

[38] *See* ETW Corp. v. Jireh Publ'g, Inc., 332 F.3d 915, 954 (6th Cir. 2003) (stating that a majority of states currently recognize the right of publicity).

[39] *Id.* at 930 (finding that the two elements are (1) "appropriation" of a person's identity; (2) "for purposes of trade") (quoting RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 46 (1995)).

[40] *Id.*

[41] C.B.C. Distrib. & Mktg. v. Major League Baseball Advanced Media, L.P., 443 F. Supp. 2d 1077, 1077 (E.D. Mo. 2006).

[42] *Id.*at 1089 (explaining that CBC was not using the players' names "with the intent to obtain a commercial advantage").

plaintiff's consent to obtain a *commercial* advantage" (emphasis added).[43]

Other recent Internet cases, however, have slowly broadened the scope of what the term "public figure" entitled to protection means[44] and have even found infringement on the right of publicity without direct commercial benefit to the appropriating party.[45] In other words, the right of publicity is beginning to include more common[46] Internet users and their personal data, rather than classic forms of publicity like the famous "white dress" photograph of Marilyn Monroe.[47] This is especially true when there is still some form of commercial benefit being reaped by the appropriating party. Luckily, the commercial use of personal data is also growing.

2. The commercial value of personal data

Commercial benefits and their attendant opportunities stemming from the misappropriation of the average user's personal information are beginning to grow. Companies, such as Datacoup,[48] are now offering a chance for Internet users to sell their data by connecting their social media and financial accounts to a central collection service, through which the company creates a profile on the "data points" they generate.[49] This profile, which is inherently personal, can be sold to companies in need of similar data profiles.[50] However, not every commercial exploitation of this data is by personal choice. The business of "data mining"[51] lends a more dubious and involuntary aspect to the commercial use of a person's digital likeness.

---

[43] *Id.* at 1085.

[44] *See* ETW Corp., 332 F.3d at 952–53 (stating that "a property right [exists] in the commercial value of every person's identity") (quoting MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 1:7 (2d ed. 2000)).

[45] *See* Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1184 (C.D. Cal. 2002) (granting an injunction against defendant for "aiding and abetting" violation of a California rights of publicity statute in a systemic way).

[46] *See* J. THOMAS MCCARTHY, 5 MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 28:1 (4th ed. 1996) ("[T]he right of publicity is the inherent right of every human being to control the commercial use of his or her identity").

[47] *Iconic images from history: Marilyn Monroe's white dress*, VIRGIN MEDIA, http://www.virginmedia.com/science-nature/technology/iconic-images.php?ssid=10 (last visited Oct. 31, 2014).

[48] *How It Works*, DATACOUP.COM, https://datacoup.com/docs#how-it-works (last visited Oct. 31, 2014).

[49] *Id.*

[50] *Id.*

[51] *See generally* Steve Kroft, *The Data Brokers: Selling your personal*

continued . . .

Data mining is "an analytic process designed to explore [large amounts of] data . . . in search of consistent patterns . . . [which are then validated] by applying the detected patterns to new . . . data."[52] The process itself can be relatively harmless, such as through its use in grocery store loyalty cards, where the process is used to track product movement via the purchases logged by the customers.[53] However, as its use has grown, involuntary data mining has taken on a more invasive and personal character.

According to a recent Bloomberg report, data mining companies are now utilizing data from social media and credit card purchases to place users on "health lists," alerting pharmaceutical companies and healthcare providers to user's symptoms and possible diseases.[54] Some lists are named things like "Suffering Seniors or Aching and Ailing," while other lists "are categorized by diagnosis, including groupings of 2.3 million cancer patients" and "14 million depression sufferers."[55] Each name on these lists is sold for fifteen cents and "can be broken down into sub-categories, like ethnicity, income level and geography for a few pennies more."[56] With a user base in Facebook alone of up to 1.35 billion,[57] these data points become a major economic opportunity that provides nothing to the users whose lives are represented by them. The same can be said for the photographs and videos the users post every day online.

Even private photos have commercial value online, both as items of commerce and criminal activity. According to a privacy app called PrivacyFix, developed by security software company AVG, the most valuable American female Facebook user's data, including photos, is

information, 60 MINUTES, (Mar. 9, 2014), http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/ (giving an overview of data mining practices and concerns).

[52] *What is Data Mining (Predictive Analytics, Big Data)*, STATSOFT.COM (2014), http://www.statsoft.com/Textbook/Data-Mining-Techniques#mining.

[53] Michelle Kessler & Byron Acohido, *Data miners dig a little deeper*, USA TODAY (July 11, 2006 10:11 PM ET), http://usatoday30.usatoday.com/tech/news/internetprivacy/2006-07-11-data-mining_x.htm.

[54] Shannon Pettypiece & Jordan Robertson, *Did You Know You Had Diabetes? It's All Over the Internet*, BLOOMBERG (Sept. 11, 2014 4:07 PM), www.bloomberg.com/news/2014-09-11/how-big-data-peers-inside-your-medicine-chest.html.

[55] *Id.* (internal quotations omitted).

[56] *Id.*

[57] Facebook, *Company Info*, NEWSROOM, http://newsroom.fb.com/company-info/ (last visited Feb. 4, 2015).

worth around $37.98 a year to Facebook itself.[58] In less systematic cases, private photos from social media have turned up around the globe in advertisements[59] while others have been "sold" as a form of Internet blackmail known as "sextortion."[60] Distinct online markets have even been formed around the accumulation and sale of personal photos, usually nudes.[61]

In the case of the Apple iCloud breach, "sets" of the hacked private celebrity photos were being sold on stolen image boards around the Internet within hours of the breach.[62] Each set contained about twelve pictures and sold for $350 apiece.[63] With a much larger hack of non-celebrity photos having just occurred in Snapchat's archives, the market has been flooded with even more marketable inventory.[64] Even if the images are given away at no charge from the source, their economic values could be realized later in pay sites and Internet advertising.[65] Personal videos can be treated similarly, with many of the same sites holding videos[66] as they do photos, subject to the same forms of appropriation.

---

[58] *See* Cotton Delo, *How Much Are You Really Worth to Facebook and Google?*, ADVERTISING AGE (May 7, 2014), http://adage.com/article/digital/worth-facebook-google/293042/.

[59] *See* CBSNEWS, *Mo. Family Holiday Photo Lands In Czech Ad*, CBSNEWS (June 11, 2009, 5:29 AM), http://www.cbsnews.com/news/mo-family-holiday-photo-lands-in-czech-ad/.

[60] *See* Anita Ramasastry, *The FBI's Alert Regarding "Sextortion": Why Cyber Blackmail, Though Illegal, Is Difficult to Stop and What Computer Users Can Do*, FINDLAW (Nov. 30, 2010), http://writ.news.findlaw.com/ramasastry/20101130.html.

[61] James Cook, *Inside The Internet's Secret Marketplace For Hacked Photos Of Naked Celebrities*, YAHOO! FINANCE (Oct. 8, 2014, 11:10 AM), http://finance.yahoo.com/news/inside-internets-secret-marketplace-hacked-151059958.html (discussing the different forums established for stolen personal photos, including the recent celebrity nudes).

[62] *Id.* ("A 'set' is a collection of images, usually about a dozen.").

[63] *Id.*

[64] *See* James Cook, *Hackers Access At Least 100,000 Snapchat Photos And Prepare To Leak Them, Including Underage Nude Pictures*, BUSINESS INSIDER (Oct. 10, 2014, 5:44 AM), http://www.businessinsider.com/snapchat-hacked-the-snappening-2014-10.

[65] *See* The Agency, *Student's anger after porn site used her Facebook pictures to offer 'no strings sex'*, THE TELEGRAPH (Nov. 12, 2014, 1:00 PM), http://www.telegraph.co.uk/technology/facebook/11225836/Students-anger-after-porn-site-used-her-Facebook-pictures-to-offer-no-strings-sex.html (providing an example of personal photos being stolen from social media and used as advertisements on the Internet).

[66] *See Uploading & Viewing Videos*, FACEBOOK, https://www.facebook.com/help/154271141375595/ (last visited Feb. 4, 2015)

continued . . .

Personal data, images, and video are being tapped for their economic value without regard to the people they represent. In the context of this new data economy, a new form of personal property can be found to provide a foundation for a digital right of publicity: the digital likeness.

3. The digital likeness

a. Definition of the digital likeness

Much like the "likeness" of the 20th century, the digital likeness is a broad category of personal information and image, including nearly any data that companies would want to appropriate for commercial use: from personal bank account information, to social media posts, to your own private photos and videos. This likeness tracks the twin elements of common law publicity: a likeness that can be misappropriated, and a commercial benefit for doing so. The average Internet user's likeness is available to the public in an increasing number of ways,[67] whether or not they realize it, such that their likeness carries with it the first element: an increasing ability to appropriate. The second element, or the commercial benefit, has already been seen, and is discussed above.[68] This emerging property interest in digital likeness and current laws to protect it, however, do not match up. The aforementioned security breaches illustrate the problems created between the two.

b. The problems with protection

The Home Depot data breach that occurred on September 2nd, 2014, compromised 56 million separate credit card accounts.[69] The accounts and their attendant information, including social security numbers, names, addresses, and of course, financial information, were

(providing information on how to upload videos); *and Photos*, APPLE.COM, https://www.apple.com/icloud/photos/ (last visited Feb. 4, 2015) (stating that the Apple iCloud can hold videos as well as photos).

[67] *See generally* Angela Stringfellow, *7 Emerging Social Networks to Watch in 2014*, AMERICAN EXPRESS OPEN FORUM (Jan. 15, 2014), https://www.americanexpress.com/us/small-business/openforum/articles/7-emerging-social-networks-to-watch-in-2014/; *and* Kyli Singh, *10 Rising Social Networks You Should Explore*, MASHABLE (July 28, 2014), http://mashable.com/2014/07/28/social-networks-on-the-rise/.

[68] *See* discussion *supra* Part II.B.2.

[69] Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's,* THE WALL ST. J. (Sept. 18, 2014 5:43 PM), http://online.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

likely sold following the security breach[70] to a willing buyer across the globe.[71] Assuming that some of the affected 56 million cardholders for Home Depot want to bring suit, several procedural and substantive issues would likely prevent the full remediation of their rights.

First, any form of remedy would be uncertain for two reasons: complexities of scale and consistency of the law. Even if only five percent of the Home Depot cardholders want to pursue legal remedy against Home Depot for this breach, this meager percentage leaves over three million plaintiffs with the same complaint against Home Depot. The most obvious choice would be a class action and such large-scale class actions are not uncommon.[72] Yet, discovery alone in such a case would likely take months or years.[73] The chances of settlement without actually solving the original issue would grow as both sides tire of the case. Yet, even in judgment, the likely remedy would not be the retrieval of stolen personal information, or even the full payment of economic benefit lost, due to varying statutory and common law schemes on this topic.

In a class action, the Home Depot plaintiffs will be faced with inconsistent remedies. State statutes control these class action decisions in the absence of a blanket federal law.[74] Therefore, even in federal court, the remedies for plaintiffs would depend not on their injuries, but the state in which they were injured. For instance, in *Pisciotta v. Old Nat'l Bancorp*, the United States Court of Appeals for the Seventh Circuit held that under Indiana law, "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs [had]

[70] *See* Kroft, *supra* note 51.

[71] *See* Matthew Goldstein, Nicole Perlroth & David E. Sanger, *Hackers' Attack Cracked 10 Financial Firms in Major Assault*, N.Y. TIMES, Oct. 3, 2014, at A1, *available at* http://dealbook.nytimes.com/2014/10/03/hackers-attack-cracked-10-banks-in-major-assault/?_php=true&_type=blogs&_r=0 (discussing how the attacks on JPMorgan Chase and nine other financial institutions are thought to have originated with hackers in Russia).

[72] For examples of class actions suits in personal data breaches, *see* In re Target Corp. Customer Data Sec. Breach Litig., 11 F. Supp. 3d 1338, 1338 (J.P.M.L. 2014); In re Adobe Sys. Privacy Litig., No. 13-CV-05226-LHK, 2014 WL 4379916, at *1 (N.D. Cal. Sept. 4, 2014); In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 942 (S.D. Cal. 2014); *and Home Depot Data Breach Class Action Lawsuit*, GIRARD GIBBS LLP (Nov. 21, 2014), http://www.girardgibbs.com/home-depot/.

[73] *See Institutional Investor Services FAQs*, Shepherd, Finkelman, Miller & Shah, LLP, http://www.sfmslaw.com/Institutional-Investor-Services/Institutional-Investor-Services-FAQs.shtml (explaining that class actions take on average "approximately two to three years," but some can be longer).

[74] Erie R. Co. v. Tompkins, 304 U.S. 64, 78 (1938) (explaining that "[e]xcept in matters governed by the Federal Constitution or by acts of Congress, the law to be applied in any case is the law of the state.").

not suffered a harm that the law is prepared to remedy."[75] In *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.,* this patchwork of state remedy availability was particularly evident.[76] A class action against Sony for a breach of the personal data of millions of users, the suit spanned several states.[77] When consolidated in the United States District Court for the Southern District of California, the Court dismissed claims brought under Massachusetts, Ohio, Texas, and New York law, mostly for lack of a remediable injury, but kept others brought under California, Florida, Michigan, Missouri, and New Hampshire law.[78] The claims that did survive summary judgment provided mostly declarative and injunctive relief, along with economic damages, but not the retrieval of the lost data.[79] All plaintiffs had substantially the same injury stemming from the same transaction, but only a few of them were able to address it. Therefore, a constant and worthwhile remedy among plaintiffs in these personal data breach class actions is unlikely under the current law.

Second, forming a class action for the breach would create further conflicting application of law issues and conflicts of law, because the current right of publicity is a creature of state law.[80] Apart from remedy, conflicting definitions of elements and degrees of appropriation required for the right of publicity would guarantee another tangled web of judicial decision-making on top of an already complex class action.[81] This problem has already been shown in the fractured decision making of the court's holding in *In re Sony*.[82]

Third, these actions would not prevent the further appropriation of personal data, the basis for the digital likeness, by later breaching groups. Each breach would beget a new suit. And in each suit, it is unlikely that the defendant entity would be required by a court to implement the changes needed to prevent new breaches due to the patchwork of remedies and legal standards that must be met. This problem is exacerbated by the fact that the cause of the injury is

[75] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 639 (7th Cir. 2007) *overruled in part on other grounds in* Remijas v. Neiman Marcus Group, LLC, No. 14 C 1735, 2014 U.S. Dist. LEXIS 129574, at *4–5 (N.D. Ill. Sept. 16, 2014).

[76] In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 953 (S.D. Cal. 2014).

[77] *Id.* (describing the plaintiffs as "a nationwide putative consumer class").

[78] *Id.* at 963–973.

[79] *Id.* at 1014.

[80] Kevin L. Vick & Jean-Paul Jassey, *Why a Federal Right of Publicity Statute Is Necessary*, 28 COMM. LAW., 14, 15 (Aug. 2011) ("There is no federal right of publicity; it is entirely a matter of state law.").

[81] *Id.*

[82] In re Sony, 996 F. Supp.2d at 1013.

outside of the defendant's direct control and may not be considered an "impeding injury" for the purposes of an injunction.[83] In federal court, a recent Supreme Court case, *Clapper v. Amnesty Int'l USA*,[84] may impose a standing analysis for the interception of a user's personal data that would require something more than a "future harm that is not certainly impending" and a harm that is not "simply the product of [the plaintiffs'] fear" of data theft.[85] However, since this case is new, many states have not adopted its standing analysis, so it would not be controlling for a state law based action. Therefore, the standing required for any injunctive relief meant to change a defendant's data protection policies would likely be questioned under an analysis similar to *City of Los Angeles v. Lyons*,[86] which is an older, more accepted standing decision in state and federal jurisprudence.

In *City of Los Angeles v. Lyons*, the Supreme Court reversed judgment on a Fourth Amendment claim brought for injunctive relief against the Los Angeles Police Department because the requested relief would not fix the previous injury, and any future injury was found to not be imminent enough.[87] The Court held that under federal law, "[an injunction] is unavailable absent a showing of irreparable injury, a requirement that cannot be met where there is no showing of any real or immediate threat that the plaintiff will be wronged again . . . ."[88]

In the case of a personal data breach like those involving Home Depot or Apple, the facts provided by the plaintiffs would likely prevent injunctive relief under the *Clapper* and *Lyons* requirements for the same reasons: injunctions would not remedy past harm and the future injury could not be certain to occur in the same place again. Although the right of publicity is currently only under state law, some states including Texas[89] and Ohio[90] that recognize the right of

[83] *See* Alison Frankel, *Why (most) consumer data breach class actions vs Target are doomed,* REUTERS (Jan. 13, 2014), http://blogs.reuters.com/alison-frankel/2014/01/13/why-most-consumer-data-breach-class-actions-vs-target-are-doomed/ (explaining that "consumers will have . . . [a] very hard time showing enough of an injury to establish their right to sue in federal court.").

[84] Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1138 (2013).

[85] *Id.* at 1141.

[86] City of L.A. v. Lyons, 461 U.S. 95, 95 (1983).

[87] *Id.* at 112–13.

[88] *Id.* at 111.

[89] *See* Tex. A&M Univ.–Kingsville v. Yarbrough, 347 S.W.3d 289, 290 (Tex. 2011) ("There must also be a reasonable expectation that the same action will occur again if the issue is not considered") (citing City of L.A. v. Lyons, 461 U.S. 95, 103 (1983)).

[90] *See* Carl L. Brown, Inc. v. Lincoln Nat'l Life Ins., No. 02AP-225, 2003 WL

continued . . .

publicity also follow the *Lyons* elements for injunctions in a way that could stop first-time data breach victims from trying to prevent continuing injury. In these states, the only available remedy to these breaches may be economic damages.

As will be seen in Part III, all of these problems with remedying security breaches can be attended to and the digital right of publicity can be expanded in the PDPBAA with minor textual adjustments.

III. ANALYSIS

A. The Personal Data Protection and Breach Accountability Act

As provided in Part II, the current legal scheme suffers from three problems with remedying the right of publicity violated in a large personal data breach: suit logistics, conflicts of law, and finality of remedy. The proposed law, the PDPBAA,[91] however, can meet each of these problems with a slight textual update to reflect the new digital likeness growing in current culture.

The PDPBAA would amend the federal code to create both a criminal and civil cause of action against the companies, service providers, and persons that allow the large-scale misappropriation of personal data through security breaches and data mining practices.[92] Further, much like the regulations promulgated by the U.S. Securities and Exchange Commission, an entity covered by the Act would have to "implement a comprehensive personal data privacy and security program that includes administrative, technical, and physical safeguards" to protect the personal information it carries.[93] There would even be measures put in place to prevent the further spread of the appropriated personal data.[94] All of this would be condensed into a filing and notification system where the federal government, by way of the Department of Homeland Security, would form an agency to receive and monitor all security reports and vulnerabilities, taking action as needed.[95]

21153280, ¶ *6 (Ohio Ct. App. May 30, 2003) (holding that "[a] party's unsupported assertion that he or she has suffered, or will suffer an injury, is not sufficient to confer standing" after referencing Lyons).

[91] *See* S. 1995. *See also Summary: S.1995–113th Congress (2013-2014)*, CONGRESS.GOV https://www.congress.gov/bill/113th-congress/senate-bill/1995 (last visited Feb. 4, 2015) (providing a summary of the purpose and content of the PDPBAA).

[92] S. 1995 §§ 101–102.

[93] S. 1995 § 202(a)(1).

[94] *See Summary:* S.1995, *supra* note 91.

[95] *See id.*

Within the structure of the PDPBAA, the solutions to the problems inherent in previous data breach suits become evident. Large groups of plaintiffs could still sue under the Act, but the now completely federal law would be consistent for the sake of remedies and elements of the claims, regardless of the state where injury occurred. Any issues with standing would be ameliorated by a statutory cause of action. Even the finality of the actions would be assured by the ongoing monitoring of a government agency, rather than the plaintiffs themselves.

Despite the stated benefits of this proposed Act, the PDPBAA does not clearly provide for the protection of personal photos and videos, which were the fodder for the Apple iCloud breach. The statutory text could be improved, then, by broadening its definition of "sensitive personally identifiable information"[96] to include actual images and videos that would reflect the digital likeness of the user or customer. This definition could then explicitly protect users from another imminent iCloud or Snapchat private photo breach and provide a new and consistent federal right of digital publicity rather than a state law based hodgepodge.

B. The Definition of Sensitive Personally Identifiable Information

The current definition of sensitive personally identifiable information in the PDPBAA states that "'sensitive personally identifiable information' means any information or compilation of information, in electronic or digital form that includes [several listed forms of data]."[97] Among the forms of data listed is any "[u]nique biometric data such as a fingerprint, voice print, face print, a retina or iris image, or any other unique physical representation."[98] The "term unique physical representation" is not defined, but is obviously a catchall for other similar biometric data. There is no clear inclusion in the long definition of sensitive personally identifiable information for a personal photo or video, forms of data which track the common law right of publicity and are frequently left unsecured or even mined by companies like Snapchat.[99]

---

[96] S. 1995 § 3(a)(15).

[97] *Id.*

[98] *Id.* at § 3(a)(15)(D).

[99] *See* Complaint, Request for Investigation, Injunction, and Other Relief, at 1, 7, In re Snapchat, Inc., (May 16, 2013), *available at* http://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf (alleging deceptive trade practices and misuse of private photos); *Snapchat Settles FTC Charges That Promises of Disappearing Messages*

continued . . .

A court may construe "unique physical representation" to include a photograph that does not contain biometric information, but a court using the plain meaning rule coupled with the statutory construction principle *ejusdem generis* (defined below), may not. The plain meaning rule is a foundational canon of statutory construction.[100] It states that the court assumes "a legislature says in a statute what it means and means in a statute what it says there."[101] Therefore, "when the words of a statute are unambiguous . . . 'judicial inquiry is complete.'"[102] Here, the statute did not define the term "unique physical representation," so a court would have to look to dictionary definitions or other forms of statutory interpretation[103] to resolve the ambiguity and find whether a personal photograph or video may fit within the category.

Since the category already contains a list,[104] the most likely canon of construction to resolve this ambiguity would be *ejusdem generis*. *Ejusdem generis* translates to mean "of the same kind or class"[105] and holds "that when a general word or phrase follows a list of specifics, the general word or phrase will be interpreted to include only items of the same class as those listed."[106] The canon is meant to "[limit] general terms which follow specific ones to matters similar to those specified" and remove ambiguity in the statute. [107] However, "it may not be used to defeat the obvious purpose of legislation."[108]

The Act's categorical list reads "[u]nique biometric data such as a fingerprint, voice print, face print, a retina or iris image, or any other unique physical representation."[109] Apart from the last catchall term, each of the other items on the list all have distinct security or

Were False, FED. TRADE COMM'N. (May 8, 2014), http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

[100] Conn. Nat'l Bank v. Germain, 503 U.S.249, 253–54 (1992) (explaining that "in interpreting a statute, a court should always turn first to one, cardinal canon above all" referring to the plain meaning rule).

[101] *Id.*

[102] *Id.* at 254 (quoting Rubin v. United States, 449 U.S. 424, 430 (1981) (internal quotation marks omitted)).

[103] *See* United States v. Am. Trucking Ass'ns, 310 U.S. 534, 542–45 (1940); Carlos E. Gonzalez, *Reinterpreting Statutory Interpretation*, 74 N.C. L. REV. 585, 596 (1996) (discussing how textual theories within statutory interpretation sometimes "read textual words according to their literal dictionary definitions.").

[104] S. 1995 § 3(a)(15)(D).

[105] *Ejusdem generis*, BLACK'S LAW DICTIONARY 631 (10th ed. 2014).

[106] *Id.*

[107] Gooch v. United States, 297 U.S. 124, 128 (1936).

[108] *Id.*

[109] S. 1995 § 3(a)(15)(D).

identification-based purposes, and therefore relate similarly to the previous categories in the statute such as passwords and pin numbers.[110] Under *esjudem generis*, the result would likely be that a casual photograph or video, not used for security or identification purposes, would be left out of the catchall term at the end of the list. Therefore, to prevent such ambiguity and unfavorable judicial interpretation, the statute should be updated to provide specifically for a user's personal photos and videos.

Since it can be demonstrated that a favorable interpretation of the statute may be difficult, the definition of "unique physical representation" should be updated to include **any picture or visual representation of the user, including any identification or personal photo or video in any format**. Unlike the original biometric focus of "unique physical representation," this inclusion would protect images that would not have direct security value but fall under the category of digital likeness and therefore would be subject to protection under the common law right of publicity. Overall, however, this Act would protect personal data in a way that is not otherwise protected today and therefore should be enacted after its stint in committee.

Like every new, sweeping law, a constitutional challenge, probably by the data-holding companies themselves, will be imminent upon the PDPBAA's enactment. Luckily, the Supreme Court and Constitution have already provided the bases for its constitutionality.

C. Constitutional Concerns

1. Commerce Clause

The PDPBAA, even with the aforementioned textual addition, will likely be upheld on three grounds: the Commerce Clause,[111] a commerce exception to First Amendment rights, and historic privacy rights. Situated in Article I of the Constitution, the Commerce Clause gives Congress power to "regulate Commerce with foreign Nations, and among the several States, and with the Indian Tribes."[112] The Clause has been used to give broad authority to Congress in statutes preventing the spread of child pornography through the Internet[113] as

[110] *See* S. 1995 § 3(a)(15)(E)–(G) (specifically including electronic security codes and "unique account identifier[s]").

[111] U.S. CONST. art. I, § 8, cl. 3.

[112] *Id.*

[113] 18 U.S.C. § 2252A (2012) (applying to anyone who "knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce . . . by computer, any child pornography").

well as the basis for statutes protecting intellectual property such as the Lanham Act.[114] However, in a striking example, the Commerce Clause is the basis for the Children's Online Privacy Protection Act ("COPPA"),[115] a clear predecessor to the PDPBAA.

COPPA is a federal statute that requires websites collecting personal information of children under the age of 13 to comply with a series of data privacy controls and parental consent practices to protect the collected information from theft.[116] By failing to comply, the websites open themselves to suit both by the Federal Trade Commission[117] and state attorneys general.[118] COPPA's basis for enforcement in the Commerce Clause can be found in its definitions section, where the Act is meant to apply to any "operator" who "operates a website located on the Internet or an online service . . . for commercial purposes, including any person offering products or services for sale through that website . . . involving commerce . . . among the several States or with 1 [sic] or more foreign nations."[119] COPPA reproduces near verbatim the Commerce Clause in its jurisdictional definition and so far has not been overturned or declared unconstitutional by any federal court.

Considering the previous statutes still in place, the PDPBAA clearly falls within the scope of Congress's power because it involves the sale of personal data that is collected and distributed throughout the United States[120] and the world.[121] Even when the data is merely collected, not sold, the commerce clause can apply to this form of commercial intercourse.[122] The Internet, the reason for the Act itself, is a web of commercial intercourse that has wide-ranging effects for

---

[114] 15 U.S.C. § 1051 (2012) (applying to marks used "in commerce").

[115] *See generally* 15 U.S.C. §§ 6501–6506 (2012). *See infra* notes 116–19 and accompanying text.

[116] *See generally* §§ 6501–6506.

[117] § 6505 (stating "this chapter shall be enforced by the Commission under the Federal Trade Commission Act").

[118] *See* § 6504(a)(1) (allowing "the attorney general of a state" to "bring a civil action on behalf of the residents of the State . . . [to] enforce compliance").

[119] § 6501(2).

[120] *See* S. 1995, § 2(2) ("identity theft is a serious threat to the Nation's economic stability, homeland security, the development of e-commerce, and the privacy rights of people in the United States").

[121] *See* Int'l Bancorp, LLC v. Societe Des Bains De Mer Et Du Cercle Des Etrangers a Monaco, 329 F.3d 359, 365 (4th Cir. 2003) (holding that "it has been well established that the Commerce Clause reaches to foreign trade.").

[122] *See* Gibbons v. Ogden, 22 U.S. 1, 189–90 (1824) (holding that the word "commerce" in the Commerce Clause "is traffic, but it is something more: it is intercourse.").

all involved.[123] Therefore, the statute would very likely be upheld under the Commerce Clause, as its ancestors, like the Lanham Act, have.[124] Further, though, the PDPBAA could be found constitutional despite the objections of the regulated companies under the First Amendment.

2. First Amendment challenges

In the face of a new, widespread regulation involving disclosure of private information, regulated parties will likely bring suit claiming a violation of their First Amendment Rights, but this will fail due to established precedent concerning the Rights' exceptions. The First Amendment of the Constitution protects the freedom of speech.[125] This freedom of speech does not stall at the spoken word, but can include any written or typed communication, including information on the Internet.[126] Even the choice not to speak has been considered protected under the Amendment.[127] Further, the Amendment's inherent rights have been extended to corporations, which many if not most of the regulated parties under the PDPBAA will be.[128] Yet, the enlarged scope of the Amendment will not guarantee success by the Act's opponents. The Supreme Court has already made a ruling on the right of publicity and the First Amendment rights of appropriators in *Zacchini v. Scripps-Howard Broad. Co.* that could be applied to the PDPBAA.

As already mentioned, the Court held in *Zacchini* that the right of publicity does not infringe upon the First Amendment rights of an appropriator, even one that relied on communication as a form of commerce.[129] In fact, the Court was "quite sure that the First and Fourteenth Amendments do not immunize the media when they

[123] *See* Am. Libraries Ass'n v. Pataki, 969 F. Supp. 160, 173 (S.D.N.Y. 1997) (finding "inescapable" that "the Internet represents an instrument of interstate commerce . . . [and] impels traditional Commerce Clause considerations").

[124] *See Int'l Bancorp*, 329 F.3d at 363–64 (holding that "'commerce' under the [Lanham] Act is coterminous with that commerce that Congress may regulate under the Commerce Clause of the United States Constitution").

[125] U.S. CONST. amend. I ("Congress shall make no law . . . abridging the freedom of speech").

[126] *See* Reno v. Am. Civil Liberties Union, 521 U.S. 844, 849 (1997) (holding that that speech on the Internet is "protected by the First Amendment").

[127] *See* Pac. Gas & Elec. Co. v. Pub. Utils. Comm'n., 475 U.S. 1, 16 (1986) ("[f]or corporations as for individuals, the choice to speak includes within it the choice of what not to say").

[128] *Id.* ("[W]e have held that speech does not lose its protection because of the corporate identity of the speaker.").

[129] Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 563, 574–75 (1977).

broadcast a performer's entire act without his consent."[130] A federal court may rely on this precedent to form a federal exception to First Amendment rights by comparing the state law right of publicity to the inherent federal right of publicity created by the PDPBAA. However, if a single case is not enough, precedent also demonstrates that commerce involving speech may not be protected under the First Amendment in certain relevant situations.

Along with *Zacchini*, the Supreme Court has held that the mere regulation of conduct that is "in part initiated, evidenced, or carried out by means of language, either spoken, written, or printed," will not guarantee the protection of the First Amendment where that conduct is in fact harmful to the public.[131] As the Supreme Court affirmed in *Ohralik v. Ohio*, "the State does not lose its power to regulate commercial activity deemed harmful to the public whenever speech is a component of that activity."[132] For instance, the Supreme Court has held the monitoring and reporting requirements for corporations promulgated under the Securities and Exchange Commission to be constitutional despite the fact that they require the corporations to speak.[133]

If the companies or individuals regulated by the PDPBAA claim that the reporting and monitoring requirements violate their free speech rights, a federal court will likely dismiss these statements, quoting the strong precedent of *Zacchini* and a general pattern of regulating commerce involving speech that otherwise would harm the public at large. Lastly, there may be another basis to uphold the PDPBAA's protections in a historic right of privacy.

3. The historic right to privacy

In finding the PDPBAA constitutional, the Supreme Court may also appeal to an ancillary public interest in a right to privacy that has persisted throughout American legal scholarship. This right exists apart from the Constitution as a basic human interest. The Supreme Court in *Griswold v. Connecticut* recognized that this "right of privacy

[130] *Id.*

[131] Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978) (quoting Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 502 (1949)).

[132] *Id.* at 456.

[133] *See* Bulldog Investors Gen. P'ship v. Sec'y of the Commonwealth, 953 N.E.2d 691, 700–01 (2011) (acknowledging that "the Supreme Court has stated . . . that 'the exchange of information about securities' is speech that is 'regulated without offending the First Amendment' because it is a means of carrying out such commercial activity") (citing Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 456 (1978)).

[is] older than the Bill of Rights . . . [and] older than our political parties . . . ."[134] Even the scholars Brandeis and Warren, who begot the idea of the right of publicity,[135] "described a 'general right to privacy for thoughts, emotions, and sensations [that] should receive the same protection, whether expressed in writing, or in conduct, in conversation, [or] in attitudes.'"[136] This right to be "let alone" became a necessity during a time of technological change that resulted in a flood of private information, where the "harm wrought by such invasions [was not] confined to the suffering of those who may be made the subjects of journalistic or other enterprise."[137] This supply increased the demand for further information on private lives as it does today with personal data and photos.[138] Acknowledging the digital likeness and the PDPBAA's protection of it would protect a historic right to have a private life as Warren and Brandeis advocated. In other words, there could be a historic basis for personal data privacy under the Act if it is passed, along with its allowances under the First Amendment and backing of the Commerce Clause.

IV. CONCLUSION

Personal data protection on the Internet today faces two daunting problems: the recognition of a property right in personal data to be protected and the remedying of protection problems. In light of these threats to data security, a new form of intellectual property could provide clearer claims for data protection and appropriation. This new form is the digital likeness, which acts as the recognition of an already expanding right of publicity found in common and statutory law. However, increasingly frequent security breaches of personal data depositories in companies such as Apple and Home Depot have left many without an easy remedy in the courts or any form of deterrence for appropriating this likeness. A new statute in committee, the PDPBAA, has the ability to alleviate the problems of suit logistics, conflicts of law, and finality of remedy while protecting the personal data that makes up the digital likeness. With a minor textual change to correct the ambiguity in protecting personal photos and videos, the Act would likely stand up to constitutional muster in court and protect the

[134] Griswold v. Connecticut, 381 U.S. 479, 486 (1965).

[135] *See* Warren & Brandeis, *supra* note 14, at 199.

[136] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1093 (2002) (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 206 (1890)).

[137] Warren & Brandeis, *supra* note 14, at 196.

[138] *Id.*

digital likenesses of millions of Internet users. With the PDPBAA in place, private photos and videos will finally be protected so as to prevent any more "Shy Godivas" from being exposed yet again in the town square of the Internet.