GOOGLE:
THE ENDEMIC THREAT TO PRIVACY

Bridget A. Sarpu*

I. Introduction

In April 2012, Google announced "Project Glass" on its social networking service Google+ (Google Plus).[1] The product, later changed to "Google Glass," is advertised as a wearable computer with a head-mounted display.[2] Imagine a pair of glasses that projects

* J.D. Candidate, May 2015, *Suffolk University Law School*. Editor-in-Chief, *Journal of High Technology Law*.

[1] *See* Nick Bilton, *Google Begins Testing Its Augmented-Reality Glasses*, NY TIMES (April 4, 2012), *archived at* http://perma.cc/T93G-AQKC (explaining that Project Glass was announced through Google+).

[2] *See* Jorge Espinosa, *How Google Glass Could Alter Our Perception Of IP*, FLORIDA BUS. REV. (May 8, 2013), *archived at* http://perma.cc/Y72A-WAN5 (describing Google Glass features); *see also* Phil Lee, *A Brave New World Demands Brave New Thinking*, PRIVACY AND INFO. LAW BLOG (June 3, 2013), *archived at* http://perma.cc/6J8-TGMZ (explaining that Google Glass can connect to the Internet, is voice-controlled by the wearer, and has a built-in computer display in the corner of one lens). The proposed launch capabilities of the device are the ability to search the web, bring up maps, take photographs and video, and share to social media. *Id. See also* Carlos Dang, *The Brave New World of Google Glass*, THE NANOBYTE (Mar. 6, 2013), *archived at* http://perma.cc/WR87-BV7U (demonstrat-

a computer screen millimeters from your eye.[3] The company indicated that it wanted to build a technology that was "seamless, beautiful, and empowering; [t]o share the world through your eyes; [t]o get answers and updates, instantly; [t]o be there when you need it, and out of your way when you don't."[4] Google Glass will allow you to take pictures, record what you see hands-free, share what you see live, obtain directions, send messages, and ask whatever is on your mind.[5] As the technology develops, more and more possibilities arise: Imagine walking up to a stranger on the street, having the glasses scan the individual's face and instantly provide information regarding the person.[6] The Google Glass on board camera is capable of recording vid-

ing, through a video Google Glass capabilities through the eyes of the wearer); Grant Atkinson, *Google Glasses Legal Issues*, LEGALMATCH (Jan. 8, 2014), *archived a* http://perma.cc/6L95-FGRL (outlining the broad issues Google Glass faces like accidents caused by those wearing the glass while driving, intellectual property issues, and reasonable expectation of privacy issues).

[3] *See* Espinosa, *supra* note 2 (describing unique features of Google Glass).

[4] *See Google Glass*, GOOGLE+, *archived at* http://perma.cc/ZB4B-GRGN?type=image (unfolding Google Glass mission and goals).

[5] *See What it Does*, GLASS, *archived at* http://perma.cc/Q5SH-BPWP (depicting Google Glass features); *see also* Lisa Sorg, *A Crack in Google Glass: Wearable Technology's Glassault on Privacy*, INDY WEEK (Oct. 9, 2013), *archived at* http://perma.cc/KA9N-2KUJ (discussing the features and services of Google Glass). "'OK Glass, take a picture,' a woman commanded, her right eye fixed on a screen hanging in her peripheral vision. Her friend posed and smiled. Seconds later, Glass complied. On the screen appeared the photo, which she could have later shared on social networks or in real time using Wi-Fi or Bluetooth." *Id.*

[6] *See* Espinosa, *supra* note 2 (noting the potential capabilities of Google Glass); *see also* Alexei Oreskovic, *Google Glass is Both Cool and Creepy*, BUSINESS INSIDER (May 19, 2013), *archived at* http://perma.cc/6HNV-M56X (explaining that some first-time Google Glass users were wearing the recording-capable device everywhere, including in crowded bathrooms); *Google Glass' Abilities Excite Surgeons*, HEALTH CITIZEN (Jan. 19, 2014), *archived at* http://perma.cc/RU9P-5H5G (commenting on the use of Google Glass by surgeons while operating on patients); Adi Robertson, *Senator Al Franken Asks Google Glass Developer to Limit Scope of Facial Recognition App*, THE VERGE (Feb. 6, 2014), *archived at* http://perma.cc/NH4-3AFG (introducing a potential Google Glass application called NameTag that uses facial recognition software). Google has not sanctioned the NameTag Google Glass app. *Id.* Senator Al Franken has urged NameTag to delay the release of their program until official privacy regulations are released. *Id. See also* Darrell Etherington, *Google Glass Getting A Face Recognition App This Month, But It Won't Get Google's Blessing*, TECHCRUNCH (Dec. 18, 2013), *archived at* http://perma.cc/432D-CBKQ (describing another new facial recognition application available for Google Glass called FaceRec); Robert H. Sloan & Richard Warner, *Beyond Notice and Choice: Privacy, Norms & Consent* 14 J. HIGH TECH. L. 370,

eo and does have the potential to utilize facial recognition software[7], even though Google has chosen not to provide any facial recognition capabilities in Glass for its first generation project.[8]

Facial recognition technology consists of software that "can pick someone's face out of a crowd, extract the face from the rest of the scene and compare it to a database of stored images."[9] "Facial recognition software is based on the ability to recognize a face and then measure the various features of the face."[10] Typical facial "landmarks" or "nodal points" that make a face distinguishable include the distance between the eyes, the width of the nose, and the length of the jawline.[11] The primary users of facial recognition software have been law enforcement agencies.[12] They have used the software to capture random faces in a crowd or have installed police cameras throughout high activity neighborhoods in attempt to reduce crime rates.[13] Other users have included the United States govern-

403 (quoting Daniel Solove stating "we are heading toward a world where an extensive trail of information fragments about us will be forever preserved on the Internet, displayed instantly in a Google search.").

[7] *See Google Chief Says Glass Privacy Fears will Fade*, PHYSORG (Sept. 2, 2014), *archived at* http://perma.cc/8SPS-5KRU (discussing the capabilities of Google Glass and the privacy concern surrounding the potential for facial recognition software).

[8] *See* Letter from Susan Molinari, Vice President, Pub. Policy & Gov't Relations Google Inc., to Rep. Joe Barton, Co-Chairman, Bi-Partisan Privacy Caucus (June 7, 2013), *archived at* http://perma.cc/FT96-GUJB (indicating that Google Glass will not include facial recognition software).

[9] *See* Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOWSTUFFWORKS, *archived at* http://perma.cc/RB53-YF28 (describing how facial recognition software works).

[10] *See id*. (discussing how facial recognition software works in separating facial features from background features). "In order for this software to work, it has to know how to differentiate between a basic face and the rest of the background." *Id.*

[11] *See id.* (stating that "[e]very face has numerous, distinguishable landmarks, the different peaks and valleys that make up facial features"). Each human face has approximately 80 nodal points that can be measured by the software. *Id.* "These nodal points are measured creating a numerical code, called a faceprint, representing the face in the database." *Id.*

[12] *See id.* (noting the use of facial recognition by law enforcement).

[13] *See id.* (explaining how law enforcement uses facial recognition software to effectively match identification). "In 2001, the Tampa Police Department installed police cameras equipped with facial recognition technology in their Ybor City nightlife district in an attempt to cut down on crime in the area." *Id.* The system failed to do the job, and thus was discontinued in 2003. *Id.* People in the area were

ment using the software for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program, which is used to identify travelers trying to enter the United States.[14] Some government agencies have used the system as a means for security, in order to prevent voter fraud.[15] With the impressive potential uses of facial recognition software, there also comes great concern involving privacy rights and privacy infringement.[16]

Google Glass has made the decision not to include facial recognition in the Google Glass device, even though the glasses could have those capabilities.[17] Their choice to not include the technology rests solely on the profound questioning of privacy issues.[18] In a Google+ article, Project Glass noted, "[a]s Google has said for several years, we won't add facial recognition features to our products without having strong privacy protections in place. With that in mind, we won't be approving any facial recognition Glassware at this time."[19]

Developers have noted that it may be possible to buy and load applications, called "Glassware," without needing Google's permission and that certain applications could provide facial recognition

seen wearing masks prohibiting the cameras from getting a clear enough shot to identify a perpetrator. *Id.*

[14] *See id.* (describing additional uses of facial recognition within airports across the country). "Boston's Logan Airport…ran two separate tests of facial recognition systems at its security checkpoints using volunteers." *Id.* Over a three month period, the system only had a 61.4% accuracy rate, leading airport officials to determine other security possibilities. *Id.* The U.S. government program US-VISIT is designed to protect against foreign terrorists and criminals. *Id.* "When a foreign traveler receives [a] visa, he will submit fingerprints and have his photograph taken." *Id.* The fingerprints and photographs will be used to verify the identity of the individual trying to enter the United States. *Id.* The fingerprints and photo are then checked against a database of known criminals and suspected terrorists. *Id.*

[15] *See* Bonsor & Johnson, *supra* note 9 (describing the use of facial recognition software as a means to prevent voter fraud at voter booths).

[16] *See* Bonsor & Johnson, *supra* note 9 (recognizing that the facial recognition software's great potential comes with drawbacks).

[17] *See* Erika Morphy, *Google Glass Drops Facial Recognition (For Now)*, FORBES (June 2, 2013), *archived at* http://perma.cc/3XR5-TMTP (noting that although Glass is capable of using facial recognition software, Google has opted out of using the software for its upcoming generation of Glass).

[18] *See id.* (noting the privacy concerns with regard to Google Glass and facial recognition software).

[19] Eric Larson, *Google Glass Won't Have Facial Recognition Apps Yet*, MASHABLE (June 1, 2013), *archived at* http://perma.cc/QA65-Y43D.

service.[20] Google claims that they do not promote the use of such apps.[21] Even though Google has claimed to have no immediate plans to offer face recognition software, the open-ended possibility has left lawmakers, legislatures, and people "freaking out."[22]

Since the announcement of the Project Glass initiative, there have been numerous articles written, letters constructed, discussions, and even legal bans regarding the unreleased glasses.[23] Some companies have even taken the liberty to design programs to stop Google Glass.[24] Every debate and concern revolves around Google Glass and the issue of privacy.[25] With numerous and current federal and state statutes in place prohibiting the unknown photographing and

[20] *See* Charles Arthur, *Google 'Bans' Facial Recognition on Google Glass - but Developers Persist*, THE GUARDIAN, *archived at* http://perma.cc/DTF8-GFA6 (recognizing that although Google has banned facial recognition, related applications do exist and have potential to be loaded onto the Glass technology).

[21] *See id*. (noting that Google does not promote the use of facial recognition apps, even if Glass can use them).

[22] *See* Will Oremus, *"Don't Be Creepy": Google Glass Won't Allow Face Recognition*, SLATE (June 3, 2013), *archived at* http://perma.cc/NE2E-QW92 (explaining how facial recognition software is a definite possibility for Google Glass in the future, and presents concern for society). *See also* Dileep Thekkethil, *Google Glass Will Read Emotions on Face, Tell Gender and Age*, THE AMERICAN BAZAAR (Sept. 1, 2014), *archived at* http://perma.cc/DC8T-VHG5 (introducing new Google Glass application SHORE, which is considered one of the forerunning apps in real-time face detections).

[23] *See* Letter from Rep. Joe Barton, Co-Chairman, Bi-Partisan Privacy Caucus, to Larry Page, CEO, Google (May 2013), *archived at* http://perma.cc/KZ7R-TVQE (providing an example of the attention Google Glass had been getting with a letter that was written by members of Congress to Google concerning Google Glass and possible constitutional violations). *See also* Richard Gray, *The Places Where Google Glass is Banned*, THE TELEGRAPH (Dec. 4, 2013), *archived at* http://perma.cc/AM9L-E9PH (listing the numerous places where Google Glass is already banned including in the car, cinemas, strip clubs, casinos, restaurants, hospitals, sports grounds, concerts, banks, and ATMs); Dan Levine, *Google Sets Roadblocks to Stop Distracted Driver Legislation*, REUTERS (Feb. 25, 2013), *archived at* http://perma.cc/62ZX-JTRH (voicing the concerns law enforcement and other groups have in regards to allowing Google Glass to be worn while driving).

[24] *See* Doug Gross, *This Gadget Can Knock Drones and Google Glass Offline*, CNN (Sept. 9, 2014), *archived at* http://perma.cc/4Y7Q-LBYN (introducing Cyborg Unplug, a "wireless anti-surveillance system," or portable router that can detect when certain technology is trying to access a user's Wi-Fi signal and then boot that individual off of it.)

[25] *See* Letter from Rep. Joe Barton, *supra* note 23 (emphasizing the potential loss of privacy if/when Google Glass is released).

videotaping of others, Americans wonder whether the new Google Glass technology could infringe on their privacy.[26]

This note explores the legal implications of facial recognition software specifically with the Google Glass technology and the potential privacy concerns that may arise. This note begins by outlining a brief history of privacy, including the birth of privacy in American and modern privacy law as it has evolved with technology. Also, the history incorporates some of Google's company history and involvement with privacy concerns over the recent years. This note then explores technology already using facial recognition software and what it really means for the public if Google were to ever choose to use the software permanently in Glass. Finally, this note assesses some of the potential solutions already being discussed to ensure Google Glass is used safely. It also discusses potential resolutions society may consider when Google Glass is finally released to the public.

II. History

A.The Birth of Privacy in America

In America, privacy has played a critical role in promoting free speech and developing important institutions throughout the country.[27] Most scholars consider Samuel Warren and Supreme Court Justice Louis Brandeis's law review article, *The Right to Privacy*,[28] as the first attempt to explain American privacy jurispru-

[26] *See* Letter from Rep. Joe Barton, *supra* note 23 (raising the concern that Google Glass could conflict with the "average American's" general expectation of privacy).

[27] *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 139-40 (Yale University Press, 2007) (discussing how anonymity can be essential to free speech). The Supreme Court has noted: "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all." *Id.* at 139. "Anonymity allows people to be more experimental and eccentric without risking damage to their reputations…Anonymity can be essential to the presentation of ideas, for it can strip away reader biases and prejudices and add mystique to a text…Anonymity thus can be critical to preserving people's right to speak freely." *Id.* at 139-40.

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

dence.[29] The co-authored article was published in response to the newest technology of the time, Kodak cameras, which took "instantaneous photographs" that the authors regarded as invading "the sacred precincts of private and domestic life."[30] According to Warren and Brandeis, these cameras weakened the public's right to privacy by "render[ing] it possible to take pictures surreptitiously."[31] In order to protect the public and prevent the "evil of the invasion of privacy," the scholars, using common law principles, developed a right to privacy that would protect the "privacy of the individual."[32] After evaluation different doctrines of law like trade secret and intellectual property, Warren and Brandeis, formed "the right to be let alone."[33] Warren and Brandeis excluded the right to privacy for those "who… have renounced the right to live their lives screened from public observation," since parts of society existed in the public eye.[34] In their opinion, candidates for public office, a person in a public position, or anyone who "makes their doings legitimate matters of public investigation," renounced the right of privacy.[35] The scholars concluded that the right to privacy was for "those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity," [36] and that "some things all men alike are entitled to keep from popular curiosity, whether in public life or not."[37]

[29] *See* SOLOVE, *supra* note 27, at 108 (examining the significance and influence article has with privacy law).
[30] Warren & Brandeis, *supra* note 28, at 195 (discussing the privacy issues specifically related to the development of the camera).
[31] Warren & Brandeis, *supra* note 28, at 211.
[32] Warren & Brandeis, *supra* note 28, at 195, 197 (developing the right to privacy as a public ideal by specifically protecting the privacy of each individual).
[33] Warren & Brandeis, *supra* note 28, at 195 (quoting Judge Cooley). Warren & Brandeis argued that "the right to life ha[d] come to mean the right to enjoy life," which they saw as "the right to be let alone." *Id.* at 193. They offered the right of privacy as "the next step which must be taken for the protection of the person, and for securing to the individual…the right 'to be let alone.'" *Id.* at 195.
[34] Warren & Brandeis, *supra* note 28, at 215 (noting that individuals under public observation have a lower expectation of privacy than an everyday person).
[35] Warren & Brandeis, *supra* note 28, at 215-16 (specifying that individuals in public office or in the constant eye of the public renounce the right of privacy to an extent).
[36] Warren & Brandeis, *supra* note 28, at 214.
[37] Warren & Brandeis, *supra* note 28, at 216.

B.Modern Privacy Law: Federal

Following the Warren and Brandeis article, numerous courts used the new "right to be let alone."[38] Specifically, Dean William Prosser, who served as a reporter for the Restatement (Second) of Torts, concluded "law of privacy comprises four distinct kinds of invasion of four different interests of the plaintiff…that each represents an interference with the right of the plaintiff…'to be let alone.'"[39] The four torts that Prosser identified were: (1) public disclosure of private facts,[40] (2) intrusion upon seclusion, [41] (3) appropriation of name or likeness, [42] and (4) false light.[43] Prosser's privacy torts became the most widely accepted model of American privacy interests

[38] *See* Benjamin E. Bratman, *Brandeis and Warren's "The Right to Privacy and the Birth of the Right to Privacy*," 69 TENN. L. REV. 623, 650 (2002) (discussing that *The Right to Privacy* "get[s] the credit for spawning a mini-revolution in the law, a revolution that eventually spread throughout the United States and throughout several fields of law to give us a wide-ranging right to privacy").

[39] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960); *see also* Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to your Digital Identity: A Tort for Recording and Disseminating an Individual's Image Over the Internet*, 49 SANTA CLARA L. REV. 313, 319 (2009).

[40] RESTATEMENT (SECOND) OF TORTS § 652D (1977) (stating "[o]ne who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public").

[41] RESTATEMENT (SECOND) OF TORTS § 652B (1977) (stating "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person").

[42] RESTATEMENT (SECOND) OF TORTS § 652C (1977) (stating "[o]ne who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for the invasion of privacy").

[43] RESTATEMENT (SECOND) OF TORTS § 652E (1977) (stating "[o]ne who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed").

and numerous states accepted these torts through the adoption of the Restatement (Second) of Torts.[44]

After Prosser's privacy torts, generally, a person who is photographed in public is essentially left without remedy.[45] Intrusions upon seclusion tort and public disclosure of private fact tort are the most suitable torts used to protect against being photographed without permission.[46] In *Gill v. Hearst Pub. Co.*,[47] the court determined that a violation of privacy under the intrusion upon seclusion tort only applied when the victim was in a private location.[48] A reporter secretly photographed a couple sitting in a park engaged in passionate embrace for an article reporting how love makes the world go round.[49] The couple, assuming they were alone in the park, wished to keep their affections private and was not pleased by the photograph and article in the Harper's Bazaar.[50] The couple sued under privacy torts.[51] However, mirroring Prosser's newsworthiness standard, the court found that when an individual exits their home, he waives his right of privacy.[52] *Gill v. Hearst* also interpreted the public disclosure of private facts torts to only apply when the matter released had no newsworthy value.[53] The *Gill* court noted that the right "to be let alone" is not an absolute right but must be balanced against the public

[44] *See* Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 897 (2006) (referencing Prosser's privacy torts as the accepted doctrine).
[45] *See* Blackman, *supra* note 39, at 321 (noting that individuals photographed in public are left without a legal remedy); *see, e.g.*, Dempsey v. Nat'l Enquirer, 702 F. Supp. 927, 931 (D. Me. 1988) (citing § 652B of Restatement (Second) of Torts).
[46] *See* Blackman, *supra* note 39, at 321 (providing a legal remedy for individuals who have unwarranted photographs taken of them).
[47] 253 P.2d 441 (Cal. 1953).
[48] *See id.* at 444-45 (concluding that unless in a private location, individual consents to being viewed by the public).
[49] *See id.* at 442 (discussing the facts prompting the lawsuit for invasion of their right of privacy).
[50] *See id.* (detailing how the couple wanted to keep their relationship out of the public eye).
[51] *See id.* (indicating the couple sued the Harper's Bazaar for a violation of their privacy).
[52] *See id.* at 446 (Carter, J., dissenting) (stating the holding of the majority opinion, specifically that anything anyone does outside of his own home is with consent to the publication thereof, because, under those circumstances he waives is right of privacy even though there is no news value in the event).
[53] *See Gill*, 253 P.2d at 443 (explaining how public disclosure of private facts torts only apply when the facts do not pertain to newsworthy information).

interest of obtaining news and information and upholding the constitutional guarantee of freedom of speech.[54]

In his dissent, Justice Carter rejected the majority's opinion and noted "there is no reason why the publisher need invade the privacy of John and Jane Doe for his purpose."[55] Quoting Warren and Justice Brandeis, Justice Carter proclaimed, "These private citizens, who desire to be left alone, should have and enjoy a right of privacy so long as they do nothing which can reasonably be said to have news value."[56]

Most privacy cases after *Gill* have supported the majority's approach in finding that privacy does not exist when an individual is in the public eye and is newsworthy.[57] After the decision in *Florida Star*,[58] judges relied on news editors to determine newsworthiness, recognizing that "a photograph with even the slightest social value is publishable without fear of liability."[59] The Supreme Court's decision also determined that the right to an individual's privacy in public is greatly weakened.[60]

Basically, under the current law, privacy in public is nonexistent.[61] With technology continuing to evolve, invading an individual's privacy has become easier and more invasive, in more ways than

---

[54] *See id.* at 443 (discussing the needed balance between the public's interest to obtain information with the right to freedom of speech).
[55] *But cf. id.* at 446 (Carter, J., dissenting).
[56] *Id.* at 447.
[57] *See e.g.*, Kapellas v. Kofman, 459 P.2d 912, 922-24 (Cal. 1969) (holding that children's privacy was not deeply intruded and the facts revealed were already public record). *But cf.* Daily Times Democrat v. Graham, 162 So.2d 474, 476-77 (Ala. 1964) (holding, in a case where a woman's underwear was photographed while an air jet in a fun-house blew up her skirt, that the photograph had "nothing of legitimate news value…[and] discloses nothing as to which the public is entitled to be informed").
[58] Florida Star v. B.J.F., 491 U.S. 524 (1989).
[59] Blackman, *supra* note 39, at 321.
[60] *See Florida Star*, 491 U.S. at 541 (holding that the publication of a rape victim's name does not violate her privacy because the information was available to the public, and finding that the government could only regulate what a newspaper could publish in order to "further a state interest of the highest order"). *But cf. id.* at 550-51 (White, J., dissenting) (noting that the majority accorded "too little weight to B.J.F.'s side of [the] equation, and too much to the other" and lamenting over the destruction of the tort of publication of private facts).
[61] *See* Blackman, *supra* note 39, at 324 (concluding that *Florida Star* court set the standard that privacy in public is nonexistent).

Warren or Justice Brandeis could have predicted.[62] Ahead of his time, Justice Carter outlined in his dissent in *Gill* four factors that could be used to define torts committed with future technologies.[63] These factors include: (1) people expect to be private when keeping to themselves, (2) intruding upon this solitude is offensive, (3) the intrusion is especially offensive when the image is reproduced, and (4) there is no news value in incidental occurrences of average people.[64] These factors may provide a foundation for future privacy torts in regards to technology and the invasion of privacy.[65]

C.Modern Privacy Law: Statewide

Currently, much of state law adopts the rights of publicity or the rights of privacy by statute.[66] These statutes cannot be sorted into "types" since most were enacted over a period of eighty years, unique to its place and time of origin: "a period during which the state of the law of the rights of privacy and publicity has grown and matured considerably".[67] Presenting a "crazy quilt of different responses," some states enacted statutes as a reaction to a refusal by the state supreme court to recognize privacy rights, while other states enacted statutes because as they watched other states enact appropriate legislation, they thought it was the sensible thing to do.[68]

New York was the first state to enact a statute in response to a public outcry when the New York Court of Appeals refused to recog-

---

[62] *See* Blackman, *supra* note 39, at 324 (indicating that lack of privacy in public "is even more troubling since technology has evolved to invade privacy in more surreptitious and invasive ways than Warren and Justice Brandeis could have ever imagined").

[63] *See* Blackman, *supra* note 39, at 324-25 (outlining Justice Carter's opinion).

[64] *See* Blackman, *supra* note 39, at 324-25 (outlining Justice Carter's opinion); *see also Gill*, 253 P.2d at 446-47 (Carter, J., dissenting) (providing his reasoning for his belief as to why the average person is entitled to privacy and his logic behind his dissent).

[65] *See* Blackman, *supra* note 39, at 325 (introducing a "new" tort as the right to personal digital identity).

[66] *See* J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY & PRIVACY, 1 RIGHTS OF PUBLICITY & PRIVACY § 6:6 (2d ed. 2014) (surveying state statutes in regards to the right of privacy and the right of publicity).

[67] *Id.* (indicating that each state statute is one of a kind and cannot be grouped by subspecies).

[68] *Id.* (distinguishing the different reasons states chose to enact right of privacy and right of publicity statutes).

nize a right to prevent the use one's picture in advertising without permission.[69] Other states enacted statutes after New York and even modeled their own statutes to be similar.[70] Over the decades, various state courts battled over whether a right of "privacy" existed.[71] This battle continued until more and more states began to enact privacy statutes.[72] States borrowed provisions and regulations from one another's statutes, making it hard to determine a place or origin for a particular provision.[73]

According to Justice McCarthy, each statute has its own particular advantages, drawbacks, and peculiarities.[74] For example, in the California statute, knowledge of use is required for the violation of the statutory right of a living person, but not for those of a deceased person.[75] Nebraska's statute is detailed but does not specify any remedies other than indicating that the plaintiff has a "legal remedy."[76] Massachusetts and Rhode Island each have two statutes, one directed at the commercial appropriation form of privacy, the other encompassing all four of Prosser's "four torts" of privacy.[77] What makes matters sometimes difficult though is that many state statutes include rights and remedies labeled "privacy," which permit damage recovery for the commercial value of one's identity.[78] This is a major

[69] *See id.* (explaining the reasons behind the New York statute).
[70] *See id.* (indicating that Utah and Virginia followed New York statutes).
[71] *See id.* (indicating that in the 1950's and'60's, Florida and Oklahoma enacted statues and states continued to enact statutes throughout the '70's and '80's like California).
[72] *See* MCCARTHY, *supra* note, 66 (presenting the history of the enactment of statutes from the 1950's to the 1980's).
[73] *See* MCCARTHY, *supra* note 66 (noting the challenges to tracing the points of origin for most of the statute provisions).
[74] *See* MCCARTHY, *supra* note 66 (describing the unique factors each statute contains).
[75] *See* MCCARTHY, *supra* note 66 (summarizing particular aspects of California's privacy statute).
[76] *See* MCCARTHY, *supra* note 66 (discussing that there are no specific remedies in Nebraska's privacy statute).
[77] *See* MCCARTHY, *supra* note 66 (comparing Massachusetts's and Rhode Island's privacy statutes).
[78] *See* J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY & PRIVACY, 1 RIGHTS OF PUBLICITY & PRIVACY § 6:7 (2d ed. 2014) (determining that many states have rights and remedies which permit damage recovery for the commercial value of an individual identity).

hallmark of the right of publicity.[79] Each statute is really "one of a kind" and is unable to be generally summarized into categories.[80] Therefore, with the release of Google Glass into society, each state may have different reaction and/or result to potential invasions of privacy.[81]

D.Google and Privacy

Because Google Glass is expected to be released spring 2014, and Google has actively assured the public that no facial recognition software will be included with Glass, there is very little information on whether Google Glass will actually infringe on the privacy of individuals.[82] The public is also unclear on Google's exact plans to incorporate privacy protections into the device now and for the future.[83] In May 2013, Representative Joe Barton, a co-chairman of the Bi-Partisan Privacy Caucus, wrote a letter to Google CEO Larry Page, expressing multiple concerns and questions about Google Glass about privacy protections in relation to the company.[84] Google is no stranger to privacy implications since the company dominates the Internet with its search engine (www.google.com), email server (Gmail), social media network (Google+), videos (YouTube), and blogs (Blogger).[85] Google not only has access to but the ability to

[79] *See id.* (noting the importance that damages can be collected for invasion of privacy of one's commercial identity).
[80] *See id*. (indicating that each statute is unique and unable to be generally categorized).
[81] *See id*. (inferring that with all the variances from state to state in privacy laws Google Glass might present privacy issues).
[82] *See* Letter from Rep. Joe Barton, *supra* note 23 (citing specific privacy concerns related to Glass); *see also* Hayley Tsukayama, *Wearable Tech Such as Google Glass, Galaxy Gear Raises Alarms for Privacy Advocates*, THE WASHINGTON POST (Sept. 30, 2013), *archived at* http://perma.cc/5N8E-DVCQ (discussing privacy concerns relating to new devices like Glass).
[83] *See id*. (noting how plans to ensure privacy with Glass are uncertain); *see also* Letter from Rep. Joe Barton, *supra* note 23 (seeking information on Google's plans to incorporate privacy protections).
[84] *See* Letter from Rep. Joe Barton, *supra* note 23 (listing some of the privacy concerns stated by the Congressional Bi-Partisan Privacy Caucus).
[85] *See* Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433, 1434-35 (2008) (noting that Google is estimated to account for nearly 60% of all Internet search queries in the United States - over six billion each month, which is more than double the next-largest search engine); *see also* Press Release, Nielsen Online, Nielsen Online Announces December U.S.

store vast amounts of personal information, creating a privacy problem that some call "the most difficult privacy [problem] in human history."[86] Privacy International, a leading advocate for human rights, in 2007 ranked Google's privacy practices as the worst compared to other service providers like Microsoft, Amazon, and eBay.[87] According to Privacy International, Google is "an endemic threat to privacy."[88]

In addition to Internet search and social networking, Google also enters the mapping services with Google Maps, by providing free detailed maps and satellite imagery to the public.[89] In May of 2007, Google introduced Street View, a new feature of Google Maps that allows users to obtain a ground level panoramic view of cities and areas across the country and around the world.[90] Google and Immersive Media conducted the digital survey of the cities by dispatching a fleet of unmarked vehicles equipped with concealed panoramic surveillance cameras.[91] When these Google cars take pictures, they upload the photographs onto the Internet that then "stitches" the images together into a virtual landscape that allows a person to view the street scene as if he/she were there.[92] Street View allows you to

Search Share Rankings (Jan. 14, 2009), *archived at* http://perma.cc/U9TV-R4SP (noting Google is the leading search provider in the United States in Dec. 2008).

[86] *See Inside the Googleplex*, ECONOMIST (Aug. 30, 2007), *archived at* http://perma.cc/CQ8-P59U (stating that Google has built the largest supercomputer where people can store their photos, emails, maps, contacts, social networks, and other private matters directly to a Google server).

[87] *See* Gemma Simpson, *Google Scores Lowest in Privacy Rankings*, ZDNET (June 12, 2007), *archived at* http://perma.cc/8QJD-QTNL (ranking Google the lowest privacy score to other service providers).

[88] *A Race to the Bottom: Privacy Ranking of Internet Service Companies*, PRIVACY INT'L (Mar. 26, 2012), *archived at* http://perma.cc/837C-TBG9.

[89] *See* Google Maps, GOOGLE, *archived at* http://perma.cc/2GCG-8HPH (providing users with a map service useful for directions).

[90] *See* Jesse Leavenworth, *Google Takes Man on the Street to New Places*, HOUSTON CHRONICLE (July 1, 2007), *archived at* http://perma.cc/F6ER-ULS3 (introducing Google Maps new feature of Street View which allows users to use ground level panoramic views of specific areas).

[91] *See id*. (explaining that the "maps capture all the glory and grime of the big city"); *see also Behind the Scenes Street View*, GOOGLE MAPS, *archived at* http://perma.cc/U67W-FXNW (discussing how Google acquired the panoramic city photos by sending unmarked cars with cameras attached to take pictures, sometimes unbeknownst to the public).

[92] *See* Leavenworth *supra* note 90 (describing how the Google cars take photos of desired location and then upload the photos to Google server).

zoom in and out, and spin around in a 360-degree camera angle to see precise details.[93] The pictures are clear and capture a plethora of images; not only of typical buildings but also in some images one can see people's faces, license plates, and cats sitting in windows.[94]

In 2010, it was discovered that Google was collecting information across the globe from unencrypted wireless networks.[95] Representative Joe Barton, similar to his involvement with questioning Google Glass, also partook in investigating whether the Google collection was accidental.[96] The FCC received complaints from privacy advocacy groups to investigate whether Google's practices violated federal communications law designed to prevent eavesdropping.[97] In March 2013, Google agreed to pay $7 million to settle charges with 38 states for the collection of data from unprotected Wi-Fi networks without permission.[98] Google also admitted that they did not adequately protect the privacy of consumers, which required them to quickly "tighten up" their systems to address the issue.[99] Lawmakers and advocates are still concerned whether the punishment is enough for Google not to revert back to "bad behavior" and to ensure that

[93] *See* Google Maps, GOOGLE, *archived at* http://perma.cc/2GCG-8HPH (offering the option of Street View which allows users a panoramic view of specific locations; users can also zoom in and out and spin the photo in a 360-degree camera angle).

[94] *See* Ryan Singel, *Request for Urban Street Sightings: Submit and Vote on the Best Urban Images Captured by New Google Maps Tool*, WIRED (May 30, 2007), *archived at* http://perma.cc/V7EJ-C893 (sharing instances where individual people, license plates, and cats can be seen in the photographs).

[95] *See* Amy Schatz & Amir Efrati, *FCC Investigating Google Data Collection*, WALL ST. JOURNAL (Nov. 11, 2010) *archived at* http://perma.cc/HLA8-A3SL (reporting on FCC's investigation of Google and their data collecting methods).

[96] *See id.* (indicating Representative Joe Barton's involvement with the Google investigation). The Representative suggested that Google's data collection was not accidental and that it was "something to look at." *Id.*

[97] *See id.* (reporting how the FCC received a complaint from Electronic Privacy Information Center urging the FCC to investigate Google's eavesdropping).

[98] *See* Brendan Sasso, *Google Pays $7 Million to Settle Wi-Fi Snooping Charges*, THE HILL, (Mar. 12, 2013), *archived at* http://perma.cc/KS6U-KE8W (discussing Google's settlement for eavesdropping on user's information without user knowledge).

[99] *See id.* (sharing information regarding Google's added privacy to their system in order to ensure better user privacy).

Google has a plan to prevent Google Glass from unintentionally collecting data about both users and non-users without consent.[100]

Google envisions a future where society embraces a larger role for machines and technology.[101] In 2010, Eric Schmidt, former Google CEO, stated:

> With your permission you give [Google] more information about you, about your friends, and [Google] can improve the quality of searches. [Google doesn't] need you to type at all. We know where you are. We know where you've been. We can more or less know what you're thinking about.[102]

E.History of Facial Recognition Software

Facial recognition technology is a division of Biometric technologies, the science of analyzing and measuring physiological data or "the identification of people by their unique features."[103] Biometrics uses an individual's distinguishable features and compares them with databases of other similar physiological characteristics.[104] Some of the more familiar systems are finger imaging, hand geometry, voice authentication, facial-recognition, retinal scanning, and iris scanning.[105]

---

[100] *See id.* (arguing that the seven million dollar settlement was not a harsh enough punishment to ensure that Google will not partake in illicit data collection again).
[101] *See* Derek Thompson, *Google's CEO: "The Laws are Written by Lobbyists,"* THE ATLANTIC (Oct. 1, 2010), *archived at* http://perma.cc/A3PN-3XFT (revealing Google's hopes of a future where society can embrace a larger role for machines and technology).
[102] *Id.*
[103] Susan McCoy, Case Comment, *O' Big Brother Where Art Thou?: The Constitutional Use of Facial-Recognition Technology*, 20 J. MARSHALL J. COMPUTER & INFO. L. 471, 473 (2002) (defining Biometric technologies).
[104] *See* Benjamin Pimentel & Benny Evangelista, *Tech vs. Terrorism/Airports Look to New Technologies to Beef Up Security*, SFGATE (Sept.17, 2001), *archived at* http://perma.cc/86XT-SRNN (describing how biometrics use an individual's distinct features and compares them with other characteristics).
[105] *See* Ellen Messmer, *Special Focus: Is Biometrics Ready To Bust Out?*, NETWORK WORLD (Oct. 7, 2002), *archived at* http://perma.cc/UU8H-EN3Y (outlining the different uses of biometrics). A computer scans the finger and reveals individual patterns much like an ink fingerprint. *Id.* The hand is placed on the flat surface of a scanner where ninety points of the hand are analyzed, such as the shape of the knuckle and dimensions of the finger. *Id*. Voiceprints are created with a

In the 1960s, facial recognition became semi-automated, where a system administrator had to locate key features in photographs.[106] Once key features were manually identified, the system would calculate the distances from the key facial features and compare the image to reference data.[107] In the 1980s, law enforcement agencies began to use the semi-automated technology.[108] Lakewood Division of the Los Angeles County Sheriff's Department used images of suspects captured in surveillance tapes and compared those images against mug shots found in their database in order to find matches.[109] By the late 1980s and early 1990s, facial recognition technology became fully automated with "Eigenface technology," allowing real time face recognition.[110] Basically, with real-time facial recognition, an image of an individual's face can be automatically recognized and matched to other images of that face in a database, without a system administrator manually locating the key features.[111] After the terrorist attacks on September 11, 2001, the United States federal government focused "[significant] enhanced attention" to biometric technologies.[112] By 2009, there were more than thirty public-

person's unique inflection and the individual highs and lows of their voice. *Id.* This biometric is useful in telephone-based procedures. *Id.* The system encodes specific measurements of distances between facial features through video surveillance. *Id*. The retina, similar to a fingerprint, is unique to each person and the scanning technology encodes its distinctive capillaries. *Id.* Iris pattern and color are mapped after a video image of the eye is taken. *Id.*

[106] *See* NSTC Subcomm., *Biometrics "Foundation Documents,"* NSTC 92, *archived at* http://perma.cc/UR7X-FHGD (explaining that in the 1960s facial recognition was semi-automated, whereas, by the 1990s, the technology advanced to become fully-automated).

[107] *See id.* (explaining how distinct features are identified and compared to already stored data).

[108] *See id*. at 67 (stating the Lakewood Division of the Los Angeles County Sheriff's Department began using a semi-automated facial recognition system).

[109] *See id.* (describing how Lakewood Division used the technology in order to identify suspects recorded on surveillance tapes).

[110] *See id*. (reporting that the discovery of using Eigenface techniques meant that reliable real time automated face recognition was possible).

[111] *See* Matthew A. Turk & Alex P. Pentland, *Face Recognition Using Eigenfaces*, VISION & MODELING GROUP, THE MEDIA LAB. MASS. INST. OF TECH. 587-90 (1991), *archived at* http://perma.cc/YD2Q-P5MR (describing how real-time face recognition works).

[112] NSTC, *Biometrics in Government Post 9/11*, 1 (2008) *archived at* http://perma.cc/3L5Q-D2HM (discussing the U.S. government's focus on biometics post 9/11).

ly available databases for facial recognition analysis.[113] Applications like Apple iPhoto, Sony's Picture Motion Browser, Windows Live Photo Gallery, Facebook "tag suggestions" and Google's Picasa all use facial recognition technology.[114]

III.Premise

Privacy torts protect individuals from the "mental pain and distress" inflicted by the broadcasting of personal details.[115] There are four different torts that encompass the common theme of the right "to be let alone":[116] (1) intrusion upon seclusion; (2) publicity given to private life; (3) publicity placing person in a false light; and (4) appropriation of name or likeness.[117]

A.Element of the Four Torts of Privacy

To recover under the first tort of privacy, intrusion upon seclusion, a plaintiff must show that a secret or private subject matter exists, that he has the right to keep that information secret, and that the information about the matter was discovered through unreasonable means.[118] "Intrusion" can refer to the physical invasion of a private place or "sensory intrusions such as… visual or photographic spying."[119] To be actionable, the intrusion must be "highly offensive

[113] *See id.* (indicating that more than thirty publicly available databases for facial recognition analysis existed by 2009).
[114] *See* Emily Schultz, *Comment to Activate Face Recognition Log On in Laptop*, TECHYV.COM, *archived at* http://perma.cc/626D-NFQG (presenting the variety of applications that currently use facial recognition technology).
[115] Warren & Brandeis, *supra* note 28, at 196 (discussing the purpose of privacy tort protections).
[116] Prosser, *supra* note 39, at 389 (stating that there are four torts that encompass the legal ramifications of the right "to be let alone").
[117] *See* Prosser, *supra* note 39, at 389 (dividing privacy torts into four distinct torts).
[118] *See* Matthew C. Keck, *Cookies, the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet*, 13 ALB. L.J. SCI. & TECH. 83, 106 (2002) (quoting Beaumont v. Brown, 237 N.W.2d 501, 505 (Mich. Ct. App. 1975) (listing the facts that a plaintiff must prove in order state a claim under the right to be free from intrusion into seclusion).
[119] *See* Clay Calvert & Justin Brown, *Video Voyeurism, Privacy, and the Internet: Exposing Peeping Toms In Cyberspace*, 18 CARDOZO ARTS & ENT. L.J. 469, 557 (2000) (quoting the leading case of Schulman v. Group W Prods. Inc., 955 P.2d 469, 489 (Cal. 1998)).

to a reasonable person."[120] Some scholars believe this is tort can protect victims of "video voyeurism," videotaping of people without their knowledge.[121]

Public disclosure of private facts tort provides an action for the "disclosure of private information that is (1) widely disseminated; (2) highly offensive to a reasonable person; and (3) not 'newsworthy' or 'of legitimate concern to the public.'"[122] In *Florida Star v. B.J.F.*,[123] the Supreme Court undermined the value of this tort when it found that a rape victim could not collect damages from a newspaper for publishing her name without her consent because the information was truthful and the newspaper obtained it from publicly available information.[124] Therefore, truthfulness and the extent to which information is publicly available or easy to find affect the "private nature" and legal action ability of disclosed information.[125] When the form of disclosure is a photograph or video, a plaintiff's

[120] *See* Keck, *supra* note 118, at 106 (defining how intrusion is actionable).
[121] *See* Calvert & Brown, supra note 119, at 557. Specifically, "video voyeurism" refers to the clandestine videotaping of people while in dressing rooms, tanning booths, and bathrooms. Id. If in a public place, it usually refers to "upskirting," the practice of placing small hidden cameras at low angles to film women's underwear. Id. This phenomenon is not limited to women. Id. at 479. According to Calvert and Brown, a plaintiff suing for video voyeurism that occurred in a dressing room can easily prove the elements of intrusion, "assuming a jury finds that [video voyeurism]…is highly offensive conduct." Id. at 557. There is evidence that public opinion may be swinging that way: in California, upskirting had become such a problem that the legislature amended its so-called Peeping Tom laws to impose liability specifically for this conduct. *See* David D. Kremenetsky, *Insatiable "Upskirt" Voyeurs Force California Lawmakers to Expand Privacy Protection in Public Places*, 31 MCGEORGE L. REV. 285, 288-90 (2000) (classifying "Peeping Tom" violations as a misdemeanor so long as occupant had a reasonable expectation of privacy).
[122] Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKELEY TECH. L.J. 1085, 1110 (2002).
[123] 491 U.S. 524 (1989).
[124] *See id.* at 541 (holding that victim could not collect damages from a newspaper who reported her identity); Andrew Jay Mcclurg, *Bringing Privacy Law Out of the Closet: A Tort Theory of Liability for Intrusions in Public Places*, 73 N.C. L. REV. 989, 1002 (1995) (citing the holding of Florida Star, 491 U.S. at 541). "[Public disclosure of private facts] is in reality an extension of defamation, . . . with the elimination of the defense of truth." Prosser, *supra* note 39, at 398.
[125] *See* Keck, *supra* note 118, at 107 (quoting U.S. Dep't of Justice v. Reports Comm., 489 U.S. 749, 763-6 (1989)).

identity must be revealed by the image in order for recovery.[126] Thus, the public disclosure tort has a catch-22 effect, because a piece of private information may be so widely disseminated by the disclosure as to become public, which will then bar the plaintiff's success.[127] Therefore, pictures or videos taken in a public space and released into the public domain may qualify the image as no longer private to begin with.[128]

False light, the third privacy tort, requires a successful claimant to show that the publicized information is both false and highly offensive, and that the defendant knew the information was untrue "or recklessly disregarded its truth or falsity."[129] With respect to Internet information privacy, this tort is inapplicable because where disclosure of personal private information like Social Security numbers or bank account numbers is involved, the information is almost always true and thus non-actionable.[130] If the information at issue

[126] *See* Calvert & Brown, *supra* note 119, at 497-98 (indicating that a plaintiff's identity must be revealed by the image in order for recovery).

[127] *See* Lin, *supra* note 122, at 1110-11 (discussing the catch-22 effect of this tort regarding the wrongful disclosure of private consumer databases, because "databases that are widely disseminated may be [part of the] public record . . . and not tortious . . . [but] conversely, databases that are . . . seemingly private . . . are often considered not to have been widely disseminated").

[128] *See* Mcclurg, *supra* note 124, at 993, 1008-09 (discussing Jackson v. Playboy Enterprises, 574 F. Supp. 10 (S.D. Ohio 1983)). In *Jackson*, three young men who were lost and asked a policewoman on the street for some directions. They were photographed without their consent while speaking with her. *Id*. at 1008. The policewoman later appeared as a nude model in Playboy magazine. *Id.* The photograph taken while she was speaking to the boys next to her nude photograph. *Id*. The court dismissed the plaintiffs' claims under all four privacy torts because "the photo was taken on a public sidewalk 'in plain view of the public eye.'" *Id.* at 1008-09. Also, Playboy's distribution of the photo without the boys' consent, was found that "'there is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public.'" *Jackson*, 574 F. Supp. at 13.

[129] Fred H. Cate, PRIVACY IN THE INFORMATION AGE 90 (1997) (noting that Prosser believed the false light tort is very closely related to common law defamation). "There has been a good deal of overlapping of defamation in the false light cases, and apparently either action, or both, will very often lie." Prosser, *supra* note 39, at 400.

[130] *See* Lin, *supra* note 122, at 1111-12 (explaining that false light tort will most likely be generally useless in a cyberspace context because certain personal and private pieces of information are almost always true). To be clear, this insight is only relevant to circumstances in which an individual's personal information is disclosed. *See also* David A. Myers, *Defamation and the Quiescent Anarchy of the*

were in the form of a photograph or image, however, the false light tort would only provide a legal recourse for someone whose image was "digitally manipulated to create a false impression about the person identified in the image."[131] As long as a photo stays "true" to a publicly available image, then the false light tort is inapplicable.[132]

Finally, commercial appropriation, the fourth privacy tort, requires a plaintiff to prove that the defendant used an aspect of the plaintiff's identity for his own advantage ("commercially or otherwise"), that the plaintiff did not consent to this use, and that the plaintiff suffered some resulting injury, in order to recover.[133] Often celebrities invoke commercial misappropriation when others profit from use of the celebrity's name or likenesses.[134] Although the tort does not require a plaintiff to be famous to recover, a plaintiff's celebrity status is extremely useful in proving both the measure of plaintiff's loss and that the defendant misappropriated the celebrity

Internet: A Case Study of Cyber Targeting, 110 PENN ST. L. REV. 667, 679-85 (2006) (describing two recent cases before the California Supreme Court involving Internet defamation). When a person's reputation is harmed via publications on the Internet, defamation law, either the common law tort or statutory form, comes into play. *Id.* at 679 (explaining defamation law will apply to cases involving reputational harm via Internet publications).

[131] Calvert & Brown, *supra* note 119, at 565 (describing the experience of an actress whose head was placed on the nude body of another woman and posted on a website as an example of a fact pattern that satisfies a false light tort claim). Moreover, like the tort of public disclosure, false light will not apply to a plaintiff unless she is identifiable in the image in dispute. *Id.* at 564 (establishing that a victim's identity must be recognizable in the posted image). However, "an identifiable facial representation" is not a "prerequisite to relief for appropriation." *Id.* at 563 (stating that Court's do not require an a identifiable facial image for the victim to receive relief). This principle comes from a New York case in which the appellate court found that a plaintiff was indeed identifiable in an image by her "hair, bone structure, body contours and stature and [her] posture." Cohen v. Herbal Concepts, Inc., 472 N.E.2d 307, 309 (1984).

[132] *See* Calvert & Brown, *supra* note 119, at 565 (noting that a photo must stay true to a publicly available image in order for false light to be inapplicable).

[133] *See* Hoffman v. Capital Cities/ABC, Inc., 33 F. Supp. 2d 867, 873 (C.D. Cal. 1999) (outlining the elements for a common law cause of action for misappropriation of a plaintiff's name or likeness); *see also* RESTATEMENT (SECOND) OF TORTS § 652C, *supra* note 42 (defining the tort of unlawful appropriation of another individual's name or likeness).

[134] *See In the Face of Danger: Facial Recognition and the Limits of Privacy Law*, 120 HARV. L. REV. 1870, 1880 (2007) (referencing how celebrities invoke their rights through commercial misappropriation).

image for personal commercial gain.[135] The doctrine of incidental use is an important consideration because it judges a "fleeting" use of likeness as non-actionable.[136]

B.The Significance of Facial Recognition Technology

Biometric data consists of "measurable, robust, and distinctive physical characteristic or person trait that can be used to identify an individual or verify the claimed identity of an individual."[137] Facial recognition software initially locates distinctive features on the face and the measurement of the facial features.[138] Each human face has approximately 80 nodal points and can be measured by the software.[139] For example, the software can measure the distance between the eyes, the width of the nose, the depth of eye sockets, the length of the jawline, etc.[140] These measurements are compiled to create an algorithm or biometric template of a person's face.[141] Then, the template is stored in a database and is compared to other template-stored images.[142] With the advancement of facial recognition technology, individuals, private companies, and government agencies are able to scan an image of a face and correlate the image with others stored.[143]

---

[135] *See* Keck, *supra* note 118, at 107 (determining that celebrity status helps prove celebrity plaintiff's losses). *See In the Face of Danger*, *supra* note 134, at 1879-80 (noting that a plaintiff does not need to be a celebrity but that celebrity status can be helpful in proving that the defendant misappropriated an image for commercial benefit).

[136] *See* Preston v. Martin Bregman Prods. Inc., 765 F. Supp. 116, 120 (S.D.N.Y. 1991) (indicating that fleeting uses of likeness are non-actionable).

[137] *See* John D. Woodward, Jr. et al., *Biometrics: A Look at Facial Recognition*, RAND, 1 (2003), *archived at* http://perma.cc/3GSR-SJ3T (defining biometric data).

[138] *See* Bonsor & Johnson, *supra* note 9 (describing how facial recognition software looks).

[139] *See* Bonsor & Johnson, *supra* note 9 (indicating the 80 nodal points on the face which can be measured by the software).

[140] *See* Bonsor & Johnson, *supra* note 9 (demonstrating how the software is capable of measuring the nodal points of the face: distance between eyes, width of nose, etc.).

[141] *See* Bryan Gardiner, *Engineers Test Highly Accurate Face Recognition*, WIRED (Mar. 24, 2008), *archived at* http://perma.cc/DTW-8MYS (explaining how the measurements of nodal points are used to create an algorithm, also known as a biometric template, of an individual face).

[142] *See id.* (describing how once an algorithm is created, it is then stored so that it can be used for future comparison with other templates).

[143] *See* Declan McCullagh, *Face-matching with Facebook Profiles: How It Was*

Biometric data is considered highly personal, individualized information.[144] In 2003, National Science and Technology Council ("NSTC") recognized the importance and private nature of biometric data and established a subcommittee designed to research biometric technology.[145] The subcommittee on Biometrics and Identity Management assists in coordinating development in federal biometrics.[146] In 2006, Biometrics and Identity Management responded to public concern regarding biometrics by urging companies to use privacy assessments whenever the use of biometric information occurs.[147] Biometrics and Identity Management's main concern with biometrics protection is the ability the technology has in accessing very private information.[148] Therefore, the United States government considers biometric data to be "sensitive personal information" and believes that standards and regulations should be followed in any implementation of technology that uses biometric data.[149]

The U.S. government classifies biometric data as "Personally Identifiable Information" ("PII").[150] PII is any information that can

Done, CNET (Aug. 4, 2011), *archived at* http://perma.cc/UT7X-B354 (stating that Facebook has a "vast database" of "wide-open profile photos" that can be used to identify you as you're walking down the street).

[144] *See* Natasha Singer, *Face Recognition Makes the Leap from Sci-Fi*, THE N.Y. TIMES (Nov. 12, 2011), *archived at* http://perma.cc/396H-6XKJ (referencing researchers who explain how facial recognition software could be used by marketers to infer personal information about random individuals on the street).

[145] *See* NSTC Subcommittee on Biometrics & Identity Management Room, BIOMETRICS.GOV, *archived at* http://perma.cc/LRT8-QUUP (outlining the purpose and mission of the new NSTC Subcommittee on Biometrics and Identity Management Room).

[146] *See id.* (explaining the objectives of Biometrics and Identity Management).

[147] *See* NSTC Subcommittee on Biometrics, *Privacy & Biometrics: Building a Conceptual Foundation*, BIOMETRICS.GOV, 35-39 (Sept. 15, 2006), *archived at* http://perma.cc/WQ4M-ATB8 (explaining the reasoning behind the importance of privacy regulation to biometric technology).

[148] *See* NSTC Subcommittee on Biometrics, *Biometrics Frequently Asked Questions*, BIOMETRICS.GOV, 1-4 (Sept. 7, 2006), *archived at* http://perma.cc/ZEB3-D7RZ (outlining the extensive amount of private data biometric technology could access).

[149] *Id.* at 21 (explaining the actions taken by government to ensure protection of biometrics data).

[150] *Rules and Policies – Protecting PII – Privacy Act*, U.S. GENERAL SERVICES ADMINISTRATION, *archived at* http://perma.cc/YNV8-PHR3 (defining biometric data as "Personally Identifiable Information").

be used to trace an individual's identity.[151] In 2006, Congress enacted legislation to protect PII.[152] 18 U.S.C. § 1028, criminalizes the use of PII to steal one's identity.[153] The statute weighs biometric data as equal to private information like one's name or Social Security number.[154] Even though biometric data is considered personal and as important to protect as Social Security numbers, biometric data fails to draw the same level of protection of the information on the Internet.[155] Because biometric data is classified as PII and is sensitive information, companies like Facebook who use biometric data to identify faces in photographs, should have given users' privacy greater respect before collecting biometric data to use for the network.[156]

Companies are turning to biometrics data in order to develop facial recognition software.[157] In June 2011, Facebook unveiled its "tag suggestions" feature, which allows users to upload a photograph to his or her Facebook page and then facial recognition software identifies the people in the pictures.[158] To some, the process sounds harmless, as Facebook is just trying to make it easier to tag pictures.[159] However, as users learn more and more about facial recognition software and the use of biometric data, users start to question privacy issues.[160]

---

[151] *See id.* (defining the purposes and uses of "Personally Identifiable Information").

[152] *See* 18 U.S.C. § 1028 (codifying the law on "fraud and related activity in connection with identification documents, authentication features and information").

[153] *See id.* § 1028(a)(1)-(8) (outlining the actions which constitute criminal violations).

[154] *See id.* § 1028(d)(7)(A)-(D) (qualifying biometric data as a means of identification in conjunction with name and Social Security number).

[155] *See* Carmen Aguado, Comment, *Facebook or Face Bank?*, 32 LOY. L.A. ENT. L. REV. 187, 195 (2012) (suggesting that biometric data fails to receive the same attention or protection as personal information such as Social Security numbers).

[156] *See id.* at 187 (arguing that Facebook is in violation of several privacy laws for lack of informing users their biometric data was being collected).

[157] *See id*. at 188 (offering Facebook as an example of a company that accumulates a database of biometric data for such uses as facial recognition).

[158] *See* Matt Hicks, *Making Photo Tagging Easier*, FACEBOOK (June 30, 2011), *archived at* http://perma.cc/FE88-LPLD (describing how "tag suggestions" works on Facebook).

[159] *See* Aguado, *supra* note 155, at 188 (discussing how "tag suggestions" on Facebook may sound harmless at first to users).

[160] *See* Aguado, *supra* note 155, at 188 (noting how some users may feel uneasy after learning how facial recognition technology works because it arguably constitutes an invasion of privacy).

IV. Analysis

A. What is the Problem?

Google Glass has presented a variety of privacy issues that concern lawmakers, bar managers, casino owners, coffee shops, and the general public.[161] However, the question is what specifically is there to worry about in a world where man is already heavily dependent on his smartphone?[162] According to the executive director of the Center of Digital Democracy, Jeffrey Chester, "The mobile device is a digital Trojan horse for privacy, since it enables marketers to know both our exact location and where we spend our time."[163] The Google Glass features are relatively modest, and do not stray far from the typical functions of an iPhone or other smartphone device: the ability to search the web, ask for directions, view maps, take photographs and videos, and access social media.[164] Philip Lee, a partner within the Privacy and Information Law Group at Field Fisher Waterhouse, sees a distinct difference though between any smartphone and Google Glass.[165] He states, "[B]ecause users wear and interact with Google Glass wherever they go, they will have a depth of relationship with their device that far exceeds any previous relationship between man and computer."[166] "Technology is a double-edged sword".[167] To some the dark side is much sharper than ever antici-

[161] *See* Gray, *supra* note 23 (listing industries having specific concerns regarding the use of Google Glass).
[162] *See* Sorg, *supra* note 5 (stating that many of the features of Google Glass such as texting, voice or video communication, and audio or video recording are currently cellphone features as well).
[163] Tsukayama, *supra* note 82 (noting that as a society "[w]e've entered a world where a consumer is identified, analyzed, tracked and can be targeted nearly 24-7").
[164] *See* Lee, *supra* note 2 (recognizing that although the capabilities are substantially similar, there are distinct differences between smartphones and wearable computers).
[165] *See* Lee, *supra* note 2 (comparing Google Glass with other smart technology, such as the iPhone, and acknowledging users interact with such devices).
[166] Lee, *supra* note 2.
[167] Dang, *supra* note 2 (introducing the idea of technology being a double-edge sword with both advantages and disadvantages to its development).

pated, while others are huge fans of Glass and feel "that privacy fears are overblown".[168]

While many believe wearable computers represent the next big shift in technology, others worry about the misuses of such technologies.[169] Since wearable technology is "always-on, always-worn and always connected, photo-snapping, video recording, social media-sharing," privacy issues are never-ending.[170] Some of these issues are of a more serious nature like the use of Glass for "crowd-sourced law enforcement surveillance", while others are "more mundane like forgetting to remove [the technology before] visiting the men's room".[171] The latter may seem unrealistic, however Allen Firstenberg, a technology consultant at the Google developers conference, admitted to an occasion of walking into the bathroom wearing his Glass without realizing it.[172] Privacy experts worry that "Glass can record video far less conspicuously than [any] handheld device" and occasions like Firstenberg's might become more frequent and fall into the hands of the wrong person.[173] Some reports have already concocted the most extreme scenarios for the "pair of glasses that can be worn by anyone and can record anything anytime."[174] Senior Editor Carlos Dang of Nanobyte, a website that reports, discusses, and blogs about all things technology, describes some ex-

[168] *See* Oreskovic, *supra* note 6 (noting the success of Google Glass despite privacy concerns by implementing features to traditional video cameras); *see also* Dang, *supra* note 2 (acknowledging that Glass may be cool but also establishes certain risks).

[169] *See* Oreskovic, *supra* note 6 (indicating the concern among casino operators regarding the use of Google Glass while gambling).

[170] Lee, *supra* note 2 (recognizing that the constant presence of wearable technology can raise a variety of privacy concerns).

[171] Lee, *supra* note 2 (listing the potential issues related to Google Glass technology).

[172] *See* Oreskovic, *supra* note 6 (sharing Firstenberg's anecdote of entering a bathroom while unaware that he was wearing Google Glass).

[173] Oreskovic, *supra* note 6 (explaining that Google Glass may be potentially misused because it is capable of recording video far less openly than traditional handheld recording devices).

[174] Dang, *supra* note 2 (outlining a variety of instances where Google Glass could be used in abusive ways). "Most of the conversations surrounding the glass is pertained to the territory of 'I wonder if the design's gonna be cool enough for me to wear outside.' But what is wrong with this picture? A pair of glasses that can be worn by anyone and can record anything anytime?" *Id.*

treme scenarios, pushing readers to question, "are [they] ready for 1984?"[175] Dang urges readers to be aware:

> With Google Glass, anyone can record every little aspect of their lives, which will include the lives of others as well. Not only does this infringe on the freedom of others, it poses a serious threat to personal security when you just can't ever know for sure if you are being secretly recorded or not.[176]

With the privacy concerns presented above, there is a large fan base that strongly feels that privacy fears are overblown, noting that Glass functions just like any other video camera with a tiny light that blinks on to let people know when it is recording.[177] Many individuals who have already started to adjust to life with Glass said they whip the device off in inappropriate situations all the time.[178] Many people, including Google Executive Chairman Eric Schmidt, believe that with the new technology come unspoken rules of etiquette.[179] During a talk at Harvard University's Kennedy School of Government, Schmidt noted, "Criticisms are inevitably from people who are afraid of change or who have not figured out that there will be an adaption of society to it."[180] Schmidt believes that of course there will be places where Glass will be deemed inappropriate but that so-

[175] *See* Dang, *supra* note 2 (describing some scenarios people may find with Google Glass). "Imagine this. You're on a date, and your date is wearing a Google Glass. And while you're talking, that person is secretly filming you and putting the video on the Internet for the world to see." *Id.* "A stalker on the prowl for a victim. He gets on a bus with you on it and records everyone inside. And out of all the people on the bus that day. He picks you. He then proceeds to follow you home and records your every move [sic] without you even knowing it." *Id.* "A terrorist is planning a bomb at an airport. He visits the place, records every single detail [sic] of the airport with his Google Glass, even the security badges and employees' face. With the footage at hand, he can now use it [to] figure a scheme to execute his plan." *Id.*

[176] Dang, *supra* note 2 (declaring that the age of privacy is dead).

[177] *See* Oreskovic, *supra* note 6 (indicating the technology contains a blinking light to alert people they are being recorded).

[178] *See* Oreskovic, *supra* note 6 (stating that users take the glasses off when encountered with inappropriate situations like gym locker room or work meetings).

[179] *See* Oreskovic, *supra* note 6 (acknowledging that there are certain places where Glass will not be appropriate but new rules of social etiquette will merge overtime).

[180] Oreskovic, *supra* note 6.

cial etiquette rules will evolve with the technology, just like previous technology.[181]

Other Glass enthusiasts believe Glass will help society "be in the moment," untethered from cellphones and neck cramps caused by the constant looking down at phones.[182] Another argument for the new wearable technology is that increased documentation by either photograph or video might not necessarily be bad, especially if it will help courts solve crimes and reach just outcomes.[183] Doctors across the country are excited for Glass because they believe it could transform the medical world and how doctors perform surgery.[184] Surgeons comment that the immediate advantage is that the doctor can constantly keep an eye on the patient, instead of looking up and down at an MRI or X-ray.[185] He also believes that, unlike before Glass, the device will enable surgeons to document critical moments during a procedure accurately and efficiently.[186] As stated before, technology is a double-edged sword and Google Glass shows great potential but also great concern.[187]

B.More Than Photograph and Video Privacy

Although most of the talk and worry of privacy has discussed the recording capabilities of the new Google Glass gadget, wearable technology has other noteworthy concerns: data collection.[188] Many privacy advocates do not focus on the videotaping but are more con-

[181] *See* Oreskovic, *supra* note 6 (noting that just like previous technological innovations such as mobile phones and wireless headsets society adapted to new rules of etiquette like not talking loudly on the bus and turning a ringer off in a meeting).
[182] *See* Sorg, *supra* note 5 (reporting the different opinions on Glass and its effect in society).
[183] *See* Atkinson, *supra* note 2 (outlining the broad issues Google Glass faces).
[184] *See Google Glass' Abilities Excite Surgeons*, *supra* note 6 (citing how surgeons have already used Google Glass in the operating room).
[185] *See Google Glass' Abilities Excite Surgeons*, *supra* note 6 (discussing the many advantages Google Glass brings to the medical field including the ability for surgeons to keep a constant eye on patients).
[186] *See Google Glass' Abilities Excite Surgeons*, *supra* note 6 (maintaining that Glass will provide doctors and surgeons all the necessary documentation they need during certain procedures like medical history and allergies).
[187] *See* Atkinson, *supra* note 2 (elucidating that Google glasses could lead to a slew of problems with detrimental results).
[188] *See* Oreskovic, *supra* note 6 (indicating that Glass data collection is more concerning than the recording capabilities).

cerned on the stream of data collected by the devices - everything from audio and video to a user's location data.[189] All connected devices including cell phones collect an enormous amount of information about individuals, and usually as consumers, we do not mind the collection.[190] Data collection simplifies, organizes, and enhances the lives of consumers.[191] However, as a community concerned about privacy, society tends to flinch as more and more networked devices collect more information, even though the reasoning is to provide services the consumer usually wants.[192] The massive amount of data Google Glass will be able to collect and the sensitive nature of some of this data creates a sense of uncertainty since many do not know how the collected information will be used.[193] Even though Glass is not very different from other technologies that collect data like cell phones or computers, because they are won on the face, advocates feel it is a horse of a different color.[194]

Privacy hawks are extremely concerned that consumers are unaware of the scale of data that will be collected by Glass and how that data will be used.[195] For example, users' data could end up being shared with firms that customize credit card offers based on users' shopping habits or insurance rates based on eating habits, all this information collected through wearable devices.[196] The Electronic Privacy Information Center sees an increase in Internet-connected devices "has the potential to exacerbate the power imbalance between consumers and the companies with which they conduct business…Information is power, and smart devices will provide much

[189] *See* Oreskovic, *supra* note 6 (citing Marc Rotenberg, the executive director of the Electronic Privacy Information Center).
[190] *See* Lee, *supra* note 2 (describing the amount of data smart technology collects).
[191] *See* Lee, *supra* note 2 (outlining the benefits data collection provides consumers).
[192] *See* Lee, *supra* note 2 (specifying the public's fears of certain data collection).
[193] *See* Tsukayama, *supra* note 82 (noting the Food and Drug Administration guidelines on medical apps make no mention of privacy and are unclear who should regulate health data pulled from wearable devices).
[194] *See* Oreskovic, *supra* note 6 (citing Ryan Calo, University of Washington law professor). "The face is a really intimate place and to have a piece of technology on it is unsettling." *Id.*
[195] *See* Tsukayama, *supra* note 82 (noting that consumers understand that certain data is being collected but would be alarmed by the amount of data expected to be collected by Glass and would be uncomfortable with the collection).
[196] *See* Tsukayama, *supra* note 82 (providing examples of potential uses of consumer data).

more information about consumers' behavior to companies than has been traditionally available."[197] What makes Glass unique, unlike most technology, is Google has patented "pay-per-gaze" advertising, which charges advertisers based on the Glass wearer's viewing habits of ads on billboards, in magazines and online.[198]

Some of the Glass-phobia may originate from Google's own track record on privacy.[199] As noted earlier, Google has had their fair share of privacy lawsuits. According to Marc Rotenberg, the executive director of the Electronic Privacy Information Center, "The fact that it's Google offering the service [Glass], as opposed to say Brookstone, raises privacy issues."[200] Recently, Google was facing a class-action over its scanning of emails sent and received by Gmail account users and by extension non-Gmail users they communicate with.[201] Google computers then analyze email content to bombard users with advertising.[202] How Google responded to this incident is even more concerning than the action itself. Google reacted to the issue by claiming, "Gmail users have 'no presumption of privacy' in regard to electronic communications.'"[203] It can only be assumed that Google's "presumption of privacy," or lack thereof would extend to Glass, which knows what you're viewing and for how long you are viewing it, whether it be medication, a new pair of shoes, etc.[204]

C.What's Next for Glass?

Although Google has announced that with the upcoming release of Google Glass will not include the feature of facial recognition software, it is hard not to think of a future without the feature.[205]

---

[197] Tsukayama, *supra* note 82 (citing statement by Electronic Privacy Information Center).
[198] *See* Sorg, *supra* note 5 (introducing Google's "pay-per-gaze" technology to be used by Glass for advertising purposes).
[199] *See* Oreskovic, *supra* note 6 (quantifying Google glasses and Google's ability to document everything an individual sees and does).
[200] Oreskovic, *supra* note 6.
[201] *See* Sorg, *supra* note 5 (acknowledging Google's class-action over its scanning of emails sent and received by Gmail users).
[202] *See* Sorg, *supra* note 5 (referencing details of the class-action lawsuit).
[203] Sorg, *supra* note 5 (noting Google's response to the class-action lawsuit).
[204] *See* Sorg, *supra* note 5 (extending Google's no privacy presumption to extend to the world of Google Glass).
[205] *See* Robertston, *supra* note 6 (asserting that the software that is essential to making Google glass what it is has a permanent place in the foreseeable future).

Even if Glass refuses to include the software, applications have already been developed that use facial recognition to identify strangers.[206] The app NameTag, can match people's faces with photos from social media accounts or other online sources.[207] The app is already attracting many responses from the public including Senator Al Franken who stated in a letter to NameTag, "Unlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a distance, without the knowledge or consent of the person being identified," he wrote.[208] "Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere — on a lamppost across the street, attached to an unmanned aerial vehicle, or, now, integrated into the eyewear of a stranger."[209]

Yes, Google has sanctioned an across-the board ban on facial recognition and NameTag is not an officially sanctioned Google Glass app, however, in its beta form, NameTag claims it can "spot a face using Google Glass" camera, send it wirelessly to a server, compare it to millions of records and in seconds return a march complete with a name, additional photos and social media profiles."[210] NameTag argues that the app will better society by making online dating and offline social interactions much safer.[211] Creator Kevin Alan Tussy also notes that the app will give society a far better understanding of all people and make it easier to meet interesting new people.[212] In fact, the potential slogan for the NameTag app is "NameTag can make the big, anonymous world we live in as friendly as a small town."[213]

---

[206] *See* Robertson, *supra* note 6 (citing Senator Al Franken's response to facial recognition application for Google Glass).
[207] *See* Robertson, *supra* note 6 (describing features of NameTag application which could help identify strangers).
[208] *See* Robertson, *supra* note 6 (explaining how the software behind facial recognition actually functions).
[209] *See* Robertson, *supra* note 6 (citing Senator Al Franken's letter to NameTag demanding that NameTag hold off on the release of their application).
[210] *See* Robertson, *supra* note 6 (referencing a description of NameTag and how it works).
[211] *See* Robertson, *supra* note 6 (noting NameTag's opinion of how the app can make the world a better place).
[212] *See* Robertson, *supra* note 6 (referencing Tussy's opinion on his new invention as a way to make society safer because it will allow users to know those around them before having to interact with them).
[213] *See* Robertson, *supra* note 6 (citing NameTag app's potential slogan).

Other Google Glass applications exist that could be used to help people suffering from autism or who may have some type of visual impairment.[214] The SHORE application enables Google Glass to detect human emotions by scanning facial expressions.[215] The application can also recognize gender and age by analyzing the facial expressions.[216] While the heated debate continues on whether Google Glass is a threat to privacy, some scientists are discussing the new frontiers apps like SHORE will conquer.[217] Individuals with autism sometimes have a difficult time interpreting the expressions of others they are interacting with.[218] With the SHORE app, emotions of the other person will appear in the Google Glass display field, notifying the Glass user, and helping the user interpret emotions.[219] SHORE also has an audio description feature, which will assist the visually impaired.[220] Glass will give the visually impaired user oral details about a person they are interacting with.[221] Applications like SHORE may ease the public's fear of facial recognition software since it could provide many users important benefits.[222]

Truly, it is only a matter of time before society may need to accept the improvement of technology and accept the use of facial recognition software.[223] Google already does a lot with reverse im-

[214] *See* Thekkethil, *supra* note 22 (introducing SHORE, a face detection system believed to help people with autism or people who are visually impaired).
[215] *See* Thekkethil, *supra* note 22 (discussing the SHORE application and its capabilities).
[216] *See* Thekkethil, *supra* note 22 (noting other SHORE special features).
[217] *See* Thekkethil, *supra* note 22 (referencing the privacy discussions related to Google Glass and opining how applications like SHORE may provide huge benefits to users).
[218] *See* Thekkethil, *supra* note 22 (noting how autistic individuals sometimes have trouble reading and understanding human emotions).
[219] *See* Thekkethil, *supra* note 22 (describing how the SHORE human emotion feature works with Google Glass).
[220] *See* Thekkethil, *supra* note 22 (introducing the audio description feature for Google Glass users who are visually impaired).
[221] *See* Thekkethil, *supra* note 22 (describing how the SHORE audio description feature works).
[222] *See* Thekkethil, *supra* note 22 (recognizing that wearable technology is the cause of much debate; however, programs like SHORE provide certain advantages).
[223] *See* Jose Pagliery, *FBI Launces a Face Recognition System*, CNN (Sept. 14, 2014), *archived at* http://perma.cc/C6HH-KBFF (inferring that society must adapt to and accept the use of facial recognition software because it's use is becoming more widespread).

age searching and identifying faces in photos, thus, it should not be hard to imagine Google using facial recognition software and comparing faces of people you meet to publically available information provided by social networks.[224] Therefore, Google may have forbidden facial recognition software use through the first generation of Glass but it can only be expected for the future of Glass.[225]

Overtime, society has proven to be moldable when it comes to accepting new means of technology.[226] Google Glass and facial recognition technology have a range of positive usable options like doctors using the technology during surgeries to perfect the operations and teach others about it.[227] Google will probably relax its privacy restrictions to make facial recognition applications available and society will adjust to the advancement.[228]

D.Solutions to Privacy Issues

As Congressman Barton noted in his letter to Google CEO, Larry Page in May 2013, "It will only be a matter of time until you'll be able to aim the lends of your device at his or her face, and using face recognition technology get the individual's address, work history, marital status, measurements, and hobbies."[229] So what can be done to prepare for the inevitable use of Google Glass?

---

[224] *See* Etherington, *supra* note 6 (describing new facial recognition application that will be released with select number of Google Glass products and society's reaction to the potential feature).

[225] *See* Etherington, *supra* note 6 (discussing how Google is forbidding certain kinds of facial recognition software).

[226] *See* Etherington, *supra* note 6 (recognizing that society has proven itself to be quite changeable on the definition of what is and isn't acceptable when it comes to how much information people decide to share). "[T]here does seem to be a general level of anxiety around the idea of Google Glass and facial recognition. But over time we've proven ourselves to be quite changeable on the definition of what is and isn't acceptable when it comes to how much information we share with others via the web, and facial recognition could become something that people grow more comfortable with time." *Id.*

[227] *See Google Glass' Abilities Excite Surgeons*, *supra* note 6 (explaining some uses Google Glass has within the medical field).

[228] *See* Oreskovic, *supra* note 6 (discussing social etiquette adjustments that society will make when the new technology is introduced).

[229] *See* Letter from Rep. Joe Barton, *supra* note 23 (quoting *Wall Street Journal*).

One response to Glass is to ban it from certain places.[230] When instructing Glass to the nearest coffee shop, one may also need to qualify the coffee shop as one that allows the technology inside.[231] Cocoa Cinnamon, a small coffee shop in Durham, took a pre-emptive strike against Glass.[232] A sign on the door prohibits people from wearing the device on the premises, making Glass as malicious as smoking and guns.[233] Companies can even order their anti-Glass signs online.[234] Casino operator Caesar's Entertainment recently announced that Glass is not permitted while gambling or when in showrooms.[235] In March 2013, Seattle's Five Point Café became the first bar to ban Glass.[236]

Public places are not the only area where Glass is being banned. Glassing and driving is also an area where Glass may be banned in order to prevent distractions while driving.[237] Some eight U.S. states are considering regulation of Google Glass while driving because law enforcement and other groups are concerned that drivers wearing the devices will pay more attention to their email than the road, ultimately causing serious accidents.[238] Although lawmakers are only considering the issue, Google is not going down without a fight and have been contacting state officials to reconsider a driving

[230] *See* Gray, *supra* note 23 (listing the establishments that have chosen to ban Google Glass including restaurants, bars, casinos, theaters, concert venues, etc.).
[231] *See* Sorg, *supra* note 5 (noting how certain coffee shops have banned the wearing of Glass).
[232] *See* Sorg, *supra* note 5 (using Cocoa Cinnamon as one example of businesses that are choosing to ban Google Glass from the premise even before the technology is publically released).
[233] *See* Sorg, *supra* note 5 (noting that Cocoa Cinnamon also prohibits smoking and guns on the premise).
[234] *See* Sorg, *supra* note 5 (citing that anti-Glass sings can be purchased at stopthecyborgs.org).
[235] *See* Oreskovic, *supra* note 6 (indicating that Glass is banned in showrooms and when gambling but can be worn in other areas of the casino).
[236] *See* Oreskovic, *supra* note 6 (referencing the bar as the first to ban Glass). "Respect our customers privacy as we'd expect them to respect yours," says a statement on Five Point Café's website. *Id.*
[237] *See* Oreskovic, *supra* note 6 (discussing the California Highway Patrol policies). There is no law that explicitly forbids a driver from wearing Glass while driving in the state [of California]. But according to Officer Elon Steers, if a driver appears to be distracted as a result of the device, an officer can take enforcement action. *Id.*
[238] *See* Levine, *supra* note 23 (outlining the concern that drivers wearing Google Glass will pay less attention to the road).

ban.[239] Since the technology could be used as a GPS, Google does not want the overall ban but advises individuals using Glass to abide by state laws that limit use of mobile devices while driving.[240] On the other hand, if a driver is pulled over because they appear to be wearing the technology, it will always be extremely difficult to prove whether Google Glass had been operating at the time.[241] Therefore, a suggested easy fix is to just altogether ban the technology while driving.[242]

Google Glass, on its own, will test the waters between man and computer, making one more connected than ever before.[243] Then, when you throw in the likely short-term additions such as facial recognition capabilities, it becomes easy to understand why Glass is heralded as "The Next Big Thing," pushing privacy issues to the next level.[244] Since Google Glass is the headline product and it is known that Glass will collect massive amounts of data from its users, society wants quick solutions to the privacy woes. As a result, privacy professionals may turn to the go-to solution regarding most privacy issues: strengthened consent requirements and standards.[245] If explicit consent is required to justify the massive collection of individual's personal information, including relationship status, employment status, likes, and dislikes, then one would think that there would be no problem.[246] Unfortunately, although consent requirements may be the easy way to handle privacy concerns regarding

[239] *See* Levine, *supra* note 23 (noting that Google has deployed lobbyists to persuade elected officials in some states that it is not necessary to restrict the use of Google Glass behind the wheel).
[240] *See* Levine, *supra* note 23 (referencing Google's plea not to ban the technology but that drivers should use the technology with care).
[241] *See* Levine, *supra* note 23 (noting an instance where a San Diego woman's traffic ticket for wearing Google Glass behind the wheel was dismissed because there was no proof the device was operating at the time).
[242] *See* Levine, *supra* note 23 (referencing the opinion of Maryland House of Delegates member Benjamin Kramer who believes it will be too hard for law enforcement to determine if Glass was being operated while driving). Kramer's presented solution is "The way to get around it is to just prohibit [Glass] altogether." *Id.*
[243] *See* Lee, *supra* note 2 (summarizing the launch of the Internet-connected Google Glass).
[244] *See* Lee, *supra* note 2 (describing Google Glass as "The Next Big Thing" because of the innovative features Google Glass will probably include).
[245] *See* Lee, *supra* note 2 (referring to consent notices as a knee-jerk reaction to dealing with massive data collection).
[246] *See* Lee, *supra* note 2 (questioning whether explicit consent is the way to justify the vast collection of personal information).

Google Glass, explicit consent tends to be lazy and not a reliable solution to address the privacy problem at hand.[247]

Explicit consent as a cure-all for all extreme data collection processes "will drive poor compliance," that in effect, "delivers little real protection for individuals."[248] According to Phil Lee, a partner in the Privacy and Information Law Group at Field Fisher Waterhouse LLP, "when [one] build[s] compliance around explicit consent notices, it's inevitable that those notices will become longer, all-inclusive, heavily caveated and designed to guard against risk."[249] Because consent notices deal with legal issues, and not design issues, product designers like those involved with Google Glass, construct their inventions with little thought to privacy.[250] In the end, these designers know they can slap on to their product a detailed consent notice for the consumer and thus, the consumer is left with a "take it or leave it" scheme on installation or first use, similar to terms of service.[251] Take it or leave propositions tend to confuse consumers, no matter how well they are explained.[252] As technology becomes more complex and invasive to privacy, consent notices become more convoluted and users may simply ignore any notice or not completely understand what they are consenting to.[253] Therefore, what can be done in regards to privacy issues and major data collection?

Privacy gurus need to devise a better solution than consent notices. Ideally, privacy professionals should try to strike a balance between the legitimate privacy expectations each individual wants with the legitimate business interests companies have to collect and

---

[247] *See* Lee, *supra* note 2 (referring to consent notices as lazy). "Sure, in some circumstances [consent] may be warranted, but to look to explicit consent as some kind of data collection panacea will drive poor compliance that delivers little real protection for individuals." *Id.*

[248] *See* Lee, *supra* note 2 (describing the danger of relying solely on explicit consent as a solution for data collection processes).

[249] Lee, *supra* note 2.

[250] *See* Lee, *supra* note 2 (discussing how consent notices are seen as a legal issue, not a design issue).

[251] *See* Lee, *supra* note 2 (noting how designers build products with little thought to privacy, because in the end, they know they can "simply 'bolt on' a detailed consent notice" to the product).

[252] *See* Lee, *supra* note 2 (explaining that take it or leave it propositions tend to confuse consumers).

[253] *See* Lee, *supra* note 2 (providing an example of how consumers tend to ignore consent notices when they become too complex through consumers disregard to online cookie consent).

utilize user data.[254] A solution is needed where innovative products and services can still be produced but remain responsive to user privacy.[255] Designers should consider and build privacy functionality into their product from the onset, instead of waiting for the issues to arise after its release.[256]

Finally, the last potential solution that may be considered for privacy concerns and Google Glass is the concept of online "personal space."[257] As stated before, society has developed an understanding of personal boundaries through social etiquette.[258] A similar concept could be conceived for the online world.[259] Promoting an understanding of an invisible boundary where each individual respects the personal online space of others is possible for the online world.[260] Furthermore, with respect to one's online personal space, designers could create their inventions with a "privacy by design" method.[261] They would need to consider the privacy problems upfront in a hope to avoid surprising users later with products that could breach one's

[254] *See* Lee, *supra* note 2 (examining how it is incumbent for privacy professionals to strike a balance between individual's expectation of privacy and businesses needs to collect data).
[255] *See* Lee, *supra* note 2 (introducing the idea where products are still designed but with a concern for user privacy throughout the design process).
[256] *See* Lee, *supra* note 2 (adopting the concept of "Privacy by Design" development where designers build products with the consideration of privacy functionality and their products from the outset).
[257] *See* Lee, *supra* note 2 (presenting a potential solution to massive data collection through the idea of online personal space).
[258] *See* Oreskovic, *supra* note 6 (describing how social etiquette has changed with the development of new technologies).
[259] *See* Lee, *supra* note 2 (introducing the concept of an online personal space); *see also* Oreskovic, *supra* note 6 (noting that just like previous technological innovations, such as mobile phones and wireless headsets, society has adapted to new rules of etiquette).
[260] *See* Lee, *supra* note 2 (developing parallels between physical boundaries and online boundaries). "In the physical world, whether through the rules of social etiquette, an individual's body language or some other indicator, we implicitly understand that there is an invisible boundary we must respect when standing in close physical proximity to another person. A similar concept could be conceived for the online world…." *Id.*
[261] *See* Lee, *supra* note 2 (referencing Privacy by Design methodologies and the California attorney general's guidance on mobile privacy as a way to deal with large data collection).

privacy expectation.[262] It is necessary for society, government, and privacy professionals to continue the conversations to find a workable solution to integrate innovative technological advancements with important privacy concerns. [263]

V. Conclusion

With the anticipation of Google Glass this upcoming year, privacy issues regarding the technology become more imminent and pressing. With legislation and rules already in place to ban the technology, society's response to the up-and-coming wearable devices will trigger a response of a "coolness" factor coupled with a "creepy" factor. Society will change with the technology and as features like facial recognition software develop. Maybe the reality will be more like George Orwell's *1984*, where one cannot enter the public without the wonderment of being recorded, or maybe society will develop like it has in the past, with certain social etiquette responses, regulations, and responsibilities. Only time will tell.

[262] *See* Lee, *supra* note 2 (recommending the Privacy by Design methodology so that businesses can avoid surprising consumers by collecting data about them that they would not expect to be collected).
[263] *See* Lee, *supra* note 2 (stating "[w]hatever the solution is, we're entering a brave new world; it demands some brave new thinking").