COMMENTS

Intrusion Upon Seclusion and Data Privacy: Shifting the Analysis for a New Problem

Hannah Harris*

I. INTRODUCTION

"Who has seen an advertisement that has convinced you that your microphone is listening to your conversations?"[1]

That is the question a professor of media design at the New School in Manhattan asks to begin the eye-opening Netflix documentary "The Great Hack."[2] The documentary uncovers how Cambridge Analytica[3]

* © 2021 Hannah Harris. Managing Editor, Volume 23, *Tulane Journal of Technology and Intellectual Property*. J.D. candidate 2021, Tulane University Law School; B.A. 2016, Communications, University of Louisiana at Monroe. The author would like to thank her family and friends for their continuous support and encouragement, and her fellow *Tulane Journal of Technology and Intellectual Property* members for their hard work and dedication.

1. THE GREAT HACK (Netflix 2019).
2. *Id.*
3. *See Cambridge Analytica*, WIKIPEDIA, http://en.wikipedia.org/wiki/Cambridge_Analytica (last visited Oct. 11, 2019) (explaining that "Cambridge Analytica was a British political consulting firm which combined data mining, data brokerage, and data analysis with strategic communication during the electoral processes . . . . The company closed operations in 2018 in the course of the Facebook-Cambridge Analytica data scandal . . . .").

used "data tracking, harvesting, and targeting" to help Donald Trump win the 2016 presidential election.[4] It is widely known that Cambridge Analytica did this by collecting thousands of data points on every adult in the United States to build detailed personality profiles.[5] The company then used these profiles to target undecided voters with the most persuasive Trumpian advertisements: a strategy that seemingly put Donald Trump in the White House.[6] While the film certainly delves into the election and the chaos that surrounded it, the crux of the documentary is much bigger than politics.[7] And while our current political climate may seem scary and unsettling, the privacy problem highlighted in this documentary is the real "dystopian horror movie for our times."[8]

Part I of this Comment delves deeper into the data threat to information privacy by providing clear explanations of technical terms and modern examples. Part II discusses the history of modern privacy law and specifically the tort of intrusion upon seclusion. Part III examines two potential hurdles in applying the tort of intrusion upon seclusion to modern data privacy cases: the secrecy requirement and the highly offensive requirement. Finally, Part IV argues that it is time for courts to stop applying the intrusion upon seclusion tort to data collection and instead apply it to data aggregation and observation. By doing this, plaintiffs will likely be able to reach the high thresholds of the secrecy and highly offensive requirements needed for a valid intrusion upon seclusion claim.

While what Cambridge Analytica did may sound extreme and outrageous, such is perhaps the new normal in our new big data driven world.[9] Today, companies can "combine diverse digital datasets and then use statistics and other data mining techniques to extract from them both

4. Emily Dreyfuss, *Netflix's The Great Hack Brings Our Data Nightmare to Life*, WIRED (July 24, 2019, 4:53 PM), http://www.wired.com/story/the-great-hack-documentary/.

5. *Facebook-Cambridge Analytica Data Scandal*, WIKIPEDIA, http://en.wikipedia.org/wiki/Facebook–Cambridge_Analytica_data_scandal (last visited Oct. 10, 2019) It is estimated that Cambridge Analytica had access to over 70 million Facebook profiles. *Id.; see also* Rebecca Davis, *A New Documentary and a Local Children's Book Tackle Big Data's Dangers From Different Angles*, DAILY MAVERICK (July 30, 2019), http://www.dailymaverick.co.za/article/2019-07-30-a-new-documentary-and-a-local-childrens-book-tackle-big-datas-dangers-from-different-angles/.

6. *Facebook-Cambridge Analytica Data Scandal*, *supra* note 5.

7. *See* THE GREAT HACK, *supra* note 1; *see also* Dreyfuss, *supra* note 4 (explaining that the documentary "uses the scandal as a framework to illustrate the data mining structures and algorithms that are undermining individual liberty and democratic society, one Facebook like and meme at a time.").

8. Dreyfuss, *supra* note 4.

9. Steve Lohr, *The Age of Big Data*, N.Y. TIMES (Feb. 12, 2012), http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html.

hidden information and surprising correlations."[10] The real threat is not the mere collection of data, but the ability of companies to aggregate that data into intimate individualized profiles.

Despite the dangers that may stem from this transformative process, the data aggregation and observation industry remains wholly unregulated.[11] In fact, "there is no comprehensive information privacy law in the [United States] regulating private sector collection and use of personal data . . . ."[12] Additionally, "neither the Constitution nor a general set of laws regulates commercial companies' overall data practices as they affect privacy."[13]

For these reasons, this Comment is not a roadmap in applying the privacy tort of intrusion upon seclusion to data collection. Instead, this Comment argues that courts should stop applying the intrusion tort to data collection altogether and instead apply the tort to the much more dangerous practice of data aggregation and observation.

II. DATAVEILLANCE AND THE THREAT TO PRIVACY

In recent years, data has become the most valuable resource on earth.[14] The underlying reason for this is because "[a]ll of [our] interactions: [our] credit card swipes, web searches, locations, likes . . . [are] all collected in real time and attached to [our] identit[ies] giving any buyer access to [our] emotional pulse."[15] These little traces of our lives are then being mined into a trillion dollar a year industry, making human beings the commodity.[16]

Why data is valuable can be summed up in two words: targeted advertising.[17] Targeted advertising uses data points to personalize

---

10. Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74, 74 (2013).

11. Ira S. Rubinstein et al., *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 273 (2008).

12. *Id.*

13. *Id.*

14. *The World's Most Valuable Resource Is No Longer Oil, But Data*, THE ECONOMIST (May 6, 2017), http://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data ("A [new] commodity spawns a lucrative, fast-growing industry . . . . A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era.").

15. THE GREAT HACK, *supra* note 1.

16. *Id.*

17. *See* Johanna Rivard, *Why Your Marketing Needs to be Data-Driven*, MKTG. INSIDER GRP. (Apr. 25, 2019), http://marketinginsidergroup.com/content-marketing/marketing-needs-data-

advertisements for consumers based on the consumer's preferences.[18] This practice, also referred to as database marketing, has in recent years formed a multi-billion dollar industry.[19] Today, "[a]lmost every major retailer, from grocery store chains to investment banks to the U.S. Postal Service, has a 'predictive analytics' department devoted to understanding not just consumers' shopping habits but also their personal habits, so as to more efficiently market to them."[20]

Targeted marketing and data observation operate on the raw data provided by an expansive supply of private and public records.[21] State public records alone cover full names, birthdays, places of birth, parent's names, mother's maiden names, marriages, divorces, addresses, professional licenses, traffic citation records, voting records, and much more.[22] Just as an example as to how deep these public records can reach, "[i]f a person is a public employee, many personal details are released to the public by way of personnel records, including home address, phone number, [social security number], salary, sick leave, and sometimes even [e-mail] messages."[23]

Prior to the dawn of the information age, these public records were only available at the individual offices that harbored them.[24] If a person wanted to garner access to a public employee's personal information, they would need to go directly to the office of the employee and make a request for such information.[25] Now, as institutions have moved their record systems onto the Internet and computerized programs, such records can increasingly be found online.[26] In fact, there are now more than 150

---

driven/ (explaining that "[t]he digital age has brought about widened reach, but pinpoint targeting accuracy.").

18. *Id.* (explaining that "[i]f you know your target user's behavior, goals, pain points, and challenges, you can develop marketing campaigns that cater to their specific needs.").

19. Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 16, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html (explaining that database marketing is a multi-billion dollar industry).

20. Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?pagewan%20ted=all.

21. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 127-28 (N.Y. Univ. Press 2004).

22. *Id.*

23. *Id.* at 128.

24. *Id.* at 131.

25. *Id.*

26. *Id.*

companies providing access to public records online.[27] Thus, instead of having to go to each individual institution to collect such records, companies can now scour millions of public records with the click of a mouse.[28]

The scale of intrusiveness and offensiveness regarding the manner in which companies use this data certainly varies. The music streaming platform Spotify is one company on the less intrusive end.[29] Spotify provides a unique experience to each user.[30] This experience includes personalized playlists based off of previously listened to songs and new music suggestions based on the user's tastes.[31] To do this, Spotify monitors "not only what users listen to, but how they interact with each song."[32] That is, if a user moves onto the next track within the first thirty seconds of the song, Spotify will not use that song when creating a personalized playlist.[33] However, if a user listens to a song in its entirety, Spotify will likely add that particular song and similar songs to the personalized playlists.[34]

On the far more intrusive side, health-care companies are now using readily available data from "data brokers, pharmacies, and social media" to uncover information about an individual's health.[35] These companies use data points ranging anywhere from age and race to shopping habits, cat ownership, and participation in sweepstakes to predict information about individuals.[36] According to Roger Smith, a senior vice president at Acurian,[37] companies can now determine, "based on your credit card history, and whether you drive an American automobile and several other

---

27. *Id.*
28. *Id.*
29. *See Spotify*, WIKIPEDIA, http://en.wikipedia.org/wiki/Spotify (last visited Oct. 11, 2019).
30. *Id.*
31. Ashley DiFranza, *Spotify: Big Data Shows Big Results*, NE. UNIV. BLOG (Oct. 4, 2019), http://www.northeastern.edu/graduate/blog/spotify-big-data/.
32. *Id.*
33. *Id.*
34. *Id.*
35. Joseph Walker, *Data Mining to Recruit Sick People*, WALL ST. J. (Dec. 17, 2013, 4:32 PM), http://www.wsj.com/articles/data-mining-to-recruit-sick-people-1387237952.
36. *Id.*
37. *Pharmaceutical Product Development*, WIKIPEDIA, http://en.wikipedia.org/wiki/Pharmaceutical_Product_Development (last visited Dec. 2, 2019) (explaining that Acurian is a unit of Pharmaceutical Product Development, a "global contract research organization providing comprehensive integrated drug development, laboratory and lifestyle management services.").

lifestyle factors . . . whether or not you have [the disease they are researching]."[38]

There are federal statutes[39] in place that prevent insurers and health-care providers from "sharing or selling personally identifiable information in patients' medical records without permission."[40] Importantly, however, the law does not "protect the clues that people leave about their health outside of their medical records—when they make credit-card purchases or search the Internet."[41] Because the individual pieces of data that the companies are collecting fall outside of the federal statute's protections, the collection and observation of medical data through data aggregation and observation is perfectly legal in the United States.[42]

Admittedly "[b]ig data creates tremendous opportunity" for societal benefits ranging from marketing to medical research to national security.[43] However, it is absolutely crucial if such progressions are going to be made that "[t]he extraordinary social benefits of big data . . . be reconciled with [the] increased risks to individuals' privacy."[44] Because the United States does not have a comprehensive law to protect individuals' privacy rights generally,[45] another solution may lie in the common law privacy tort of intrusion upon seclusion.

III. PRIVACY LAW AND INTRUSION UPON SECLUSION

A. Privacy Law Generally

Privacy law in the United States begins with Samuel Warren[46] and Louis Brandeis.[47] In fact, the first sentence of their groundbreaking

38. Walker, *supra* note 35.

39. *See* Wrongful Disclosure of Individually Identifiable Health Information, 42 U.S.C. § 1320d-6.

40. Walker, *supra* note 35.

41. *Id.*

42. *Id.*

43. Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE 25, 25 (2013).

44. Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 N.W. J. TECH. & INTELL. PROP. 239, 241 (2013).

45. *See* SOLOVE, *supra* note 21, at 67.

46. *See Samuel D. Warren*, WIKIPEDIA, http://en.wikipedia.org/wiki/Samuel_D._Warren (last visited Oct. 11, 2019).

47. Louis Brandeis was an American attorney, associate justice of the United States Supreme Court, and the co-author of the renowned Harvard Law Review article "The Right to Privacy." *See Louis D. Brandeis*, WIKIPEDIA, http://en.wikipedia.org/wiki/Louis_Brandeis (last visited Oct. 11, 2019).

Harvard Law Review Article, *The Right to Privacy* rings as true today as it did in 1890: "T[hat] the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection."[48] The law review article, which was the first of its kind on privacy, came about after Samuel Warren became irritated at newspaper coverage into his personal affairs.[49] He thus enlisted his former law partner to help formulate a general right to privacy.[50]

The relevancy of an article that was written 130 years ago is astounding.[51] The Warren and Brandeis article extensively discussed how "[r]ecent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the, individual what Judge Cooley calls the right 'to be let alone.'"[52]

Seventy years after *The Right to Privacy* was published, William Prosser[53] used the hundreds of privacy-involved court decisions that followed Warren and Brandeis' article to break the privacy laws into four distinct torts: (1) intrusion upon seclusion, (2) public disclosure of private facts,[54] (3) false light in the public eye,[55] and (4) appropriation.[56] The torts defined in Prosser's law review article were then used in the Second Restatement of Torts,[57] which remains the primary authority for courts on

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

49. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 383 (1960).

50. *Id.*

51. *See* Warren & Brandeis, *supra* note 48.

52. *Id.* at 195 (quoting THOMAS M. COOLEY, *COOLEY ON TORTS* 29 (2d ed. 1888).

53. *See William Lloyd Prosser*, WIKIPEDIA, http://en.wikipedia.org/wiki/William_*Lloyd*_*Prosser* (last visited Oct. 11, 2019). (explaining that Prosser was an American legal scholar, the Dean of the College of Law at UC Berkley, and the author of *Prosser on Torts*, which is "universally recognized as the leading work on the subject of tort law for a generation." Additionally, he was the Reporter for the *Restatement (Second) of Torts* and the author of the law review article *Privacy*.).

54. *See* RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW. INST. 1977) (explaining that public disclosure of private facts as a tort that creates liability for a person who gives publicity to a matter concerning the private life of another that is highly offensive to a reasonable person and is not of a legitimate concern to the public.).

55. *See id.* § 652E (explaining that false light in the public eye creates liability for a person who gives publicity to a matter concerning another that places the other before the public in a false light if the false light would be highly offensive to a reasonable person and the tortfeasor had knowledge or acted in reckless disregard as to the falsity of the publicized information.).

56. *See id.* § 652C (explaining that appropriation creates liability for one who appropriates to his own use or benefit the name or likeness of another); *see generally* Prosser, *supra* note 49.

57. *See id.* § 652B.

privacy law to this day. This Comment will focus solely on the tort of intrusion upon seclusion per its relevance here.[58]

B. Intrusion Upon Seclusion

The *Restatement (Second) of Torts* defines the tort of intrusion upon seclusion as "[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."[59] The tort of intrusion upon seclusion involves three main elements: (1) the intrusion must be intentional, (2) the intrusion must be upon the solitude of another or his private affairs,[60] and (3) the intrusion must be highly offensive to a reasonable person.[61]

With respect to the first element, the Restatement is clear that the intrusion need not be physical.[62] The comments provide further insight stating that the intrusion "may be by some other form of investigation or examination into [the victim's] private concerns . . . ."[63] Further, it is not necessary that the victim be aware of the tortfeasor's conduct.[64] Thus, courts have found that intrusions including "eavesdropping upon private conversations by means of [wiretapping] and microphones" do indeed fall under intrusion upon seclusion.[65] The Restatement provides an example: When A taps B's telephone wires and installs a recording device to record B's conversations, A has invaded B's privacy through intrusion upon seclusion.[66] Because the first element will not present a hurdle for the purposes of this Comment, the next two elements are of most importance.

The second element requires that the intrusion be upon the solitude of the victim's private affairs or concerns.[67] That is, "the thing into which

---

58. *Id.*
59. *Id.*
60. *See* Prosser, *supra* note 49, at 391 (explaining that "[i]t is clear also that the thing into which there is prying or intrusion must be, and be entitled to be, private.").
61. *See* RESTATEMENT (SECOND) OF TORTS § 652B; *see also* Prosser, *supra* note 49, at 390-91 (explaining that "[i]t is also clear that the intrusion must be something which would be offensive or objectionable to a reasonable man . . . .").
62. *Id.*
63. *Id.* at cmt. b.
64. *Id.*
65. Prosser, *supra* note 49, at 390.
66. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b, illus. 3.
67. *Id.*

there is prying or intrusion must be, and be entitled to be, private."[68] The tort applies if the plaintiff is confined to a private hospital room[69] or even having a private conversation at a table in a public restaurant.[70]

The final element to prove an intrusion upon seclusion claim is the highly offensive requirement.[71] This tort requires that the claimant show the intrusion is highly offensive to a reasonable person.[72] This begs the question: What is highly offensive? Highly offensive is based on an objective standard of the reasonable person, but the interference with the plaintiff's seclusion must be a substantial one.[73] Thus "there is no [intrusion upon seclusion claim] when the landlord stops by on Sunday morning to ask for the rent."[74]

IV. HURDLES IN APPLYING INTRUSION UPON SECLUSION TO DATAVEILLANCE

A. The Secrecy Requirement

The secrecy requirement for a valid intrusion upon seclusion claim presents issues for "dataveillance"[75] causes of action. The requirement that the intrusion be "upon the plaintiff's seclusion or solitude, or into his private affairs" also presents issues.[76]

The first issue with applying the tort of intrusion upon seclusion to a dataveillance claim is the fact that, as a 2002 Alabama court opinion put it, "[a] wrongful-intrusion claim cannot be based upon information voluntarily given to the defendant by the plaintiffs . . . ."[77] Additionally, information that is widely available to the public is not considered a secret, and therefore a valid intrusion upon seclusion claim cannot be brought in response to the collection of widely available information.[78] This stems directly from the illustrations provided in the Restatement itself.[79] For

68. Prosser, *supra* note 49, at 391.
69. *See* Barber v. Time, Inc., 159 S.W. 2d 291 (1942).
70. *See* Safari Club Int'l v. Rudolph, No. 14-55113 (9th Cir. 2014).
71. *See* RESTATEMENT (SECOND) OF TORTS § 652B.
72. *Id.*
73. *Id.*
74. Prosser, *supra* note 49, at 391.
75. SOLOVE, *supra* note 21, at 33 (defining "dataveillance" as the "systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons.").
76. Prosser, *supra* note 49, at 389.
77. Johnson v. Stewart, 854 So. 2d 544, 549 (Ala. 2002).
78. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 498 (2006).
79. *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW. INST. 1977).

example, "A is drunk on the public street. B takes his photograph in that condition. B has not invaded A's privacy."[80] For these reasons, "plaintiffs bringing claims involving surveillance in public have generally not been successful."[81] Thus, public information is insufficient to meet the secrecy requirement for a valid intrusion upon seclusion claim.[82]

The fact that information given voluntarily to a defendant or information that is available to the general public is not sufficient to meet the secrecy requirement presents an issue in applying the intrusion upon seclusion tort to data collection. This is because data collection usually involves information gathered from social media posts that the plaintiff voluntarily puts forth or public records.[83] Illinois Courts are particularly illustrative in explaining the issue presented in applying the intrusion upon seclusion tort to data collection.[84]

In *Busse v. Motorola, Inc.*, the plaintiffs brought suit against a research firm that purchased their data from their cell phone company so that the firm could conduct a study concerning any connection between cell phone use and mortality.[85] The firm not only used information supplied by the cell phone company, which included customer names, social security numbers, dates of birth, street addresses, etc., but also collected data from public databases such as death records.[86]

The plaintiffs brought an intrusion upon seclusion claim against the research firm.[87] However, the court found that the plaintiffs did not have a valid intrusion upon seclusion claim for the research firm's use of their personal information because none of the information that the research firm had obtained was considered private or a secret.[88] In making its decision, the court viewed only the collection of data as the basis for the

---

80. *Id.* at cmt. c, illus. 6.

81. Solove, *supra* note 78, at 497; *see also* Muratore v. M/S Scotia Prince, 656 F. Supp. 471, 482-83 (D. Me. 1987) (holding that photographers that harassed a plaintiff in public did not meet the secrecy requirement for a valid intrusion upon seclusion claim because there must be an "intrusion into a physical realm that is uniquely the plaintiff's.").

82. *See Johnson*, 854 So. 2d at 549 (explaining that "public information . . . cannot form the basis for an invasion-of-privacy claim.").

83. *See generally*, *Dataveillance*, WIKIPEDIA, http://en.wikipedia.org/wiki/Dataveillance (last visited Oct. 12, 2019).

84. *See* Busse v. Motorola, Inc., 813 N.E.2d 1013 (Ill. App. Ct. 2004); Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995).

85. *Busse*, 813 N.E.2d at 1015.

86. *Id.*

87. *Id.* at 1015-16.

88. *Id.* at 1017.

intrusion claim, and found that such pieces of individual data, alone, were not sufficiently private to meet the secrecy requirement.[89]

In *Dwyer v. American Express Co.*, the plaintiffs brought suit against their credit card company after the company rented out the plaintiffs' consumer profiles to third parties.[90] In creating these consumer profiles, the company compiled data extracted from the plaintiffs' credit card transactions and other personal information that the company had.[91]

The court found for the credit card company, relying on the fact that the plaintiffs voluntarily provided their credit card transaction summaries and other personal information.[92] Furthermore, the court held there was no valid intrusion upon seclusion claim because the plaintiff's information had been voluntarily disclosed and therefore did not meet the secrecy requirement.[93] Once again, as in *Busse*,[94] the court did not consider in its decision the compilation of the plaintiff's data as the invasion of privacy, but instead, the collection of the individual data.[95]

It is apparent from the study of the aforementioned cases that the issue presented in meeting the secrecy requirement for a valid intrusion upon seclusion claim does not lie in whether or not the information is private, but the fact that courts look to the collection of data as the intrusion, instead of the observation of the aggregated data profile as a whole.

B. The Highly Offensive Requirement

Another hurdle in overcoming the application of intrusion upon seclusion to dataveillance is that the information at issue must be highly offensive.[96] Even if the action surpasses the secrecy requirement, the action at issue must still be highly offensive to a reasonable person.[97]

The Restatement illustrates examples of what is considered highly offensive, stating that

> there is no liability for knocking at the plaintiff's door, or calling him to the telephone on one occasion or even two or three, to demand payment of a

89. *Id.* at 1018.
90. Dwyer v. Am. Express Co., 652 N.E.2d 1353, 1354 (Ill. App. Ct. 1995).
91. *Id.*
92. *Id.*
93. *Id.*
94. *Busse*, 813 N.E.2d 1013.
95. *Dwyer*, 652 N.E.2d at 1353-54.
96. *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW. INST. 1977).
97. *Id.*

> debt. It is only when the telephone calls are repeated with such persistence and frequency as to amount to a course of hounding the plaintiff, that becomes a *substantial burden to his existence*, that his privacy is invaded.[98]

In terms of applying the intrusion upon seclusion tort to data collection, the highly offensive requirement presents an obstacle.[99] Most of the information collected in databases would not be considered highly offensive information to a reasonable person because "[e]ach particular instance of collection is often small and innocuous."[100] For example, courts have found that information such as telephone numbers, names, street addresses, etc. are not highly offensive because such information is not offensive or embarrassing.[101]

The highly offensive requirement is not an insurmountable threshold for dataveillance claims.[102] However, a theoretical shift is necessary for courts to find that such intrusion allegations meet the highly offensive threshold.[103] As with the secrecy requirement, this shift stems from courts' refusal to apply the intrusion upon seclusion tort to the observation of aggregated personal data, instead of the collection of personal data.[104] The highly offensive requirement could be met easily if courts begin to realize that "the danger [to the plaintiff] is created by the aggregation of information."[105] The next Part of this Comment presents arguments for overcoming the secrecy requirement and the highly offensive requirement in applying the intrusion upon seclusion tort to data aggregation and observation, instead of data collection.

V. OVERCOMING THE ELEMENTS

Because of the digital revolution, our personal information can be gathered and combined quicker and easier than ever.[106] Law Professor Daniel Solove writes: "[i]nformation breeds information" and our personal data is now "being combined to create a digital biography about us."[107] Solove refers to this phenomenon as "the aggregation effect"

98. *Id.* at cmt. d (emphasis added).
99. *See* SOLOVE, *supra* note 21, at 59.
100. *Id.*
101. *See* Busse v. Motorola, Inc., 813 N.E.2d 1013 (Ill. App. Ct. 2004).
102. *See* RESTATEMENT (SECOND) OF TORTS § 652B.
103. *See* SOLOVE, *supra* note 21, at 59.
104. *Id.*
105. *Id.*
106. *Id.* at 44.
107. *Id.*

because "a comprehensive collection of data about an individual is [worth] vastly more than the sum of its parts."[108]

The real danger to our data privacy lies not in the collection of our personal information through voluntary disclosures or public records, but in the stories of our lives that can be extracted from that data in its entirety.[109] For this reason, it is crucial for courts to realize that the intrusion upon seclusion threat to individuals does not occur in the mere collection of data, but in the observation of such data once it has been aggregated and processed to form a digital biography of each individual.[110] Recognition of the intrusion upon seclusion tort at the observation stage would provide a massive trampoline for a plaintiff attempting to clear the secrecy and highly offensive hurdles.

A. Overcoming the Secrecy Requirement

Overcoming the secrecy requirement for a valid intrusion upon seclusion claim is only possible if courts shift their analysis on data privacy cases from one of application to data collection to one of application to data aggregation and observation. Recall that the secrecy requirement stems from the Restatement's definition that the intrusion must be "upon the solitude or seclusion of another or his private affairs or concerns."[111] This definition alone simply cannot be applied to data collection, as such information was either voluntarily disclosed or found in a public record. However, if a company were to unlock new information about an individual from the public data available through aggregation and observation, such new information should certainly be considered private, as it was never voluntarily disclosed or available to the general public through a public record.

The Cambridge Analytica-Facebook scandal is illustrative.[112] In early 2018, it was revealed that Cambridge Analytica harvested the

---

108. *Id.* (quoting Julie E. Cohen, *Examined Lives: Informational Privacy and the Subjects as Objects*, 52 STAN. L. REV. 1373, 1397 (2000)).

109. *Id.* (explaining that "[i]nformation that appears innocuous can sometimes be the missing link, the critical detail in one's digital biography, or the key necessary to unlock other stores of personal information.").

110. *See id.* at 44-47.

111. RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW. INST. 1977).

112. *See Facebook-Cambridge Analytica Data Scandal*, *supra* note 5; *see also* Busse v. Motorola, Inc., 813 N.E.2d 1013 (Ill. App. Ct. 2004). In *Busse*, the court only applied the intrusion upon seclusion tort to the data collection phase and did not consider whether or not the aggregation of the processed data met the secrecy requirement for a viable intrusion upon seclusion claim.

personal data of millions of people's Facebook profiles without their consent and used it for political advertising purposes.[113] Cambridge Analytica first did this by paying small sums of around $3 to U.S. voters who took a personality survey.[114] The survey gave users an "OCEAN" score based on the user's openness, conscientiousness, extroversion, agreeableness, and neuroticism.[115] The survey was based on sound psychological research that has been used for decades.[116] Like many modern applications, the survey required that the user log in through their Facebook profile.[117]

Next, Cambridge Analytica garnered access to not only the individual's Facebook account that they had provided, but the accounts of all the individual's Facebook friends.[118] This process provided Cambridge Analytica with the Facebook profiles of over fifty million United States voters.[119] Finally, Cambridge Analytica used algorithms to combine the Facebook data with other now easily matchable sources such as voter records to create digital biographies of each individual voter.[120] Such biographies contained approximately 5,000 data points on each individual.[121] These digital biographies were then used to create tailored advertisements to voters based on their own data.[122]

Since the Cambridge Analytica scandal, a few plaintiffs have brought suit against the company for intrusion upon seclusion.[123] Most of the cases have not yet been decided; however, courts will likely find that there is no substantial basis for the claims because the information obtained was

---

113. *Facebook-Cambridge Analytica Data Scandal*, *supra* note 5.

114. Alex Hern, *Cambridge Analytica: How Did it Turn Clicks Into Votes*, THE GUARDIAN (May 6, 2018, 3:00 PM), http://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie.

115. Erin Brodwin, *Here's the Personality Test Cambridge Analytica Had Facebook Users Take*, BUS. INSIDER (Mar. 19, 2018, 3:01 PM), http://www.businessinsider.com/facebook-personality-test-cambridge-analytica-data-trump-election-2018-3.

116. *Id.*

117. *Id.*

118. Hern, *supra* note 114.

119. *Id.*

120. *Id.*

121. *Id.*

122. *Id.*

123. *See* Rubin v. Facebook, Inc., COURT LISTENER, http://www.courtlistener.com/docket/6346601/rubin-v-facebook-inc/ (last visited Dec. 2, 2019); Atlas Consumer Law, *Files Federal Class Lawsuit Against Cambridge Analytica, Facebook & Mark Zuckerberg on Behalf of Plaintiffs*, PR NEWSWIRE (Mar. 27, 2018, 7:22 AM), http://www.prnewswire.com/news-releases/atlas-consumer-law-files-federal-class-lawsuit-against-cambridge-analytica-facebook--mark-zuckerberg-on-behalf-of-plaintiffs-300620666.html.

either voluntarily provided (through Facebook) or obtained through a public record (voter records, etc.).[124] This is because the court will likely apply the tort only to the collection phase of such a process. In fact, in *In re Facebook, Inc.*, the United States District Court for the Northern District of California recently dismissed a plaintiff's intrusion upon seclusion claim regarding the Cambridge Analytica scandal, stating that the plaintiffs consented to having their information shared.[125] However, in applying this tort in such a narrow way, the California court failed to alleviate the real dangers posed from such processes.

The real danger posed by the Cambridge Analytica-Facebook scandal was not the collection of individuals' Facebook data and voting records, it was the aggregation and processing of such data to create digital biographies used as political weapons. If courts were to apply the intrusion upon seclusion claim to the aggregation and observation of the individual's data, the secrecy requirement would easily be met. As Solove put it, "[i]nformation breeds information,"[126] and there were clearly missing links of private information uncovered by aggregating the individuals' single threads of data into digital biographies. To put it simply, if there were no missing links to be found by aggregating an individuals' data, why would companies even bother?

B. Overcoming the Highly Offensive Requirement

Overcoming the highly offensive requirement for a valid intrusion upon seclusion claim is also only possible if courts apply the intrusion tort to data aggregation and observation instead of data collection. Recall that for a valid intrusion upon seclusion claim, the intrusion must be highly offensive to a reasonable person.[127] It is clear from past decisions that the single threads of data collected are unlikely to be seen as highly offensive.[128] However, when observed in the aggregate, such data certainly could reach a highly offensive threshold.[129]

While what is considered offensive will still be left up to a jury, such a shift in analysis would give courts a better way to consider these

---

124. *See* Atlas Consumer Law, *supra* note 123.

125. *In re* Facebook, Inc., No. MDL No. 2843, 2019 U.S. Dist. LEXIS 153505, at *1, *65-71 (N.D. Cal. Sep. 9, 2019).

126. SOLOVE, *supra* note 21, at 44.

127. RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW. INST. 1977).

128. *See* Busse v. Motorola, Inc., 813 N.E.2d 1013 (Ill. App. Ct. 2004); Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995).

129. SOLOVE, *supra* note 21, at 44.

situations. One way to consider the standard of offensiveness is to consider the plaintiff's expectations about their personal data.[130]

This consideration is relevant to offensiveness because "people selectively spread around small pieces of data . . . and they have the expectation that in each disclosure, they are revealing relatively little about themselves."[131] By taking these traces of data and processing them into digital biographies, for purposes wholly unrelated to why the individual disclosed the information in the first place, data aggregation and observation harshly "unsettles expectations" about what an individual meant to disclose about themselves from their random traces of data.[132] The Restatement provides some guidance here by using the following example: A, a young woman, attends a "Fun House," and while there a concealed jet of compressed air blows her skirt over her head, revealing her underwear.[133] While she is in that position, B takes a photograph. The Restatement explains that in this situation, B has invaded A's privacy.[134] In this, courts must consider the fact that "[p]eople expect certain limits on what is known about them and on what others will find out."[135]

The Cambridge Analytica-Facebook Scandal is once again illustrative. Cambridge Analytica used separate strands of data collected from Facebook profiles and public records to process and create digital biographies on U.S. voters.[136] The company then used such digital biographies to narrowly tailor advertisements that appealed to each individual voter in order to persuade them to vote for a particular candidate.[137] While such information that was collected from the voters was mostly voluntarily disclosed information from Facebook and public voting records, when viewed in the aggregate or at the observation phase, such information could certainly be regarded as highly offensive.[138]

More important is the voter's expectations about the usage of such data. Such voters likely made Facebook profiles to keep up with friends and registered to vote to exercise their rights. It is unlikely that they ever

130. *See* Solove, *supra* note 78, at 508.
131. *Id.* at 507.
132. *Id.*
133. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c, illus. 7 (AM. LAW. INST. 1977).
134. *Id.*
135. Solove, *supra* note 78, at 507.
136. Hern, *supra* note 114.
137. *Id.*
138. *Id.*; *see also* THE GREAT HACK, *supra* note 1 (In the film, Brittany Kaiser, one of the whistleblowers, explicitly states: "we targeted those whose minds we thought we could change until they saw the world the way we wanted them to.").

expected that such information would eventually be compiled, processed, and weaponized against them as political warfare in a presidential election.[139]

If a court were to consider whether or not such unprecedented, aggregated digital biographies were highly offensive, the court would likely find that the aggregation and observation of such data would meet the highly offensive requirement.[140] While these cases will ultimately turn on the exact facts of each particular case, modifying the court's analysis to one of data aggregation and observation instead of data collection would certainly be beneficial in jumping the hurdle of the highly offensive requirement.[141]

VI. CONCLUSION

To this day, Warren and Brandeis still put it best: "[p]olitical, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."[142] It cannot be adequately expressed how much our political, social, and economic environments have changed since Warren and Brandeis recognized the right to privacy in 1890.[143] Arguably, with the advent of digital technology and our nonchalance about putting our entire lives online, we need privacy protections more than ever. It certainly is not a provable statement that the outcome of the 2016 presidential election would have seen a different outcome without Cambridge Analytica's abuse of data for targeted advertising;[144] however, it should not be ignored either. A whistleblower from Cambridge Analytica said in the documentary "The Great Hack": "I do know that [Cambridge Analytica's] targeting tool was considered a weapon."[145]

As "[t]he story of privacy law is a tale of changing technology and the law's struggle to adapt in effective ways[,]"[146] it is time for courts to adapt their analysis in data privacy cases. Courts should stop applying the intrusion upon seclusion tort to data collection and instead apply it to data

139. *See* THE GREAT HACK, *supra* note 1.
140. *See* RESTATEMENT (SECOND) OF TORTS § 652B (AM. LAW. INST. 1977).
141. *Id.*
142. Warren & Brandeis, *supra* note 48, at 193.
143. *See id.*
144. Hern, *supra* note 114.
145. *The Great Hack*, *supra* note 1.
146. SOLOVE, *supra* note 21, at 56.

aggregation and observation.[147] We have already seen the negative effects that unregulated data aggregation and observation can have on individuals, political outcomes, and much more. However, what is even more frighteningly perhaps is that we are likely not yet capable of fully understanding just what is at stake.

147. *See* Busse v. Motorola, Inc., 813 N.E.2d 1013 (Ill. App. Ct. 2004); Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995).