PROTECTING USERS OF SOCIAL MEDIA

*Margaret Ryznar**

Social media platforms started as a fun way to connect with friends and family. Since then, they have become a science fiction nightmare due to their capacity to gather and misuse the data on their users.[1]

For example, in early 2018, a whistleblower revealed that major election and referendum votes were influenced by "psychological warfare" on Facebook users through data obtained by Cambridge Analytica.[2] A few years before this, Facebook admitted to running a psychological experiment on its users that may have altered their moods to see whether "emotional contagion" could be spread.[3] Meanwhile, in 2014, the free online dating website OkCupid acknowledged that it intentionally

* Professor of Law, Indiana University McKinney School of Law. Thanks to Carolyn Kelly for valuable comments on an earlier draft.

1 "One well-recognized threat" to privacy that arises from the conversion of our social interactions into data "is from the robust concentrations of electronic information aggregated into colossal databases." Woodrow Hartzog, *Social Data*, 74 OHIO ST. L.J. 995, 995 (2013). However, other issues arise from social media use. For example, Facebook has led to many divorces because it alerts spouses to infidelity in addition to providing proof of it for court. *See, e.g.*, Shane Witnov, *Investigating Facebook: The Ethics of Using Social Networking Websites in Legal Investigations*, 28 SANTA CLARA COMPUTER & HIGH TECH. L.J. 31, 32 (2011) (noting that a majority of matrimonial lawyers have used evidence from social networks).

2 *See, e.g.*, Carole Cadwalladr, *"I Made Steve Bannon's Psychological Warfare Tool": Meet the Data War Whistleblower*, GUARDIAN (Mar. 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump. A Cambridge University academic allegedly developed an app that pulled the Facebook data of fifty million people without their consent when their Facebook friend used the app. *Id.* Facebook acknowledged that it allowed the Cambridge researcher in cognitive and behavioral neuroscience to obtain the data with user permission, but the app did so without the consent of millions of users. *Id.* Then, a political intelligence firm built psychological profiles on people who would be targeted with certain messaging to influence them in, for example, the 2016 U.S. presidential election and the Brexit vote in the United Kingdom. *Id.* "Research suggests that social media data and information about a user's website choices can be used to determine a user's personality." Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1403 (2017).

3 *See* Calli Schroeder, Note, *Why Can't We Be Friends? A Proposal for Universal Ethical Standards in Human Subject Research*, 14 COLO. TECH. L.J. 409, 410–11 (2016).

made incompatible matches for research purposes.[4] Even without such meddling, online dating can lead to lawsuits.[5]

It is not irrational for social media providers to seek to capitalize on their data when they provide the platforms for free.[6] Indeed, their business model is to sell data to third parties for marketing and other purposes.[7] Yet, users should be able to expect that their data is not used to hurt them or is not sent to disreputable companies. Indeed, fewer people would use social media if the price were incurring a mood disorder or being manipulated to vote in a particular way.[8]

While technology continues to push the boundaries of law as it evolves, effective legal protection has not evolved with it.[9] As evidenced by recent events, the field of privacy has failed social media users.[10] Meanwhile, the field of cybersecurity arose to address cybercrime, but many of the questionable uses of

4 James Grimmelmann, *The Law and Ethics of Experiments on Social Media Users*, 13 COLO. TECH. L.J. 219, 223–24 (2015) (summarizing some of the experiments conducted on unknowing social media users).

5 *See, e.g.*, Phyllis Coleman, *Online Dating: When "Mr. (or Ms.) Right" Turns Out All Wrong, Sue the Service!*, 36 OKLA. CITY U. L. REV. 139, 157–58 (2011).

6 Yet, social media companies do not correct misperceptions regarding this. "Companies often summarize their data privacy policy as a series of services for the user's benefit without making clear what value the company is getting from the consumer's personal information." Lauren Henry, Note, *Institutionally Appropriate Approaches to Privacy: Striking a Balance Between Judicial and Administrative Enforcement of Privacy Law*, 51 HARV. J. ON LEGIS. 193, 194 (2014).

7 *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 62–63 (2013); *see also* Katheryn A. Andresen, *Marketing Through Social Networks: Business Considerations—From Brand to Privacy*, 38 WM. MITCHELL L. REV. 290, 293–94 (2011) (explaining the business model of social networking websites).

8 "I'd feel betrayed to find out that a company that purports to be a conduit to help me find others' content turned out to be shaping my experience according to its political agenda." Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 337 (2014).

9 "In 1986, Congress passed the Stored Communications Act ('SCA') to provide additional protections for individuals' private communications content held in electronic storage by third parties. . . . Yet, because Congress crafted the SCA with language specific to the technology of 1986, courts today have struggled to apply the SCA consistently with regard to similar private content sent using different technologies." Christopher J. Borchert et al., *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36, 36 (2015).

10 Privacy as a concept is complicated, evading definitions and standards. *See* Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1333 (2013) (noting regulators' reliance on "'privacy by design' as a critical element of their ongoing revision of current privacy laws. . . . But [Fair Information Practices] are not self-executing."); Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717, 723 (2013) (noting, for example, the FTC's past decision to make social media companies have a privacy policy, but not imposing any content for that policy). *See generally* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

social media data were legal. The legality of these problematic actions has received criticism and prompted calls for change.[11]

There are several choices lawmakers and policymakers have when it comes to the protection of social media data from exploitation by social media companies. Among these are fiduciary duties in corporate and trust law, as well as the duty of care in tort law.[12] However, can these centuries-old legal frameworks grasp the risks and consequences of the improper use of big data generated by social media, or must they be tweaked?

This Essay examines the benefits and drawbacks of fiduciary duties and the duty of care frameworks in the context of social media. Any framework must hold data holders responsible for data breaches while fitting their business model.

I. FIDUCIARY DUTIES

Fiduciary duties are a package of obligations imposed on those entrusted with the interests of others, often in regard to financial holdings in the fields of corporate law and trust law.[13] The two main fiduciary duties are the duty of loyalty and the duty of care.[14] The duty of care essentially requires the fiduciary to pursue the interests of the other party to the fiduciary relationship, whereas the duty of loyalty basically demands that the conduct of the fiduciary be free from conflict and self-dealing.[15] A fiduciary may also owe subsidiary duties, such as duties of good faith.[16]

---

11 "As technological innovation accelerates, so does the need to recalibrate individual expectations, social norms, and, ultimately, laws and regulations." Tene & Polonetsky, *supra* note 7, at 73. "Consumers, companies, and policymakers increasingly think about collection and control of personal information, and the media prominently highlights these issues." Nicole A. Ozer, *Putting Online Privacy Above the Fold: Building a Social Movement and Creating Corporate Change*, 36 N.Y.U. REV. L. & SOC. CHANGE 215, 215 (2012).

12 *See* Ari Ezra Waldman, *Designing Without Privacy*, 55 HOUS. L. REV. 659, 710 (2018). Other legislative choices include heightened Institutional Review Board (IRB) requirements when academic researchers are involved in particular or implementing a "right to be forgotten" like the European Union. *See, e.g.*, Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349, 353 (2015); Lauren B. Solberg, Note, *Data Mining on Facebook: A Free Space for Researchers or an IRB Nightmare?*, 2010 U. ILL. J.L. TECH. & POL'Y 311, 312. Another possibility is a citizen-suit provision in relevant legislation, coupled with a prohibition on mandatory binding arbitration. This would help level the playing field between individual users and a massive, wealthy corporation that controls huge flows of information and valuable social networks. Knowing that regular users can sue might also provide an incentive for social media companies to police themselves. *See* Joshua A.T. Fairfield & Christoph Engel, *Privacy as a Public Good*, 65 DUKE L.J. 385, 385 (2015) (noting that people's attitude toward their own privacy impacts others, making privacy a public good).

13 *See generally* ROBERT H. SITKOFF & JESSE DUKEMINIER, WILLS, TRUSTS, AND ESTATES 588 (10th ed. 2017).

14 Andrew D. Appleby & Matthew D. Montaigne, *Three's Company:* Stone v. Ritter *and the Improper Characterization of Good Faith in the Fiduciary Duty "Triad,"* 62 ARK. L. REV. 431, 431 (2009).

15 *See id.* at 432.

16 *See id.* at 431.

Fiduciary duties have traditionally involved a financial relationship between the parties,[17] but this does not prevent their application to social media companies. Users generate data, which is valuable because marketers routinely purchase it to better target their advertisements.[18] Trust is a significant factor in people's willingness to share personal information on online social networks.[19] Thus, the fiduciary duty model may be applicable.[20]

There are several reasons to apply a fiduciary duty framework to social media. Fiduciary duties have few exceptions, making them strong protectors of users. When engaged in self-dealing, for example, the fiduciary in trust law is subject to a no-further-inquiry principle—good faith and fairness to the beneficiaries are not a defense.[21] This would also prevent social media companies from abrogating these duties in their contracts with users,[22] thus barring Facebook from contractually requiring its users to weaken the company's duties of loyalty and care. This is important given the contractual nature of the relationship between users and social media companies.[23]

One useful feature of this framework is its subset of subsidiary duties, such as the duty for social media platforms to do due diligence on companies buying or otherwise seeking the big data generated by social media users.[24] For example, Facebook would have to explore the background of companies seeking its data with the intention of preventing the Cambridge Analytica scenario.[25] Another relevant and important fiduciary duty is to delegate work with the data only to reasonable parties, carefully selecting, instructing, and monitoring them.[26] Finally, the duty of prudence in trust law requires a degree of care, skill, and caution.[27] These fiduciary

17 *See id.* at 440 (discussing the traditional context of a fiduciary duty arising between a shareholder and the director of that same corporation).

18 *See* Dennis D. Hirsch, *The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation?*, 34 SEATTLE U. L. REV. 439, 447 (2011) (noting that websites, network advertisers, data brokers, secondary users, and the government all use data on individuals).

19 Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RES. L. REV. 193, 193 (2016).

20 *See* Ari Ezra Waldman, *Privacy, Notice, and Design*, 21 STAN. TECH. L. REV. 74, 122 n.245 (2018) ("Many scholars, including Daniel Solove, Jack Balkin, Jonathan Zittrain, Danielle Citron, and others, have recommended a shift toward a fiduciary or trustee model to ensure corporations take consumer privacy seriously. Notably, scholars suggested that changes to law on the books would be necessary before any such fiduciary relationship took hold.").

21 SITKOFF & DUKEMINIER, *supra* note 13, at 599.

22 *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1179 (2009) (noting users will not negotiate enough privacy with the social media company in many circumstances).

23 *See, e.g.*, *In re* Facebook Internet Tracking Litig., 263 F. Supp. 3d 836, 841 (N.D. Cal. 2017).

24 As of 2017, there are over 455,000 Tweets per minute and three million posts shared per minute on Facebook—and these numbers are growing. Jeff Schultz, *How Much Data Is Created on the Internet Each Day?*, MICRO FOCUS BLOG (Oct. 10, 2017), https://blog.microfocus.com/how-much-data-is-created-on-the-internet-each-day/.

25 *See supra* note 2 and accompanying text.

26 SITKOFF & DUKEMINIER, *supra* note 13, at 658–60.

27 Specifically, a trustee shall invest and manage trust assets as a prudent investor would, by considering the purposes, terms, distribution requirements, and other circumstances of the

duties would slow the involvement of bad actors seeking big data from social media platforms.

However, there are drawbacks to imposing fiduciary duties on social media structures. Among these are the number of duties and the strictness of the standard, which may be ill fitted to impose on a voluntary, nonfinancial relationship. For example, the conflict of interest that social media companies have with user data is practically inherent to their business model, possibly leading to the distortion of the fiduciary duty standard. Fiduciary duties may simply be too inflexible for the social media context. These concerns are less prevalent in the duty of care in tort law.

II. DUTY OF CARE

The duty of care is a legal obligation that a party act toward another as a reasonable person in the circumstances would.[28] In a tort case, if the actions do not meet the standard of care, then the actor may be liable for any injuries caused.[29]

The duty of care between two parties depends on their relationship. For example, product manufacturers have a duty to consumers to make safe products, property owners have a duty to visitors to protect them, and business directors have a duty to shareholders to make reasonable decisions in the best interests of the business.[30]

However, courts have been hesitant to establish a duty of care owed by data aggregators to consumers who are not the customers.[31] Indeed, "[w]hen consumers seek to enforce a breached duty of care claim, courts struggle to coherently establish when and between whom the duty existed."[32] Two recent cases reflect the courts' hesitancy:

> In *Willingham v. Global Payments, Inc.*, the court held that a payment processor owed no duty to consumers using the company's platform to send funds to merchants. Similarly, in *In re Zappos.com, Inc.*, the court declined to treat a company statement about the security policy as an enforceable contract and also denied the existence of an implied contract to safeguard the data.[33]

If the courts continue to find no duty of care in the social media context, legislators may decide to introduce a statute that imposes such a duty.[34] For

---

trust. *Id.* at 624. This can be translated to the social media context by requiring social media companies to manage user data with prudence.

28 *See* David W. Barnes & Rosemary McCool, *Reasonable Care in Tort Law: The Duty to Take Corrective Precautions*, 36 ARIZ. L. REV. 357, 379 (1994).

29 *See id.*

30 *See, e.g.*, *id.* at 386.

31 Matthew Hector, *Do We Really Have* No Place to Hide*?*, 24 J. MARSHALL J. COMPUTER & INFO. TECH. & PRIVACY L. 57, 64 (2005) (reviewing ROBERT O'HARROW, JR., NO PLACE TO HIDE (2005)).

32 Merritt Baer & Chinmayi Sharma, *Does Equifax Owe Victims a Duty of Care?*, LAWFARE (Sept. 12, 2017), https://www.lawfareblog.com/does-equifax-owe-victims-duty-care.

33 *Id.*

34 *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) (considering the role of courts

example, a duty of care has been codified in statutes like the Data Protection Act in the United Kingdom.[35] Effective legislation must delineate what is encompassed in the duty of care because social media companies can exploit vague language. Congress can also assign a federal agency such as the Federal Communications Commission some responsibility for oversight and development of more detailed regulations, but clear statutory language is necessary to guard against regulatory capture.

Applying the duty of care to the social media context accepts social media's function to collect and profit on people's data. Social media users do not produce confidential information—they produce big data. In contrast, for example, a lawyer representing a client must use reasonable care to avoid inadvertent disclosure of confidential information.[36]

Thus, the duty of care can acknowledge the business model of firms in big data, while requiring that they vet the companies with which they interact. It continues to incentivize Facebook and other social media companies to engage in exchanging free services with users for data, while limiting the possibility of data compromise. This would avoid giving user data to companies like Cambridge Analytica, but would not harm Facebook's relationships with established businesses like Sephora.[37] While it is difficult to determine which actions would breach the duty of care, perhaps at least "novel, unexpected use of existing information" can be discouraged.[38]

Given the social media model, it may be that the duty of care is more appropriate than fiduciary duties. This would justify the application of the duty of care from tort law to the modern-day problem of data protection in social media.

CONCLUSION

The current framework for protecting users of social media does not work. Modern cybersecurity laws do not apply to the social media model of sharing or selling user data. In contrast, both the centuries-old fiduciary duties and the duty of care in tort law offer ways to protect the data of social media. They provide remedies to social media users by allowing them to sue the social media company that failed to uphold the duty owed, which would influence the way social media companies use their data and self-police. The adaptability of ancient common-law doctrine to modern dilemmas could thus save social medial users a lot of grief, undue influence, and harm.

---

versus legislatures in protecting threats to privacy by technology in the Fourth Amendment context).

35 Data Protection Act 1998, c. 29 (UK).

36 JOHN M. BURKOFF, CRIMINAL DEFENSE ETHICS: LAW AND LIABILITY § 5:9 (2d ed. 2018).

37 *See supra* note 2 and accompanying text.

38 Tene & Polonetsky, *supra* note 7, at 68. "Limited public awareness about these practices has contributed to a regulatory environment in which the aggregation and brokering of personal data has largely gone unchecked." Mary Madden et al., *Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans*, 95 WASH. U. L. REV. 53, 65 (2017).