WAKE FOREST JOURNAL OF BUSINESS AND INTELLECTUAL PROPERTY LAW

VOLUME 20 FALL 2019 NUMBER 1

FINDING THE LINE: THE RELATIONSHIP BETWEEN PRIVACY AND SMARTPHONE APPLICATIONS

James Kuritzkes[†]

 James Kuritzkes is a J.D. candidate at Wake Forest University School of Law in the class of 2020. He is a graduate of Trinity College where he earned a B.A. in Economics. James would like to extend his sincere gratitude to the Journal's Board of Editors and Staff for their invaluable assistance with this article. James would also like to thank his family and friends for their continuous support and encouragement.

Whether the certification architecture that emerges protects privacy depends upon the choices of those who code. Their choices depend upon the incentives they face. If protecting privacy is not an incentive--if the market has not sufficiently demanded it and if law has not, either--then this code will not provide it.[1]

— Lawrence Lessig

I. INTRODUCTION

Since smartphones became the standard cellular device, there has been widespread concern on how to protect the data that individuals share with smartphone applications.[2] Despite a clear need for regulation in this space, state and federal lawmakers have yet to devise a comprehensive legislative scheme to govern smartphone applications' data collection practices.[3] In his 1999 book, *Code and Other Laws of Cyberspace*,[4] Lawrence Lessig argues that four modalities govern legislative regulation: the law, social norms, the market, and architecture.[5] Using Lessig's four modalities as a guide, this Article postulates important considerations for lawmakers as they devise a regulatory framework for data collection by smartphone applications.

Lessig hypothesizes that technological privacy hinges on the incentives of the architects who code the technology.[6] Because application developers are incentivized by profit,[7] Lessig's theory underscores the conflict of interest that all application developers face.[8] Once their applications launch, developers become the stewards of the personal information that their applications collect, and they must choose whether to safeguard the information or to sell the information to increase their revenue streams.[9] Increasingly, developers have elected to monetize, choosing to sell the personal information collected

[1] Lawrence Lessig, *Code Is Law: On Liberty in Cyberspace*, HARV. U. MAG., (Jan. 1, 2000), https://www.harvardmagazine.com/2000/01/code-is-law-html.

[2] *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy Before the S. Comm. on the Judiciary*, 112th Cong. 112–857, at 4 (2011) (statement of Sen. Patrick J. Leahy) (discussing the privacy implications of smartphones and other mobile applications).

[3] *Id.* at 5.

[4] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[5] *Id.* at 88–89.

[6] Lessig, *supra* note 1.

[7] Eleanor Lumsden, *Securing Mobile Technology & Financial Transactions in the United States*, 9 BERKELEY BUS. L.J. 139, 161 (2012).

[8] *Id.* at 161–62.

[9] Mihailis E. Diamantis, *Privileging Privacy: Confidentiality as a Source of Fourth Amendment Protection*, 21 U. PA. J. CONST. L. 485, 499–500 (2018).

by their applications.[10] As of May 2019, seven in ten application developers have chosen to augment their revenues instead of protecting users' privacy.[11]

This is not to say that we should prohibit applications from the responsible collection of users' personal data. Developers have legitimate purposes to collect user information and often rely on collecting analytical data to improve their applications.[12] Additionally, the nature of many applications requires them to collect personal information to function properly.[13] For example, to provide accurate directions, a Global Positioning System ("GPS") application must collect both the user's location and desired destination in order to transmit that data to a server.[14] Data collection of this nature is appropriate if the application (responsibly) does not store that data after the user ceases to use the GPS application. In this case, the application is no more intrusive than is necessary given the service that it provides.[15] Moreover, the data collected–a user's location and destination–is commensurate with what a reasonable user would expect necessary to ensure proper GPS function.

However, not all applications use straightforward data. One such application, which this Article will use in several of its illustrations, is the Facebook for smartphones application. The Facebook application is the most downloaded, third-party application on both the Google Play Store and the App Store,[16] and the application frequently attracts scrutiny.[17] Critics contend that the application's data collection practices constitute a breach of privacy because they believe that

[10] Sam Schechner & Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*., WALL ST. J. (Feb. 22, 2019, 11:07 AM), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[11] Narseo Vallina-Rodriguez & Srikanth Sundaresan, *7 in 10 Smartphone Apps Share Your Data with Third-Party Services*, THE CONVERSATION (May 29, 2017, 9:48 PM), https://theconversation.com/7-in-10-smartphone-apps-share-your-data-with-third-party-services-72404.

[12] Yafit Lev-Aretz, *Data Philanthropy*, 70 HASTINGS L.J. 1491, 1513 (2019).

[13] *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy Before the S. Comm. on the Judiciary*, *supra* note 2, at 95.

[14] *See id.*; Vallina-Rodriguez & Sundaresan, *supra* note 11.

[15] *See Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy Before the S. Comm. on the Judiciary*, *supra* note 2, at 12.

[16] Michael Potuck, *These are the All-Time Most Popular iOS Apps and Games from 2010-2018*, 9TO5 MAC (Jul. 2, 2018), https://9to5mac.com/2018/07/02/all-time-most-popular-ios-apps-games/; *Facebook*, ANDROIDRANK, http://www.androidrank.org/application/facebook/com.facebook.katana (last updated Oct. 20, 2019); Schechner & Secada, *supra* note 10.

[17] Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. 1333, 1404 (2013).

application collects far more data than it functionally requires.[18] Facebook contends that it requires such massive amounts of data because of the wide assortment of services that the application provides.[19] Facebook's privacy policy makes it clear that the application attempts to derive as much data as possible, including users' cell phone signal strength, battery life, and the device's serial number.[20] So, how should the data collecting practices of an expansive application like Facebook be regulated?

Many scholars have employed Lessig's modalities to steer regulation in different contexts.[21] Scholars generally agree that the modalities present an effective framework when considering potential regulations.[22] However, there has yet to be a thorough application of the modalities to the regulation of data contained on smartphones. Scholars have analyzed the concept of smartphone data privacy, and there is general agreement that regulations are necessary to protect users' data.[23] The need for regulations is especially pertinent given smartphones' ability to record health-related data.[24] There is also a consensus among scholars that the most challenging issue that legislatures must consider is the dichotomy between privacy and convenience.[25] Indeed, users appreciate notifications about changes in weather at their current location;[26] however, are users willing to constantly share their location with weather applications to receive this service? Moreover, are smartphone users' content with weather

[18] *See* Schechner & Secada, *supra* note 10.

[19] *See Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last visited Oct. 28, 2019).

[20] *Id.*

[21] *See*, *e.g.*, James Grimmelmann, *Regulation by Software*, 114 YALE L.J. 1719, 1725 (2005).

[22] *Id.*; William McGeveran, *Programmed Privacy Promises: P3P and Web Privacy Law*, 76 N.Y.U.L. Rev. 1812, 1815 (2001).

[23] Grimmelmann, *supra* note 21, at 1726; McGeveran, *supra* note 22, at 1815.

[24] Stacy-Ann Elvy, *Paying for Privacy and the Personal Data Economy*, 117 COLUM. L. REV. 1369, 1389 (2017); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 874 (2016); Jamie Lynn Flaherty, *Digital Diagnosis: Privacy and the Regulation of Mobile Phone Health Applications*, 40 AM. J.L. & MED. 416, 418–21 (2014); *see also*, Cynthia A. Brown & Carol M. Bast, *Professional Responsibility: Making "Smart" Ethical Decisions While Making the Most of "Smart" Technology*, 48 CREIGHTON L. REV. 737, 756–61 (discussing whether legislatures need to legislate the ability of smartphone applications to secretly record their users utilizing the smartphone's camera and speaker).

[25] Ashton McKinnon, *Sacrificing Privacy for Convenience: The Need for Stricter FTC Regulations in an Age of Smartphone Surveillance*, 34 J. NAT'L ASS'N ADMIN. L. JUDICIARY 484, 487 (2014).

[26] David Nield, *The Best Weather Apps You Can Put on Your Phone*, POPULAR SCI. (May 9, 2019), https://www.popsci.com/best-weather-apps-for-your-phone/.

applications' usage and storage of their data? This Article will consider the opposition between privacy and convenience as it addresses considerations raised by the four modalities.

The remainder of this Article consists of five sections. Sections II through V discuss one of the four aforementioned modalities, and Section VI offers conclusions. Each modality discussion begins with an overview of that particular modality and describes why it is significant, with the remainder of each section reflecting on the implications of that modality.

II. THE LAW

The law is a legislative tool that seeks to eliminate the undesirable externalities of certain actions through deterrence, retribution, incapacitation, and rehabilitation.[27] The law operates by creating explicit mandates that command people to behave, or refrain from behaving, a certain way.[28] When these commands are not followed, the government can enforce the mandate by sanctioning violators.[29] Lessig summarizes the role that law plays by stating, "Law (in at least one of its aspects) orders people to behave in certain ways; it threatens punishment if they do not. . . . [The law] promises strict punishments if these orders are not followed. In this way, we say that law regulates."[30]

The government recognizes the importance of regulating smartphone applications,[31] but Congress is widely unversed in the back-end mechanics of smartphone applications.[32] Increasingly, federal lawmakers have begun to rely on congressional testimony from the application's coders and officers of smartphone manufacturers.[33] However, because these companies must often sacrifice profits to increase privacy, the objectivity of this testimony is questionable.[34]

---

[27] *See* Thomas A. Green, *Freedom and Criminal Responsibility in the Age of Pound: An Essay on Criminal Justice*, 93 MICH. L. REV. 1915, 2030 (1995).

[28] Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 507 (1999).

[29] *Id.* at 507–08.

[30] *Id.* at 507.

[31] *See generally* Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?*, N.Y. TIMES (Nov. 2, 2019), https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html.

[32] *Id.*

[33] Reed Albergotti & Tony Romm, *Apple Preaches Privacy. Lawmakers Want the Talk to Turn to Action*, WASH. POST (July 15, 2019), https://www.washingtonpost.com/technology/2019/07/15/apple-preaches-privacy-lawmakers-want-talk-turn-action/.

[34] Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-

The above issues have created a hazy legal landscape for application regulation that have all but stalled legislative innovation.[35] Some legal theorists opine that congressional inaction creates more detriment than incorrect action.[36] Given the cloudiness of application regulation, state and federal legislatures should consider the rudimentary legal doctrine of criminal law when creating application privacy regulations. In other words, Congress must consider general legislative values and translate those values into a digital world.

Criminal law seeks "to forbid and prevent conduct that unjustifiably and inexcusably inflicts or threatens substantial harm to individual or public interests."[37] Although punishment is not automatic for people who do not follow the law, the mere threat of incurring a penalty dissuades most people from violating the will of the legislature.[38] Moreover, the severity of the punishment seems to correlate with the law's efficacy.[39] Consider the differences between the criminal offenses of shoplifting and speeding. Though both crimes produce negative externalities, shoplifters tend to damage society more than speeders.[40] While it is true that speeders are more likely than non-speeders to cause severe property damage and even loss of life, the vast majority of speeders do not cause any lasting damage to society.[41] To the contrary, successful shoplifters always cause damage to society, because they deprive the shop owner of his or her property, thereby causing a tangible economic loss.[42] Accordingly, a rational state legislature would want to discourage shoplifting more than it would want to discourage speeding.

State legislatures recognize the negative externalities associated

---

phone.html.

[35] *Id.*

[36] *See*, *e.g.*, Michael J. Teter, *Letting Congress Vote: Judicial Review of Arbitrary Legislative Inaction*, 87 S. CAL. L. REV. 1435, 1446 (2014) ("Congressional inaction has led to a judicial vacancy emergency that threatens the administration of justice and has stymied enforcement of duly enacted laws, many aimed at protecting the public.").

[37] MODEL PENAL CODE § 1.02(1)(a) (AM. LAW INST., Proposed Official Draft 1962).

[38] Green, *supra* note 27, at 1923.

[39] *See* John P. Dawson, *Economic Duress—An Essay in Perspective*, 45 MICH. L. REV. 253, 267 (1947).

[40] *Compare* Dena Cox, Anthony D. Cox & George P. Moschis, *When Consumer Behavior Goes Bad: An Investigation of Adolescent Shoplifting*, 17 J. CONSUMER RES. 149, 149 (Sep. 1990), https://www.jstor.org/stable/2626807 (finding that "American consumers steal about $11.6 billion in merchandise a year"), *with Speeding*, NHTSA (last visited Feb. 15, 2020) https://www.nhtsa.gov/risky-driving/speeding ("Speeding endangers not only the life of the speeder, but all of the people on the road around them, including law enforcement officers.").

[41] *See Speeding*, *supra* note 40.

[42] Cox et al. *supra* note 40.

with speeding and shoplifting, as every jurisdiction has statutes that deter both types of behaviors.[43] However, state legislatures understand that they have limited resources to achieve such a mandate.[44] The dichotomy between punishments for speeders and shoplifters epitomizes the above limitation. While speeding violations rarely result in more than a fine, shoplifting often results in an arrest.[45] Most of society fears an arrest more than it fears paying a fine of a few hundred dollars.[46] Thus, while certain people may be willing to speed and risk incurring a fine, far fewer are willing shoplift and risk incarceration. In this way, state legislatures seek to create regulations that are the most beneficial for society.

The above example demonstrates that one well-established legal value is that we, as a society, seek to discourage theft.[47] Generally, theft occurs when one intentionally obtains the "property of another with the purpose to deprive him thereof."[48] While definitions of the crime are jurisdictionally specific, the "spirit" of laws criminalizing theft is to secure society's property rights.[49]

Property rights are vital to society because of the net social benefit that they provide.[50] Innovators who seek to develop an idea face significant risk because, in the beginning, they must provide the capital necessary to create their innovation.[51] However, for innovators, the potential profit from their innovation outweighs the risk because of the

---

[43] *See*, *e.g.*, N.C. Gen. Stat. § 20-141; N.C. GEN. STAT. § 14-72.1.

[44] *See generally* John Rappaport, *Criminal Justice, Inc.*, 118 COLUM. L. REV. 2251, 2269 (2018) (discussing the negative externalities that result from the private and public enforcement of shoplifting laws); Amanda Essex et al., *Trends in State Speed Legislation*, NAT'L CONF. ST. LEGIS. TRANSP. 3–4 (January 2016), https://www.ncsl.org/Portals/1/Documents/transportation/speed_limit_rpt2.pdf.

[45] U.S. DEP'T. OF TRANSP., NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., DOT HS 811 769, SUMMARY OF STATE SPEED LAWS, at vi—ix, (12th ed. 2012), https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/summary_state_speed_laws_12th_edition_811769.pdf; *see also Shoplifting and the Law of Arrest: The Merchant's Dilemma*, 62 YALE L. J. 788, 793–94 (1953).

[46] *See* Rappaport, *supra* note 44, at 2279–81 (explaining the consequences of arrest); Maximilian A. Bulinski & J.J. Prescott, *Online Case Resolution Systems: Enhancing Access, Fairness, Accuracy, and Efficiency*, 21 MICH. J. RACE & L. 205, 220 (2016) ("[I]n many circumstances, people unreasonably fear arrest.").

[47] *E.g.*, Saul Levmore, *Convergence and Then Downstream Divergence in Torts and Other Law*, 92 S. CAL. L. REV. 769, 769 (2019) ("All legal systems discourage theft.").

[48] MODEL PENAL CODE § 223.2 (AM. LAW INST., Proposed Official Draft 1962).

[49] *See generally* Steven J. Eagle, *The Development of Property Rights in America and the Property Rights Movement*, 1 GEO. J. L. & PUB. POL'Y 77, 89–90 (2002).

[50] *Id.* at 93.

[51] *See generally* Andrew Lee, *Intellectual Property, Moral Rights, and Social Utility: A Classically Liberal Exploration of the Normative and Practical Implications of Intellectual Property Rights*, 7 N.Y.U. J.L. & LIBERTY 431, 461 (2013).

potential legal monopoly created by a patent.[52] Such innovation would be thwarted in a world where theft is allowed, as others would simply plagiarize the innovation, and the innovator would not receive as much of a benefit.[53] Moreover, people would be dissuaded to acquire property for deprivation because the cost would be less than the cost of conventionally acquiring property. Therefore, the cost of anarchically protecting their property would diminish the value received from the property.

In applying these property values to smartphone data, the major question that legislatures must answer is how to maximize the social benefit that these applications provide, while protecting the user.[54] Smartphone applications have a positive net impact on productivity.[55] Therefore, legislatures must strike a balance between safeguarding users' data and not being too restrictive on applications so as to allow them to be useful.

One possible solution to the data collection question would be to place a blanket time limit on the length of time that applications can retain data that they collect from smartphones. Such a limitation would allow applications to collect necessary data while preventing them from creating vivid profiles of users. This limit would make the user the gatekeeper of his or her personal data, as he or she could simply refuse to allow the application to re-copy that data in the future.

A time limit is not a universal answer, however, as most applications require indefinite amounts of information to function properly.[56] Thus, legislatures must also bifurcate essential and non-essential data. Facebook, for example, would be severely burdened if a legislature enacted a blanket prohibition on retaining data obtained from a smartphone for longer than one year.[57] One of the application's

---

[52] *Id.* at 433.

[53] *Id.* at 444–45.

[54] Kenneth Einar Himma, *Toward a Lockean Moral Justification of Legal Protection of Intellectual Property*, 49 SAN DIEGO L. REV. 1105, 1120 (2012).

[55] *See* Larry Alton, *One Decade Later: Are Smartphones All Good for the Workplace?*, FORBES (June 22, 2017), https://www.forbes.com/sites/larryalton/2017/06/22/one-decade-later-are-smartphones-all-good-for-the-workplace/#4d10c9a458eb.

[56] *See* James O'Toole, *Mobile Apps Overtake P.C. Internet Usage in U.S.*, CNN BUSINESS (Feb. 28, 2014), https://money.cnn.com/2014/02/28/technology/mobile/mobile-apps-internet/; *see also* J. Clement, *Mobile Internet Usage Worldwide – Statistics & Facts*, STATISTA (Sept. 11, 2019), https://www.statista.com/topics/779/mobile-internet/.

[57] *See* Sara Ashley O'Brien, *I Downloaded 14 Years of My Facebook Data and Here's What Happened*, CNN BUSINESS (Mar. 25, 2018), https://money.cnn.com/2018/03/24/technology/facebook-data/index.html; *see also How Much Data Does Facebook Use?*, WIREFLY, https://www.wirefly.com/guides/how-much-data-does-facebook-app-use (last visited

essential features is that it allows users to post photos to the application from their smartphone's library.[58] If the Facebook application was prohibited from retaining these photos indefinitely, its users would not be able to fully construct a social media timeline.

One final consideration is the juxtaposition between the properties of tangible objects and the non-physical properties of the data contained on a smartphone. These differences will prevent legislatures from merely extending the prevailing definitions of theft into a digital context. Theoretically, data can be infinitely copied; thus, when an application obtains any data stored on a smartphone, the application is "copying" the data instead of "taking" it.[59] The smartphone's owner is not deprived of the data if it is copied in the same way that a shop owner is deprived of an item when it is shoplifted.[60] Because the data remains on the smartphone, the application has not deprived the user of his or her ability to use the data.[61] Thus, merely extending current laws against theft would not adequately protect smartphone data.

III. SOCIAL NORMS

Lessig's second modality states that legislatures should consider societal norms when creating regulations.[62] As Frank Easterbrook ruminates, "Beliefs lawyers hold about . . . new technolog[ies], are highly likely to be false. This should make us hesitate to prescribe legal adaptations for cyberspace. The blind are not good trailblazers."[63] Though comical, Easterbrook's statement emphasizes the truth about state and federal legislatures' lack of technological authority. Therefore, state and federal legislatures would be wise to consider society's perception of proper data collection when creating smartphone laws.

Like the law, social norms also regulate human behavior.[64] However, social norms distinguish themselves from the law because

---

Feb. 7, 2020).

[58] *See How Do I Take and Share Photos and Videos Using the Camera on Facebook?*, FACEBOOK, https://www.facebook.com/help/162347444215311?helpref=popular_topics (last visited Feb. 10, 2020).

[59] *See* Stuart P. Green, *When Stealing Isn't Stealing*, N.Y. TIMES, Mar. 29, 2012, at A27.

[60] *See id.*

[61] *See id*.

[62] LESSIG, *supra* note 4, at 87–89.

[63] Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207 (1996).

[64] Lawrence Lessig, *The Laws of Cyberspace*, 2, HARV. U. (Apr. 3, 1998), https://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf.

they are highly malleable and decentralized.[65] According to Lessig, "[s]ocial norms [are] understandings or expectations about how I ought to behave, enforced not through some centralized norm enforcer, but rather through the understandings and expectations of just about everyone within a particular community."[66]

At first glance, social norms may appear to be inferior to the law; however, the two concepts overlap tremendously.[67] In fact, social norms arguably control the law. Society chooses the officials who will serve on legislatures.[68] These elected officials create the law; however, society can remove officials who create laws that contradict society's understandings or expectations of proper behavior by not re-electing the lawmaker.[69]

Despite the differences between social norms and codified statutes, they both have the same effect. That is, both phenomena regulate societal behavior through a series of disincentives for those who do not conform.[70] Those who violate the law are subject to statutorily prescribed condemnation. Likewise, those who violate social norms become outcasts and suffer societal condemnation, such as rebuke, isolation, censure, or increased scrutiny.[71]

Societal norms have come to value privacy, and society labels those who seek too much information as "intruders."[72] Society is predominately unaware of the extent to which smartphone applications track users.[73] However, past events indicate that society is not content with the data collection practices of certain applications. In March 2018, the Facebook–Cambridge Analytica data scandal sparked ubiquitous outrage from society because society viewed Cambridge Analytica's data collection to be excessively intrusive.[74]

The wake of the scandal illustrates a situation where societal norms usurped the law to become the ultimate regulator. The United States Government did not take any action against Cambridge Analytica, and

---

[65] *See id.* at 2–3.

[66] *Id.* at 2.

[67] Melvin A. Eisenberg, *Corporate Law and Social Norms*, 99 COLUM. L. REV. 1253, 1254 (1999).

[68] Robert S. Summers, *How Law Is Formal and Why It Matters*, 82 CORNELL L. REV. 1165, 1173 (1997).

[69] *Id.*

[70] *See* Eisenberg, *supra* note 67, at 1255 (defining social norms as "rules and regularities concerning human conduct, other than legal rules and organizational rules").

[71] *Id.* at 1276.

[72] Bernard W. Bell, *Secrets and Lies: News Media and Law Enforcement Use of Deception as an Investigative Tool*, 60 U. PITT. L. REV. 745, 750–51 (1999).

[73] Alexander Tsesis, *Data Subjects' Privacy Rights: Regulation of Personal Data Retention and Erasure*, 90 U. COLO. L. REV. 593, 602 (2019).

[74] *Id.* at 607–08.

the Federal Trade Commission settled with Facebook for a nominal fine.[75] However, society's punishment was much more drastic, as there was a mass exodus of users and business partners from both Facebook and Cambridge Analytica.[76] The fallout of this exodus resulted in substantial harm to both companies.[77] Facebook's stock lost more than $100 billion in market capitalization in the days after Cambridge Analytica's practices became public, and Cambridge Analytica quickly filed for bankruptcy protection in the United Kingdom.[78]

The outrage surrounding the Facebook-Cambridge Analytica data scandal highlights the dissonance between the data collection that is occurring and what society deems acceptable. In creating laws to protect smartphone data privacy, legislatures should seek to align societal expectations with the actual data collection practices. The State of California moved in this direction by allowing users to become more educated on websites' usage of their information when it enacted the California Online Privacy Protection Act of 2003.[79] This Act, which is still in effect, requires websites to post a conspicuous link to the site's privacy policy.[80] (Though this is a state law promulgated by California, it is a *de facto* law nationwide. The internet's ubiquity virtually guarantees that all websites avail themselves of jurisdiction in the state of California.).[81] However, despite the privacy policy mandate, there are scant regulations that dictate what corporations must publish in their privacy policies.[82] Corporations have taken advantage of the lack of regulation in this area by constructing illusory privacy policies that allow them extensive latitude.[83]

Facebook's privacy policy is notoriously vague. The policy states

---

[75] *Id.* at 608.

[76] *See* Abinaya Vijayaraghavan & Supantha Mukherjee*, Cambridge Analytica Files for Bankruptcy in U.S. Following Facebook Debacle*, REUTERS (May 18, 2018, 2:39 AM), https://www.reuters.com/article/us-cambridge-analytica-bankruptcy/cambridge-analytica-files-for-bankruptcy-in-u-s-following-facebook-debacle-idUSKCN1IJ0IS.

[77] *Id.*

[78] Anthony Mirhaydari, *Facebook Stock Recovers All $134B Lost After Cambridge Analytica Data Scandal*, CBS NEWS (May 10, 2018, 7:56 PM), https://www.cbsnews.com/news/facebook-stock-price-recovers-all-134-billion-lost-in-after-cambridge-analytica-datascandal/.

[79] CAL. BUS. & PROF. CODE § 22575 (Deering Supp. 2018).

[80] *Id.*

[81] John Yates & Paul Arne*, Protecting Your Visitors: California's Online Privacy Protection Act Could Set Standards*, LOCALTECHWIRE.COM, https://www.mmmlaw.com/files/documents/publications/article_228.pdf (last visited Feb. 6, 2020).

[82] *Id.*

[83] Joel R. Reidenberg et al., *Ambiguity in Privacy Policies and the Impact of Regulation*, 45 J. LEGAL STUD. S163, S182 (2016).

that Facebook collects three categories of information from users: things you and others do and provide; device information; and information from Facebook's partners.[84] The policy provides users with a non-exhaustive list of examples of data that fall within each category.[85] However, the porousness of these categories leaves substantial room for interpretation and renders the policy illusory.[86] Moreover, the informal tone of the policy masks Facebook's intended usage of the data, which, as Facebook discusses in SEC filings, is to monetize the data by selling it to third parties.[87]

Facebook uses the vagueness of the policy that it created to its advantage, and it collects significantly more information than it needs to function.[88] In one study, it was determined that Facebook habitually collects every facet of information about a smartphone that the phone's framework permits.[89] However, Facebook's privacy policy fails to delineate that it collects all of this information.[90] Given the outcry from the Facebook–Cambridge Analytica scandal, it is unlikely that users of the Facebook application would willingly share this information if they knew that they were volunteering it.

The dissonance between the amount of data that Facebook collects and the amount of data users reasonably believe that it collects provokes concerns about the validity of its privacy policy. Rudimentary contract law states that a crucial component of a contract is mutual assent.[91] In other words, a contract is not valid unless the accepting party "intends to engage in the conduct" described in the contract.[92] However, "there is no manifestation of mutual assent to an exchange if the parties attach materially different meanings to their manifestations and . . . a party knows or has reason to know the meaning attached by the other."[93]

---

[84] *See generally Data Policy*, FACEBOOK, https://www.facebook.com/policy.php (last visited Oct. 28, 2019) (describing the information Facebook processes).

[85] *Id.*

[86] Reidenberg et al. *supra* note 83, at S165.

[87] Facebook, Inc., Annual Report (Form 10-K) (Jan. 31, 2019).

[88] *See generally* Dylan Curran, *Are You Ready? Here is All the Data Facebook and Google Have on You*, THE GUARDIAN (Mar. 30, 2018), https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy.

[89] Jake Kanter, *Facebook is Tracking You in Ways You Never Knew — Here's the Crazy Amount of Data it Sucks Up*, BUSINESS INSIDER (June 12, 2018), https://www.businessinsider.com/facebook-reveals-all-the-way-it-tracks-user-behaviour-2018-6; Curran *supra* note 88.

[90] *Data Policy*, *supra* note 84.

[91] RESTATEMENT (SECOND) OF CONTRACTS § 17 (AM. LAW INST. 1981). ("[T]he formation of a contract requires a bargain in which there is a manifestation of mutual assent to the exchange and a consideration.").

[92] *Id.* at § 19.

[93] *Id.* at § 20.

Thus, if Facebook knows or has reason to know that users believe that Facebook's rights under its privacy policy are substantially more limited than they actually are, Facebook, cannot rely on users assent to the policy's terms. There is caselaw supporting this hypothesis. In *In re: Telephone Infomation Needed for a Criminal Investigation*, the Northern District of California found that "subscribers cannot be said to have consented" to Verizon's privacy policy when the policy allowed Verizon unfettered ability to share subscriber information with the government and other third parties.[94]

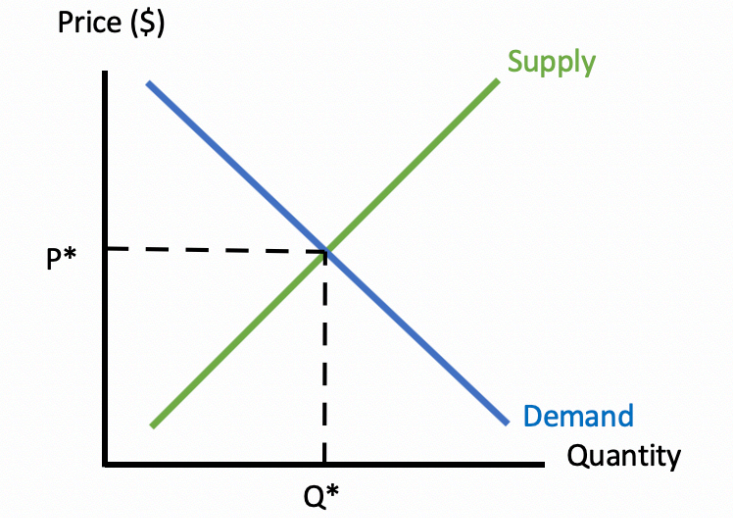
Legislatures, therefore, should aim to increase the transparency of data collection policies through lawmaking. One method that legislatures could pursue is to require applications to provide a uniform section in its privacy policy that lists every facet of information that the application intends to passively collect. This transparency would likely result in a decrease of superfluous data collection in order to avoid increased scrutiny. Additionally, legislatures could require applications to provide annual notifications of the data that they collected to users via email. Such an active publication requirement would help users to better understand the information that is collected by applications.

These regulations, which are aimed at increasing transparency, will help society understand the data that applications are collecting. As mentioned earlier in this Section, society can powerfully regulate applications by refusing to use the application and, in turn, decrease the amount of revenue that the company can generate.[95] Such regulation would force developers to tailor their data collection policies in order to avoid losing business.

[94] 119 F. Supp. 3d 1011, 1038 (N.D. Cal. 2015).
[95] *See* Viiayaraghavan & Mukherjee, *supra* note 76; Mirhaydari, *supra* note 78.

IV. MARKET FORCES

Market forces are an economic theory whereby the price of a given commodity regulates the demand and the supply of that commodity.[96] For any commodity, demand is the quantity of the commodity that consumers are willing and able to purchase at a given price.[97] Likewise, supply measures the quantity of a commodity that producers are willing and able to produce at any given price point.[98] The below diagram illustrates a typical supply and demand curve:



As the graph indicates, when the price of a commodity increases, the demand for that commodity decreases while the quantity of that commodity increases.[99] This is because fewer consumers are willing to pay for a commodity as its price increases, while producers are more willing to supply that commodity when it sells for a higher price.[100]

The supply and demand curves intersect at a central point.[101] In economics, this point is known as the equilibrium point.[102] At this point, a market price generates an equal amount of demand and supply for a product or service.[103] In the short term, transactions may occur at any point along the supply and demand curves.[104] Eventually, however,

---

[96] *Market forces*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/market%20forces (last visited Feb. 9, 2020).
[97] N. GREGORY MANKIW, PRINCIPLES OF ECONOMICS 67 (2018).
[98] *Id.* at 73.
[99] *Id.* at 68.
[100] *Id.* at 67.
[101] *Id.* at 76.
[102] *Id.*
[103] *Id.*
[104] *Id.* at 77.

the market will reach its equilibrium point.[105]

In a perfectly competitive market, there are a number of producers creating a fungible commodity, and there are few, if any, barriers to entry.[106] In these markets, there is a high elasticity of demand, because consumers can easily substitute producers and not feel much of an effect.[107] When perfect competition exists, producers cannot charge much more than it costs to create the good because, if they were to do so, consumers would quickly switch to another producer.[108] The market for nails exemplifies such a phenomena. When a consumer goes to a hardware store to purchase nails, they will likely purchase the cheapest possible box of nails, as there is hardly any differentiation between different types of nails. On the above diagram, perfect elasticity would result in a rotation of the demand curve such that it becomes horizontal. Accordingly, if a producer increases price beyond the equilibrium point, consumers will refuse to purchase its commodity.

Conversely, in a monopolistic market, there is one producer creating a unique commodity, and there are high barriers to entry (often, these barriers take the form of patents).[109] Here, there is a low elasticity of demand, because consumers who want that commodity have no choice but to buy from that one producer.[110] Thus, market forces allow the producer, in theory, to demand whatever price they choose, as consumers cannot pursue any substitutes.[111] Monopolies cause the demand curve to rotate to a vertical line on the above chart.[112] Pharmaceutical drugs exemplify typical monopolistic markets because, when the drug is protected by a patent, only a single drug exists to treat a certain medical condition.[113] Thus, consumers will theoretically pay whatever price the pharmaceutical company demands to obtain the medication.[114]

The same market forces that drive the price that a producer can charge for a commodity also drive the amount of data that an application can require from a user. The App Store and the Google Play Store

[105] *Id.*
[106] *Id.* at 290.
[107] *Id.* at 93–95.
[108] *Id.* at 93.
[109] *Id.* at 293.
[110] *Id.*
[111] *Id.* at 296–97.
[112] *Id.* at 294.
[113] Thomas G. Donlan, *Pharmaceuticals: Dangerous Monopoly of Power*, BARRONS (Aug. 11, 2017, 11:06 PM), https://www.barrons.com/articles/pharmaceuticals-dangerous-monopoly-of-power-150250716.
[114] *Id.*

contain numerous free applications.[115] Although these applications are free, the application's developers profit from collecting data and selling that data to third parties.[116] The maximum amount of data that an application can demand, however, hinges on the uniqueness of the application. Perfectly competitive applications, such as a standard calculator, cannot require more information than they need to run the application. If one downloads a calculator application and sees that they must create a profile, giving the developer their name, location, and birthday, the user will likely quickly delete the app and download a different calculator. On the other hand, monopolistic applications, such as Facebook, provide an exclusive service that cannot be replicated by other applications. These monopolistic applications can demand significantly more personal information because users will not be able to turn to substitute applications.

Legislatures should aim to prevent monopolistic applications from gathering more data than necessary. In creating regulations to curtail monopolistic data collection practices, legislatures can borrow from antitrust principles. Section 2 of the Sherman Antitrust Act of 1890 criminalizes unilateral conduct that monopolizes or attempts to monopolize a market.[117] Contrary to the statute's plain meaning, the Supreme Court has determined that Section 2 does not act as a *per se* ban on monopolies.[118] Rather, the Court has held that the Section condemns the usage of monopolistic power to increase prices or constrain output.[119]

Several applications, such as Facebook and Google, have reciprocal data sharing arrangements with many other applications.[120] One of the most ubiquitous of these arrangements is an agreement to streamline the process of logging in by allowing users to log in with their credentials from the underlying application.[121] These applications can provide this service because it enjoys substantial market power over the internet.[122]

---

[115] *See* Thomas H. Au, *Anticompetitive Tying and Bundling Arrangements in the Smartphone Industry*, 16 STAN. TECH. L. REV. 188, 190–91 (2012).

[116] Nicole Nguyen, *A Lot of Apps Sell Your Data. Here's What You Can Do About It*, BUZZFEED NEWS (May 1, 2018), https://www.buzzfeednews.com/article/nicolenguyen/how-apps-take-your-data-and-sell-it-without-you-even.

[117] Sherman Antitrust Act, ch. 647, 26 Stat. 210 (1890).

[118] *Cf.* United States v. Line Material Co., 333 U.S. 287, 309 (1948).

[119] Chi. Bd. of Trade v. United States, 246 U.S. 231, 245 (1918).

[120] Scott R. Peppet, *Freedom of Contract in an Augmented Reality: The Case of Consumer Contracts*, 59 UCLA L. REV. 676, 727 (2012).

[121] Amanda Schupak, *What Are You Sharing When You Sign In With Facebook?*, CBS (Nov. 3, 2015), https://www.cbsnews.com/news/what-are-you-sharing-when-you-sign-in-with-facebook-or-google/.

[122] *Id.*

As of July 2019, Facebook and Google had 2.375 billion and 2 billion registered users, respectively.[123] These user bases rank ahead of every other website in the world.[124] Therefore, Facebook and Google are using monopolistic power to offer this service.

Facially, it appears that harmonizing the sign-in process has pro-competitive effects because the streamlined process promotes efficiency.[125] However, the harmonized sign-in process provides the application with another opportunity to mine data about a user.[126] Thus, signing in with Facebook or Google increases the privacy price of registering a profile with either service. To remedy this anti-competitive effect, legislatures should consider banning the collection of all non-essential data from third parties that allow users to sign-in with popular social networking applications. By preventing applications from forming reciprocal data sharing arrangements, legislatures will lessen the monopolistic power of dominant smartphone applications.

V. ARCHITECTURE

Lessig's final modality considers the application's architecture.[127] By that, Lessig references "the constraint of the world as [we] find it, even if this world as [we] find it is a world that others have made."[128] For example, Lessig says:

> Smokeless cigarettes present less of a constraint [than conventional cigarettes] because they can be smoked in more places. Cigarettes with a strong odor present more of a constraint because they can be smoked in fewer places. How the cigarette is, how it is designed, how it is built—in a word, its architecture—affects

[123] *Most Popular Social Networks Worldwide as of October 2019, Ranked by Number of Active Users (in millions)*, STATISTA, https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users (last visited Nov. 29, 2019).

[124] *Id.*

[125] Larry Drebes *How Social Login Is Changing Business – and Your Privacy*, FORBES (Feb. 28, 2012 12:01 PM), https://www.forbes.com/sites/forbesleadershipforum/2012/02/28/how-social-login-is-changing-business-and-your-privacy/#41fa5b957485.

[126] *Id.*

[127] LESSIG, *supra* note 4, at 38.

[128] Lessig *supra* note 64 at 3.

the constraints faced by a smoker.[129]

Thus, this modality reflects the inherent constraints of smartphone applications. Nearly all smartphone users are constrained by others' decisions. Application developers represent a tiny subset of the global population and, therefore, a tiny subset of all smartphone users.[130] Because users do not develop the applications themselves, they must accept all of the constraints that the applications' developers create. While applications often do contain privacy settings, these are also the product of the developer.[131] Therefore, with respect to smartphone applications, users must accept applications' passive data collection techniques unless developers choose not to collect such data.

In the physical world, when a party seeks to gather information about another, the requesting party must employ active data collection methods.[132] In other words, the requesting party must ask the responding party a series of questions, and the responding party must actively provide a response.[133] Because the responding party must actively respond, the responding party knows the precise information that the requesting party seeks.[134] Moreover, the responding party can choose whether and how to respond, and the responding party knows exactly what information that they provided.[135]

Active forms of data collection are virtually unnecessary for smartphone applications, as the application's developers can code applications to automatically harvest as much data as the smartphone will allow the application to obtain.[136] Facebook, for example, uses active collection techniques when a user creates an account or edits the information displayed on their profile page.[137] The vast majority of Facebook's data collection comes from tracking user activity on the site

---

[129] LAWRENCE LESSIG, CODE: VERSION 2.0, at 123 (2006).

[130] *How Many Software Developers Are in the US and the World in 2019?*, DAXX: BLOG (Feb. 10, 2020, 5:00 PM), https://www.daxx.com/blog/development-trends/number-software-developers-world.

[131] Moshin Quadir, *National Cybersecurity Awareness Month (NCSAM) 2019: Beef Up Your Privacy With These Hidden Settings In Apps*, PUREVPN (Feb. 10, 2020, 5:00 PM), https://www.purevpn.com/blog/hidden-privacy-settings-in-apps-scty/.

[132] Brian Bagdasarian, *Conversational Data Collection: Active Data vs Passive Data*, HUBSPOT, https://blog.hubspot.com/customers/converstional-data-collection-active-passive (last updated Apr. 19, 2018).

[133] *Id.*

[134] *See id.*

[135] *See id.*

[136] *See* Michael L. Rustad, *How the EU's General Data Protection Regulation Will Protect Consumers Using Smart Devices*, 52 SUFFOLK U. L. REV. 227, 228 (2019).

[137] *See generally* FACEBOOK, https://www.facebook.com (last visited Oct. 29, 2019).

and from embedding tracking cookies into the user's operating system.[138] These tracking schemes are essentially contracts of adhesion because users must accept Facebook's architecture as they find it.

A concern that arises is how smartphone applications store and transmit the data that they collect. Just as users must accept the architecture of smartphone applications' data tracking mechanisms, they must also accept the applications' stewardship with respect to the storage of that data.[139] Because there is no standard level of security for data storage,[140] this means that users must accept an array of security levels over their data. Furthermore, it seems unlikely that smartphone applications will volitionally curtail their data collection practices.[141] Legislatures across the United States have allowed the industry to self-regulate.[142] However, self-regulation is not achieving optimal results. Therefore, state and federal legislatures must intervene with regulations.

An important factor that this Article does not consider, however, is the social cost of increasing application regulations. In order to create regulations, legislatures must allocate resources toward educating themselves about smartphone data privacy and performing the legislative process.[143] Given that time is finite, smartphone data regulations would detract from legislatures' ability to regulate in other pertinent areas. Additionally, increased regulation of smartphone applications would likely increase the cost of complying for developers.[144] Developers would likely pass this cost along to consumers in the form of charging for their applications, or by decreasing the applications' capabilities.

Legislatures must also consider the appropriate punishments for failing to conform with regulatory mandates. Given the massive revenue streams of larger developers, such as Facebook and Google, fines are insufficient. These large corporations can likely absorb any fine that regulators impose.[145] Therefore, legislatures should consider

---

[138] *See In re* Facebook Internet Tracking Litig., 263 F. Supp. 3d 836, 840 (N.D. Cal. 2017); Natasha Singer, *What You Don't Know About How Facebook Uses Your Data*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

[139] *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1138–39 (2019).

[140] *See id.* at 1136–37, 1139.

[141] Schechner & Secada, *supra* note 10.

[142] *Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy Before the S. Comm. on the Judiciary*, *supra* note 2, at 5.

[143] Albergotti & Romm, *supra* note 33.

[144] Thompson & Warzel, *supra* note 33.

[145] *See* Marie Zimmerman, *The "Big Four": Antitrust, Political Power, and Big Tech in the Twenty-First Century*, 97 DENV. L. REV. F. 200, 207 (2019) (detailing how Facebook and Google are not affected by billion-dollar fines).

criminal penalties or penalties that impose sanctions on developers' ability to operate.

Ultimately, the most efficient method of regulation appears to be societal norms. Because social norms are significantly more malleable than the law, they can adjust to society's concerns much quicker than laws can.[146] Moreover, social norms are much less socially expensive to create than laws.

Smartphone applications rely heavily on users to generate revenue for the developer.[147] As the Facebook-Cambridge Analytica scandal highlighted, users can impose significantly more punishment on developers than any government body.[148]

In order for social norms to regulate, there must be sufficient transparency for society to make informed decisions.[149] Thus, legislatures should aim to increase transparency and allow society to regulate.

There are some scholars, however, who believe that societal norms have no place in regulatory agendas.[150] In her article, *On the Regulation of Social Norms*, Dorothea Kübler indicates that social norms are far from optimal.[151] For example, in 19th century America, anti-Irish employment discrimination was the social norm, even though there was little empirical data that Irish were inferior workers.[152] Looking back, she notes that it would have been entirely inappropriate for the government to codify regulations punishing the Irish for an immutable characteristic such as their heritage.[153]

---

[146] *See* Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1248–49 (2005).

[147] *See* Hemant Bhargava et al., *The Move to Smart Mobile Platforms: Implications for Antitrust Analysis of Online Markets in Developed and Developing Countries*, 16 U.C. DAVIS BUS. L. J. 157, 171 (2016) (discussing the amount of profit Facebook was earning from advertising on its mobile app).

[148] *See supra* text accompanying note 76.

[149] *See supra* Section III.

[150] *See generally* Dorothea Kübler, *On the Regulation of Social Norms*, 17 J. L. ECON. & ORG. 449, 449–59 (2001); *see also* Kate Klonick, *Re-Shaming the Debate: Social Norms, Shame, and Regulation in an Internet Age,* 75 MD. L. REV. 1029, 1042 (2016) (stating that allowing social norms to dictate justice would lead to "anarchy"); Louis Kaplow & Steven Shavell, *Fairness Versus Welfare*, 114 HARV. L. REV. 961, 974 (2001) ("We emphasize that it would be a logical error to take the appeal of notions of fairness, which we suggest is based on their roots in social norms, as a justification for according the notions independent weight in assessing legal policy.").

[151] Kübler, *supra* note 150, at 451.

[152] *Id.* at 452.

[153] *Id.*