Privacy-Oriented Regulation
of Social Media Platforms
by
Harry Han

An honors thesis submitted in partial fulfillment
of the requirements for the degree of
Bachelor of Science
Undergraduate College
Leonard N. Stern School of Business
New York University
May 2019

Professor Marti G. Subrahmanyam    Professor Michael Posner
Faculty Adviser                   Thesis Adviser
Acknowledgements

While many people have contributed to this paper, I would like to especially thank three people:

- I would like to thank Professor Michael Posner for his insights, editing guidance, and passion for the subject area of human rights—especially for pushing myself and the rest of my BPE classmates during Senior Capstone to think beyond the numbers.
- I would like to thank Professor Marti Subrahmanyam and everyone at the NYU Stern Office of Student Engagement for organizing the program.
- Lastly, I would like to thank my friend Jennifer, who was always there for me—especially during the (rare, but) turbulent times of creating this thesis.

Disclosure

- This paper specifically discusses regulations as they pertain to the US.
- This thesis was researched and written concurrently for another course, also in partial fulfillment of my degree. As such, some portions of this paper may overlap with the mentioned paper, titled “BPE Senior Paper: Facebook’s Broken Data Privacy,” submitted 23 December 2018. Professor Michael Posner was my advisor for both papers; and Professor Marti Subrahmanyam, the faculty advisor, was aware of this concurrent research arrangement.
# Table of Contents

**Acknowledgements** ........................................................................................................... ii

**Disclosure** .......................................................................................................................... ii

I. **Introduction** ...................................................................................................................... 1
   a. Examples of Facebook’s privacy violations ........................................................................ 2

II. **Defining privacy** ............................................................................................................. 8
   a. The importance of privacy .................................................................................................. 8
   b. Privacy in a historical context ............................................................................................ 9
   c. Privacy in a digital context ................................................................................................. 10
      i. Case study of “notice and choice” ................................................................................. 13
   d. Privacy in social media ..................................................................................................... 17
      i. Economic factors .......................................................................................................... 17
      ii. Societal factors ........................................................................................................... 23
   e. Discussion .......................................................................................................................... 24

III. **Analytical methodology** ............................................................................................... 27
   a. Goals of regulators ........................................................................................................... 27
   b. Contextual integrity: A new framework for assessing privacy norms ............................... 28

IV. **Current proposals** .......................................................................................................... 31
   a. Decrease information asymmetry between the platform and the user ............................. 31
   b. Increase liability ............................................................................................................... 33
   c. Decrease incentives from aggregation ............................................................................ 36
   d. Discussion ........................................................................................................................ 38

V. **Recommendations** .......................................................................................................... 39
   a. What elements are missing from current proposals? ....................................................... 39
   b. Policy recommendations ................................................................................................ 41
      i. Increase fines .................................................................................................................. 42
      ii. Overhaul “notice and choice” .................................................................................... 42
      iii. Ban certain data mining activities ............................................................................. 45
      iv. Create a regulatory body around product-specific differences .................................... 46
      v. Help develop data portability and interoperability ....................................................... 48

VI. **Conclusion** ..................................................................................................................... 48

**Appendices** ...................................................................................................................... 53

**References** ....................................................................................................................... 56
I. Introduction

[Mark Zuckerberg]: Yeah so if you ever need info about anyone at Harvard
Zuck: Just ask.
Zuck: I have over 4,000 emails, pictures, addresses, SNS
[Redacted Friend's Name]: What? How'd you manage that one?
Zuck: People just submitted it.
Zuck: I don't know why.
Zuck: They "trust me"
Zuck: Dumb fucks.¹

Facebook was created by Mark Zuckerberg in 2004 while he was a student at Harvard University.² Since then, Facebook has grown to become the third most-visited website in the world.³ With more than 2.3 billion monthly active users, Facebook not only connects people on the internet, but its sheer scale and presence also influences how we view the physical world itself.⁴ In fact, the word “Facebook” is used interchangeably with the word “internet” in countries like Myanmar.⁵ Users publish more than a billion new posts on the platform every day, each offering a glimpse of the user’s personal life, political opinions, and even casual thoughts.⁶

However, Facebook’s incredible reach has not been entirely positive. In recent years, several high-profile scandals have highlighted how Facebook has failed to uphold its users’ expectations, or even harmed them in some cases:

⁴ Facebook Q1 2019 Results, (Facebook Investor Relations, 2019).
a. **Examples of Facebook’s privacy violations**

In 2007, Facebook launched Beacon, a program for advertisers “which would announce to a user’s friends what that user was browsing for, or buying, online.” Users were enrolled by default. “[M]any had no idea that the feature existed until it revealed upcoming holiday gifts, or, in some cases, exposed extramarital affairs.” Following intense public criticism, Facebook shut down the program in 2009.

In 2016, Facebook subsidiary WhatsApp was reprimanded in the European Union (EU) for providing users’ phone numbers and other data to Facebook without their consent. While WhatsApp has temporarily paused the data sharing program, Facebook’s recently announced plans to deepen integration between the core social media product (“Blue App”), Instagram, and WhatsApp have raised concerns for the EU’s Data Protection Commission (DPC).

“Over the last decade,” Facebook has had data sharing agreements with at least 60 electronics manufacturers and application developers—"including Apple, Amazon, BlackBerry, Microsoft and Samsung”— which gave Facebook unfiltered and preferential access to user data on “[smartphones], televisions, and other systems” with very little oversight. In addition, Facebook had granted access to “Huawei, … Lenovo, Oppo and TCL,” all of which have “a

---

7 Ibid.
close relationship with China’s government.” By the time The New York Times reported the story in 2018, only 22 of 60+ agreements had been terminated.12

In 2013, Facebook acquired Israeli data analytics firm Onavo.13 Since 2016, Facebook has operated two distinct programs:

- Onavo Protect, a consumer-facing virtual private network application that promised to “reduce their data usage, block dangerous websites, keep their traffic safe from snooping”; and
- Project Atlas, an invite-only internal program that paid 15-23-year-old users up to $20/month as part of a usage study.14

However, both these programs routed substantially all of the device’s internet traffic through Facebook’s servers without disclosure, revealing device usage information beyond Facebook’s services such as “[non-Facebook] app usage, web browsing history, web search history, location history, personal messages, photos, videos, emails, and Amazon order history.” This enabled Facebook to quickly identify popular rivals’ usage statistics and adjust its corporate strategy. For instance, “data revealed WhatsApp was sending over twice as many messages per day as Messenger … convincing Facebook to pay a steep sum of $19 billion to buy WhatsApp.” Moreover, Onavo’s data helped Facebook “discover new trends in mobile usage, keep an eye on competitors and figure out what features or apps to copy.”15 In part due to this data, for instance, Instagram launched Stories, a “near-perfect copy” of Snapchat’s Stories feature introduced three

---

years earlier.\textsuperscript{16} Within eight months, Instagram Stories overtook Snapchat Stories in daily active users.\textsuperscript{17}

As recent as 2017, Facebook allowed major services like Airbnb, Netflix, and Spotify to have broad and deep access to private user data, including powers to “read, write and delete users’ private messages.” The latter companies have publicly denied using these privileges, instead implying that Facebook was reckless in offering more privileges than necessary.\textsuperscript{18}

Since 2012, Facebook has stored “between 200 million and 600 million … account passwords … in plain text”—i.e. unencrypted and thus readable to the human eye. They remained “searchable by more than 20,000 Facebook employees,” who had requested this data more than nine million times.\textsuperscript{19} A further investigation by Facebook found that “millions of Instagram users[\textsuperscript{1}]” passwords were also stored in plaintext.\textsuperscript{20}

Until 2017, Facebook allowed advertisers to target “Jew haters,” who its algorithms had automatically identified.\textsuperscript{21} While Facebook has removed the keyword and publicly apologized after public backlash, its data mining activities continue to miscategorize users into legally protected categories in violation of differing local regulations around the world. Most recently,

\textsuperscript{16} Casey Newton, "Instagram's New Stories Are a near-Perfect Copy of Snapchat Stories," \textit{The Verge} 2016.
\textsuperscript{17} Kurt Wagner, ""Stories' Was Instagram’s Smartest Move Yet," \textit{Vox} 2018.
Facebook received criticism in Canada as its system allowed employers to post job advertisements with a specific age range, which is illegal under Canadian human rights law.22

“In 2014, the political consulting firm Cambridge Analytica sought to build psychological profiles of American voters” by purchasing profile information of 87+ million Facebook users. This trove of information originally came from a third-party personality quiz, which downloaded data of not only the ~500,000 quiz takers, but also all of their friends.23 Donald Trump’s 2016 presidential campaign then hired Cambridge Analytica to target voters by building psychographic profiles.24 According to the campaign’s digital content director, “Without Facebook we wouldn’t have won.”25 The New York Times’ report in March 2018 brought the scandal and the issue onto a national stage. Years before the scandal became public news, Zuckerberg had ironically remarked: “I just can’t think of any instances where that data has leaked from developer to developer and caused a real issue for us.”26

Introduction (continued)

Facebook has been historically against being regulated, particularly with the rise of lobbying efforts in recent years.27 However, that attitude seems to be gradually softening. Immediately following the Cambridge Analytica report, Zuckerberg called for regulations that

25 Osnos.
would require political advertisements to disclose their source of funding, while not addressing its business model at all. More than a year and many new scandals later, Zuckerberg wrote an op-ed in The Washington Post outlining four key aspects in which Facebook should embrace regulation: harmful content, election protection, privacy, and data portability.

Some critics remarked that Zuckerberg’s post was just another attempt to influence the discourse of regulating technology companies in Facebook’s favor. There seems to be some truth: Zuckerberg’s keynote remarks at the 2019 F8 Developer Conference suggesting that the “future is private” simply announced that they are shifting research and development resources to inherently private and secure applications like WhatsApp, rather than devoting attention to fixing fundamental issues related to its business model that caused the previously mentioned privacy scandals.

In each of these cases, widespread news coverage outlined how Facebook had broken the trust of its users. Despite these recurring scandals, regulators currently disagree on how to regulate social media companies like Facebook. At the very least, they seem to be taking notice starting with a monetary fine: Facebook announced it was expecting a short-term fine of approximately $3–5 billion from the Federal Trade Commission (FTC) for privacy violations, particularly related to Cambridge Analytica. There are numerous proposals ranging from introducing more user controls, increasing disclosure, undoing mergers & acquisitions (M&A), and even jailing corporate executives. However, because there are no case studies fully

---

28 Laurie Segall, "Mark Zuckerberg in His Own Words: The Cnn Interview," CNN 2018.
applicable to the unique situation of social media platforms, these platforms must be carefully and critically examined so that the government does not under-regulate nor over-regulate. This paper will therefore assess these proposals in the context of privacy.

This paper lays out its argument by answering the following three questions:

- **Defining privacy:** What is the current state of privacy in the context of social media platforms?
- **Current proposals:** What are the current proposals to regulate social media platforms, and what is missing?
- **Recommendations:** How should lawmakers instead approach regulating social media companies?

By using Facebook as a case study, this paper finds that social media platforms do not conform to the historical interpretation of privacy, nor even how online companies generally uphold privacy. In fact, this paper argues that social media platforms have a business model which places strong economic incentive on collecting and processing as much user data as possible. Bolstered by the fact that the user does not pay platforms money in exchange for their services, the platform has an incentive to always undermine individual privacy for corporate profit.

Because a fundamental transaction of social media platforms involves disclosing information for purposes of connecting with others, this paper argues that ‘privacy’ cannot be understood as a historically binary classification of ‘privacy invaded’ or ‘privacy upheld.’ Instead, this paper utilizes Cornell Tech professor Helen Nissenbaum’s contextual integrity framework to evaluate privacy norms that underpin social relationships online. By analyzing various ongoing proposals to regulate social media platforms, this paper concludes that several
analytical elements are missing: product-specific differentiation, the tradeoffs of data aggregation, and machine learning & artificial intelligence (ML & AI) implications.

II. Defining privacy

a. The importance of privacy

“in a society where modern information technology is developing fast, many others may be able to find out how we act. And that, in turn, may reduce our freedom to act as we please – because once others discover how we act, they may think that it is in their interest, or in the interest of society, or even in our own interest to dissuade us, discourage us, or even stopping us from doing what we want to do, and seek to manipulate us to do what they want to do.” -Paul Sieghart

Privacy is a fundamental human right. As Joseph Cannataci, United Nations Special Rapporteur on the right to privacy, argues, privacy is fundamentally associated with personal autonomy. By controlling others’ access to information as well as how we choose to disclose information, principles of privacy ensure that individuals can freely express their thoughts, hold beliefs without interference, freely receive and assess information, and protect critical parts of their identities like sexual orientation.

Therefore, privacy’s role in self-actualization is codified in the United Nations’ Universal Declaration of Human Rights. The loss of this privacy is devastating: As Harvard Business School professor Shoshana Zuboff posits, “If you have nothing to hide, then you are nothing.”

---

38 Emphasis added. Derek Thompson, Why Surveillance Is the Climate Change of the Internet, Crazy/Genius (The Atlantic, 2019).
b. Privacy in a historical context

Historically, privacy has been understood to be a “right to be let alone.”39 This right has been since been conceptualized as a protection against invasions of people’s private lives, whether “from snooping journalists, from nosy neighbors, [or] from advertisers.”40 In fact, as Berkeley Law professor William Prosser wrote, invasion of privacy is valid legal tort that protects people from:

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity which places the plaintiff in a false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff’s name or likeness.41

Such violations are widely recognized, allowing people to seek recourse via the courts when their privacy has been invaded. In essence, when people have complete ownership over a subject matter or place, no outsider may infringe into that space without explicit knowledge and permission. This principle were affirmed through Griswold v. Connecticut (1965), where the US Supreme Court recognized that married couples have a right to marital privacy when discussing the use of contraceptives.42 When viewed this way, privacy means restricting outsiders from learning about activities occurring within

---

40 Thompson.
private property or information concealed in a private location, such as one’s house or in a vault.

c. Privacy in a digital context

The recent rise of digital technologies has arguably clashed with the historical understanding of privacy. For companies whose primary business activity occurs online—like websites or digital platforms—a series of legal codes, precedents, and customs broadly protect behaviors that compromise user privacy.

First is the “third party doctrine.” Companies that act as intermediaries—for instance, facilitating a transaction between a buyer and a seller, or facilitating social connections between two people—are considered third parties, which nullifies the Fourth Amendment’s implied right to privacy. As initially defined in *Katz v. United States* (1967), affirmed in *United States v. Miller* (1976), and again affirmed in *Smith v. Maryland* (1979), case law in the US asserts that people have “no reasonable expectation of privacy” when private information is transmitted to a third party because they can redistribute such private information to anyone else.43 This is particularly relevant for internet companies that facilitate connections between parties. For instance, telephone networks like AT&T, internet service providers (ISPs) like Comcast, credit card companies like American Express, and social media platforms like Facebook would all

---

be considered third parties. Each of these companies can retain as much transactional data as they please, and even sell it.

Moreover, The Communications Decency Act of 1996 provided further leniency for internet companies to behave recklessly. The Act was the first comprehensive law to govern the internet. Within, §230 provided that “No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.” For years, this provision enabled internet companies to create countless digital innovations without fear of being liable for the behaviors of its users. However, this laissez-faire regulatory attitude is fundamentally incompatible with the fact that technology companies could also behave in a way that negatively affects its users. In light of developments in big data, large technology companies have amassed powers to influence millions of users with a single algorithmic or design change. Facebook has used §230 to their advantage: The provision allowed them to develop an attractive and compelling platform. However, when fake news began a conversation about the role of platforms and regulators, Facebook COO Sheryl Sandberg remarked that Facebook does not want to be the “arbiter of truth.”

---

45 For instance, see Dwyer v. American Exp. Co (1995), where American Express was able to freely sell transaction data because it was a third party which generated such records as part of business. Dwyer V. American Exp. Co, 652 NE 2d 1351 (1995).
Second, privacy invasions arising out of internet companies are difficult to prove in court, unlike physical intrusions that Prosser envisioned above. Journalist Derek Thompson provides an interesting observation: “All this surveilling and harvesting and desiccating—I don’t understand how it will actually hurt me.”\(^{49}\) In *Spokeo v. Robbins* (2016), the internet company running a “people search engine” was found not liable for damages because the plaintiff failed to prove he had suffered an “injury-in-fact” due to an incorrect listing.\(^{50}\) Therefore, for internet users seeking legal action when their digital privacy is violated, the burden of proof is much higher. For Facebook, the Cambridge Analytica scandal is not something users can directly sue Facebook for—the damage is simply not objectively quantifiable.

And third, there currently is no broad regulation about digital privacy apart from intentional intrusions like hacking. Currently, almost all data privacy regulations are “sectoral”—i.e. specific to a certain subject or demographic. For instance, the Healthcare Insurance Portability and Accountability Act (HIPPA) regulates medical information, the Graham-Leach-Bliley Act (GLBA) governs financial information; and the Children’s Online Privacy Protection Act (COPPA) governs children under 13 years old.\(^{51}\) There is no federal statute guaranteeing privacy of digitally stored information. The only relevant sectoral law is the Privacy Act of 1974, which only applies to data residing in federal agencies’ computer systems—it does not apply to private sector companies like Facebook.\(^{52}\)

---

\(^{49}\) Emphasis in audiovisual material. Thompson.


The aforementioned sectoral data privacy laws—HIPAA, GLBA, and COPPA—has only one primary purpose: controlled disclosure. These laws substantially require companies to explicitly disclose what information is being collected, how they are collected, and how they will be processed or used, so that relevant parties may elect to opt-out where applicable. Many of these necessitated disclosures are standardized across multiple intermediaries. For instance, “all HIPPA notices must have the same introductory sentence, informing readers of the purposes of the policy.”

Regulators like the FTC have applied the same standard to social media platforms: It chose to require companies to disclose their intentions rather than prescribing a minimum standard of privacy protection. Because of this disclosure, online companies are generally not legally liable for any privacy violations. This principle comes in different names: George Washington Law School professor Daniel Solove calls it “notice and choice,” while Scott Bender calls it “take it or leave it.”

i. Case study of “notice and choice”

The current system of “notice and choice” is grossly incompatible with how digital companies operate today. I observe four major drawbacks to the current approach:

First, privacy policies are unnecessarily long. Lorrie Cranor of Carnegie Mellon University has calculated that “it would take a user an average of 244 hours per year to read the

---

53 Solove and Hartzog, 587; Waldman, 66.
privacy policy of every website she visited,” placing substantial burdens on internet users if they want to fully understand how their information will be used.\footnote{Aleccia M McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," \textit{Journal of Law and Policy for the Information Society} 4 (2008): 563; Waldman, \textit{Privacy as Trust: Information Privacy for an Information Age}, 84.}

Second, privacy policies—and even Terms of Service documents to a similar extent—are typically presented as “take it or leave it,” which users often blindly accept.\footnote{Laura Hautala, "Why It's Meaningless to Accept a GDPR Privacy Policy," \textit{CNET} 2018.} As a result, Margrethe Vestager, the European Commissioner for Competition, describes these “unbalanced” documents as follows: “It’s your data, but you give us a royalty-free global license to do, basically, whatever we want. … [T]his is what you accept without a blink of an eye when it’s digital.”\footnote{Osnos.} While not trust breaches, some companies have taken the opportunity to insert satirical Easter Eggs into these documents. For instance, Apple forbids the use of their products to develop nuclear weapons, and an online blog offered $1,000 to the first person who reported that she read the privacy policy completely.\footnote{TechTalk, 2012, \url{https://techtalk.pcpitstop.com/2012/06/12/it-pays-to-read-license-agreements-7-years-later/}; Chris Hoffman, "10 Ridiculous EULA Clauses That You May Have Already Agreed To," \textit{MakeUseOf} 2012.} This frustration to users was succinctly captured in the below comic:
Third, privacy policies are difficult to understand. Since they are legal documents, they utilize language that is difficult to comprehend for the average person. In fact, these privacy policies are freely available online as premade templates, further suggesting that badly written privacy policies are an industry norm. Moreover, because privacy policies do not require the company to disclose how its proprietary intellectual property is used, obscuring how platforms utilize user data once disclosed to them. Ultimately, companies use privacy policies as a method to avoid regulatory responsibility by obscuring how they operate.

And fourth, privacy policies can change without any prior notice. Because there is no regulation requiring prior notice or consensus approval from the users, companies can change privacy policies as often as they would like, which makes legal enforcement difficult. In one instance, Facebook users and interest groups unsuccessfully attempted to fight the platform’s

---

60 Randall Munroe, Faust 2.0, xkcd (2008).
61 Waldman, Privacy as Trust: Information Privacy for an Information Age, 66.
62 See Appendix A: Google Search for “Privacy Policy Generator.”
63 Waldman, Privacy as Trust: Information Privacy for an Information Age, 66.
64 Ibid., 84; Balkin, 1199-205.
changing privacy policy in court.\textsuperscript{65} Often, the only notice provided to users is resembles the following phrase: ‘\textit{By continuing, you agree and accept the updated Privacy Policy and Terms of Service.}’ Recently, a major wave of privacy policy updates occurred in May 2018 when the European Union’s General Data Protection Regulation (GDPR) went into effect. Because many companies updated their privacy policies at once without providing any prior notice, internet pundits began satirizing the mass notifications:

\textit{Figure 2: "We've updated our Privacy Policy"}\textsuperscript{66}

Unfortunately, the practical outcome of the “notice and choice” system is that online platforms use confusing privacy policy documents to maintain their obscurity, perpetuating the asymmetric relationship with the end user. Moreover, a website’s privacy policies are often separate documents from its terms of use, suggesting the entire industry interprets privacy as not an integral component of its operations.\textsuperscript{67}

\textsuperscript{66} Nadimir Gluten, 2018, https://twitter.com/nadimpatel_/status/999111866633871361; Munroe.
\textsuperscript{67} Solove and Hartzog, 588.
d. **Privacy in social media**

While social media platforms are also considered digital companies, they exhibit additional unique characteristics that further contradict and diminish the historical understanding of privacy. The discussion below has been split into economic and noneconomic factors.

i. **Economic factors**

Facebook’s primary revenue source is by selling advertisements on its platform. When viewed this way, Facebook is simply another medium for advertisers to reach consumers, much like newspapers.\(^68\) However, there are three major economic characteristics of social media companies that makes regulating them unique to newspapers or other internet companies: network effects, aggregation effects, and multi-sided markets.

*Figure 3: Value-Cost as Size Increases Under Network Effects*\(^69\)

First are network effects. Network effects describe the phenomenon where each incremental user increases the value of the service for all users.\(^70\) For instance, telephone and


email systems’ value to all users increase as more users use the service. Moreover, these network effects grow exponentially. As shown visually above, as the user base grows linearly, the value of the system increases exponentially.\textsuperscript{71} Social media platforms exhibit especially strong network effects because its operations are entirely digital, contrasting against other industries like telephone networks that required physical infrastructure to be built. Because social media content can freely flow over the same communication lines that carry internet videos, emails, and news, social media companies’ marginal cost to service an additional user is zero.\textsuperscript{72} Combined with the fact that there are tangible switching costs from being present on multiple platforms, users typically prefer a specific platform.\textsuperscript{73} Therefore, platforms exhibit a “winner take most” competitive dynamic, where even small differences between competitors can compound to create a near-monopolistic market structure.\textsuperscript{74} These divides are anecdotally apparent when examining the preferred social media platform for certain countries: e.g. WhatsApp is dominant in India, Line is dominant in Japan, and KakaoTalk is dominant in South Korea.\textsuperscript{75} This points to the conclusion that social media companies have a strong strategic to increase its user base as much as possible. For years, Facebook employees ended their meetings by chanting “domination!”, reflecting the importance of leveraging network effects.\textsuperscript{76}

Second is aggregation effects. Many scholars often do not distinguish between network effects and aggregation effects. If network effects describe the incremental user value simply as a function of the number of users, aggregation effects describe the incremental user value as a

\textsuperscript{73} Eisenmann, Parker, and Van Alstyne.
\textsuperscript{74} Ibid.; Parker, Van Alstyne, and Choudary.
\textsuperscript{75} Cam MacMurchy, "A Closer Look: Apple’s Troubles in China Grow as Wechat Undermines Iphone’s Appeal," 9to5Mac 2019.
function of data supplied and analyzed. Particularly for social media platforms, vast amounts of personal information can be easily collected, aggregated, then analyzed to derive behavioral patterns. Just like network effects, aggregation powers also grow exponentially. With increased data input, the algorithms are able to derive deeper insights about user behaviors. Therefore, social media platforms have an incentive to collect a higher quantity of data (i.e. deeper tracking), as well as collect information from a wider array of sources (i.e. new forms of tracking). Even if users were able to place a monetary valuation to their personal data, social media platforms would always value the same data at a higher value due to aggregation effects.

In essence, aggregation effects allow companies to correlate multiple sources of information to generate new data about its users. Below is one such example:

1. **Case study of Target’s data mining**

In 2012, The New York Times published a piece about Andrew Pole, a statistician who worked for Target. By combining Target’s internal customer data alongside publicly available information—a customer’s visit patterns, purchase habits, product preferences, payment methods, address, education level, marriage status, etc.—Pole was able to create a statistical model which accurately predicted whether a woman was pregnant so Target could send baby-related marketing materials. This is important because shopping habits are difficult to change once they are formed. Only major life events, such as a new baby, trigger shoppers to change

---

79 Ibid., 45.
80 Ibid., 45-46.
their habits. Target hired Pole out of rational economic decision-making: By investing in a method to detect pregnancies early, Target got a head start in convincing new parents to shop with them.

However, in one instance, Target’s targeted advertising campaign upset the father of a young girl, who lamented: “My daughter got [these coupons] in the mail! She’s still in high school, and you’re sending her coupons for baby clothes and cribs? Are you trying to encourage her to get pregnant?”

It later turned out that the girl was indeed pregnant—she simply had not told her father yet. On one hand, Target was able to accurately predict a pregnancy by analyzing seemingly separate and public pieces of information, which reflects the immense power of big data.

**Economic factors (continued)**

And the third are multi-sided markets. Social media platforms operate three-sided markets that effectively marginalizes user power. Most platforms serve two-sided markets. For instance, Uber’s platform connects two sides: Drivers and riders. Each side of the market has ‘skin in the game’ due to the fact that money changes hands from one side to another. Because each side is responsible for the wellbeing of the other, Uber has an incentive maintain the platform such that drivers and drivers have mutual respect for the other, which in this instance is enforced through both driver and rider ratings. However, Facebook operates what Ben Thompson posits is a three-sided market:

- Users use the service for free, who disclose personal information and generate data;

---

84 Thompson.
• Content providers who upload content for free, driving publicity for themselves; and
• Advertisers, who pay Facebook for users’ attention (i.e. advertisement slots in the News Feed and elsewhere)

The key difference between Uber and Facebook is that the user does not pay Facebook for its services. Therefore, Facebook’s top incentive is to ensure that its advertising revenue is maximized, because its profitability is solely dependent on their revenues. Because advertisers pay Facebook based on quantifiable engagement metrics, Facebook’s innovations tend to encourage as much personal information disclosure as possible:

As soon as users sign up for Facebook, they are prompted to invite their non-user friends via email. The main page is an infinite “News Feed” which shows posts alongside how that user’s friends have interacted with each post. This information is presented before the actual content in bold font. This news feed has been increasingly optimized to prioritize friends and families’ interactions to drive “active engagement”:

---

85 "Privacy, Sharing, and Trust: The Facebook Study."
86 Osnos.
These changes make each post more relevant to the user, prompting reciprocal interaction. Over time, Facebook engineers were able to identify specific behavioral cues that encouraged users to spend time on the platform, like sending emails “saying that someone has uploaded a picture of them.”\(^{88}\) Even sponsored posts or advertisements deceptively begin with a statement of how many of the user’s friends have liked the brand, which deceptively portrays advertisements as genuine posts.\(^{89}\)

In turn, Facebook is able to utilize this user data to create unique features like suggesting tags, interest groups, and events. These interactions very closely mimic human socialization.\(^{90}\) By leveraging these tactics, Facebook reported in 2014 that it captures 3 petabytes (PB), or three

---

\(^{87}\) Emphasis added. The image is a replication of Waldman, "Privacy, Sharing, and Trust: The Facebook Study," 224.

\(^{88}\) Osnos.

\(^{89}\) Waldman, "Privacy, Sharing, and Trust: The Facebook Study."

\(^{90}\) Waldman, *Privacy as Trust: Information Privacy for an Information Age*, 67-69.
million gigabytes, of new data every day. In context, the sum of all information housed within American academic research libraries account for approximately 2 PB.

**ii. Societal factors**

While social media was originally intended to digitize existing social relationships, these platforms have since grown to affect many other aspects of society.

For instance, social media has become an integral tool for civics and law enforcement. In particular, successful political campaigns such as Barack Obama’s 2008 US Presidential Election campaign, Donald Trump’s 2016 US Presidential Election campaign, as well as Hong Kong’s 2016 legislative elections demonstrate the power of social media in engaging voters and influencing election outcomes. In another example, many law enforcement agencies have begun augmenting their investigations with social media information with success.

On the other hand, social media companies have increasingly demonstrated that its algorithms can isolate users’ perspectives as they are shown increasingly homogenous content that conforms to their existing viewpoints. For instance, research published by MIT following

---

the 2016 US Presidential Election demonstrates that many users only see content that is consistent with their existing beliefs.95

In extreme cases, social media can also be weaponized. Recognizing the potential for social media platforms to influence significant events like elections, Sri Lanka has blocked access to social media websites following its recent terrorist attacks on 2019 Easter Day, while India has blocked suspicious numbers from spreading false or misinformation during the 2019 Parliamentary Elections.96 And the most pertinent example is China, whose government exerts significant control over how social media platforms are run. The government has prescribed an extensive list of keywords that are banned, and even uses profile data to assign a “social credit score.”97

e. Discussion

The effectiveness of an advertisement is dependent on two factors: how effectively the advertiser provides content that matches the platform’s demographics, and the platform’s ability to identify subsegments within its user base to serve advertisements to. Early internet pioneers discovered that relevant advertisements perform at a much higher rate than generic ones.98

Therefore, social media platforms appealing to every type of user must develop and maintain its competitive advantage by developing ways to effectively categorize its users.

This incentive to granularize behavioral insights can lead to a dangerous erosion of privacy as it pertains to personal autonomy. Empirically, the trend has started since the 1950’s. The rise of consumerism after World War II drove companies to manipulate people into buying “largely wasteful conveniences and unnecessary, ultimately unsatisfying, packaged goods of all kinds.” To promote this new culture, companies significantly increased their reliance on advertising to differentiate brands while promoting aspirational lifestyles.99

To make advertising more effective, companies turned to surveillance as the preferred means of gathering information about target audiences.100 This is where privacy and profit became a zero-sum game: Data is increasingly seen as a commodity that companies could use as ‘raw material’ to turn into profit.101

Zuboff calls the eventual outcome “surveillance capitalism.”102 Surveillance capitalism is especially prevalent for social media platforms like Facebook. Because Facebook is provided free of charge to users and funded by advertisers, privacy advocates are quick to point out that ‘If you are not paying for something, then you are the product.’103 Embedded within this statement is a tradeoff: In exchange for being able to connect with family and friends, users must disclose details about their lives which platforms will use for profit.

Internally, Zuckerberg has remarked that privacy was ‘no longer a social norm,’ implying that users would sacrifice their privacy regardless of what Facebook’s policies were.104 In fact,

---

100 Ibid.
102 Zuboff.
103 Will Oremus, "Are You Really the Product?," *Slate* 2018.
104 Osnos.
Cambridge Analytica whistleblower Brittany Kaiser declared, “Privacy doesn’t exist in a post-Facebook crisis era.”

In an era where increasing parts of our lives become networked, privacy advocates and pundits often decry that “privacy is dead.” They evoke Jeremy Bentham’s panopticon, where a single person—the platform, in this instance—can observe what every person in a circular building is up to.

However, it is also clear that privacy violations have a real chilling effect for the rest of society. While the exact harm may not be quantifiable or measurable at the individual level, social media platforms’ business models centered around pervasive information gathering and surveillance implies that the harms of scandals like Cambridge Analytica are not concentrated at the individual level, but rather a consequence society suffers as a whole. In a situation where society is collectively harmed, regulations are appropriate. Moreover, it is clear that for sharing-oriented social media platforms like Facebook, strictly interpreting privacy as the “right to be let alone” is critically flawed: How could voluntary social media posts be possibly anonymized or done with the intention to “be let alone”?

Therefore, privacy within social media platforms must be examined from a different perspective—one which incorporates the principles of personal autonomy but also recognizes the unique nature of these platforms.

---

106 See e.g. Christopher Mims, "Privacy Is Dead. Here’s What Comes Next," The Wall Street Journal 2018; Selinger and Hartzog.
108 Thompson.
III. Analytical methodology

a. Goals of regulators

Cornell University professor Tarleton Gillespie remarks that the analytical scope of regulating social media companies should be separated into two: “governance of platforms” and “governance by platforms.”\(^{109}\) Currently, platforms try to regulate themselves through ‘best practices,’ which are sets of behaviors or standards that corporations have defined themselves. While this is useful for establishing a direction for future regulations, they are not fundamentally held accountable to the same extent as explicit laws. For instance, platforms stress that they have the “power” to regulate activities occurring within the platform, while they also stress that they do not have the “responsibility” to do so.\(^ {110}\) The result is platforms acting only when convenient, rather than upholding a baseline of principles.

Unfortunately, lawmakers have given wide credence to social media platforms’ best practices. In one hearing, Senator Lindsay Graham asked Zuckerberg to “submit to us some proposed regulations,” which would effectively solidify the social media platform’s own way of thinking.\(^ {111}\) This heightens the risk that these best practices are codified into formal regulations.\(^ {112}\)

Recognizing that lawmakers may be influenced by the platforms themselves, it is important to set clear goals that regulations must address. Based on the analyses conducted above, there seems to be three critical goals. An effective regulation must therefore ultimately address these concerns:

---


\(^{110}\) Ibid.


• Decrease information asymmetry between the platform and the user;\textsuperscript{113}
• Increase platforms’ liability for privacy violations; and
• Decrease platforms’ economic incentives from aggregation.

b. **Contextual integrity: A new framework for assessing privacy norms**

As New York Law School professor Ari Waldman notes, there is a privacy tradeoff that occurs “as a matter of course” when using social media platforms, because users must disclose personal information for the service to properly function.\textsuperscript{114}

Therefore, reconciling the two seemingly opposing goals—upholding privacy while ensuring that users benefit from digital social networking—requires a new method of analysis. Rochester Institute of Technology professor Evan Selinger writes that “Informational privacy is a tenuous, revisable, ongoing discussion expressed in debates between individuals, groups, and institutions about how to set and enforce norms.”\textsuperscript{115} Defining privacy around such norms is arguably critical to shaping the regulation of these platforms.

In fact, users openly express that there are different social contexts, even within a single service like Facebook. University of Virginia professor Sid Vaidhyanathan points out that for social media platforms like Facebook, its method of organizing “Friends” does not accurately reflect how users organize their social relationships in real life. Facebook simply uses algorithmic processing to suggest new connections and posts—however, users have complicated classifications in their real lives that Facebook cannot fully mimic.\textsuperscript{116} For instance, many users

\textsuperscript{113} Parker, Van Alstyne, and Choudary, Ch. 8.
\textsuperscript{114} Waldman, *Privacy as Trust: Information Privacy for an Information Age*.
\textsuperscript{115} Selinger and Hartzog.
\textsuperscript{116} Vaidhyanathan.
want to separate their professional connections from their personal connections. Depending on
the application, users draft different comments. And depending on the occasion, users behave
differently.

Much like a political litmus test, norms of informational privacy are therefore highly
context-dependent. Therefore, finding the optimal balance of privacy and convenience is a
complicated procedure. To standardize the analytical approach, this paper will use Cornell Tech
professor Helen Nissenbaum’s “contextual integrity” (CI) framework, which posits that privacy
is the “appropriate flow of information.”¹¹⁷ When information flows from one party to another
according to pre-agreed principles, the resulting interaction heightens trust, benefits both parties,
and upholds privacy.

Nissenbaum contends there are five attributes associated with every information flow.
For instance, when someone authorizes a wire transfer at her bank:

- **Data subject**: A banking transaction.
- **Sender of data**: The ‘home’ bank.
- **Recipient of data**: The ‘recipient’ bank.
- **Data type**: The customer’s identification information, amount to be transferred, and
  when to execute.
- **Data transmission principle**: Personal information should only be disclosed via an
  official channel (e.g. SWIFT) and should only be used to conduct the transaction
  being requested. A log of the transaction, including information such as transacting

---

parties in addition to minimally required information about the customer, may be retained for a predetermined period of time known to the customer. All other information must be destroyed.

A privacy violation would occur if any of these five areas were modified without knowledge or consent of the parties involved. For instance, if the banking customer’s financial information were transmitted through an unencrypted and unofficial connection, her privacy would have been violated.

Using the CI framework, examples of previously mentioned Facebook scandals could be classified into unauthorized expansions or modifications of the following five CI attributes:

- **Data subject**: Users voluntarily uploaded data for social connectivity purposes, but the data was used for election influence campaigns or corporate M&A strategy.
- **Sender of data**: Facebook became the sender of personal information to unauthorized or unknown parties.
- **Recipient of data**: Third-party data brokers became a recipient of personal information. Personal information and usage habits were published to unauthorized people, transferred to a corporate parent, or handed over to political consulting firms.
- **Data type**: Without explicit authorization, electronics manufacturers gathered deep device-level information.
- **Data transmission principle**: Users’ activity on Facebook were promised to be kept secure but was transmitted, and millions of passwords were not kept encrypted.

This simple classification exercise shows that Facebook has violated every single CI attribute over the years. While they may not have been legally liable, every violation previously
mentioned shows a severe mismatch between user expectations and corporate motivations. In fact, every single violation was capable of affecting the company’s bottom line.

Therefore, evaluating regulatory proposals using the CI framework requires a careful assessment of how they will mitigate the risk of social media platforms continuing to mine user data for their economic gain.

IV. Current proposals

This section will evaluate approximately ten regulatory proposals relating to social media platforms. They have been categorized according to the three policy objectives as outlined above. A condensed and tabularized form of this section can be found as Appendix B: Tabularized Proposals.

a. Decrease information asymmetry between the platform and the user

In July 2018, Senator Mark Warner proposed to introduce a transparency bill that would require platforms to regularly disclose any new ways that previously disclosed information would be used, as well as the estimated monetary value of such data.118 In some ways, Facebook is already making progress through user-friendly disclosure prompts such as “Why am I seeing this ad/post?”119 This proposal would be effective in informing users of how platforms are processing the data into inferences, and would potentially increase the frequency in which users can choose to opt-out. Under the CI framework, this proposal would make the transmission principle much more explicit to users, decreasing the opportunity for platforms to deviate and

---

119 Catherine Shu, "New Facebook Tool Answers the Question ‘Why Am I Seeing This Post?’," TechCrunch 2019.
violate informational privacy. However, companies would likely oppose the requirement to obtain repeated permissions for processing old, existing data. In addition, companies would likely oppose assigning and disclosing a monetary value for user data since it would compel users to view usage of the platform as ‘transactional’ and thus impact how freely they use the platform. Zuboff also suggests that regulations should pay higher scrutiny to algorithmically generated data as a result of processing submitted data.¹²⁰

Senator Warner has also proposed to adapt the ‘first party consent’ requirement from the EU’s GDPR, where data collection and processing would only be allowed if the user has explicitly authorized it.¹²¹ This means companies would no longer be able to acquire, process, nor sell user information without obtaining the user’s explicit permission first. Under the CI framework, this proposal would introduce strict restrictions on creating new transfers or widening the recipient pool of already authorized transfers. This proposal would be effective in eliminating scandals like Cambridge Analytica, arguably the most egregious violation of digital privacy, where data was transferred without permission. Within weeks of the Cambridge Analytica scandal starting, Facebook has permanently cut ties with third-party data brokers, which suggests that the company recognizes the risk of having data being mishandled outside its own infrastructure.¹²² However, this proposal does not address the potential abuses from data aggregation, which is discussed below. In fact, because such regulations will have an unintended effect of decreasing competition, social media platforms would likely accept this proposal. Once

¹²⁰ Zuboff.
¹²¹ McCabe.
platforms obtain permission from users, they may be able to infinitely collect and process data even if no third-party was allowed to access them.

b. Increase liability

In April 2019, Senator Elizabeth Warren proposed a regulation that would hold corporate executives personally liable—including jail time of up to one year for the first offence—for any federal statute that the company breaks. While companies are already required to follow local laws, this proposal effectively makes the company’s agents—i.e. executives—personally liable for their subordinates’ actions. This proposal is intended for companies with greater than $1 billion in revenue and where the infraction affects more than 1% of the US population. While intended to hold companies more accountable to their actions by increasing the cost of legal violations, because the proposal does not provide a specific goal, it radically increases the likelihood that social medial platforms introduce preemptive censorship. The risk is that social media platforms overcorrect by restricting what activities may take place within the platform. Therefore, the CI framework seems somewhat inapplicable for this proposal. The result is not encouraging appropriate information flows—but rather, platforms redesigning themselves to decrease the variety of activities users may do.

In April 2019, British regulators introduced a sweeping proposal to regulate harmful content online. It “targets a wide array of web content, including child exploitation, false news, terrorist activity and extreme violence,” while also raising the possibility that corporate executives would face personal liability when platforms fail to police their own platforms. This proposal seems consistent with Zuckerberg’s proposal of introducing harmful content regulations

123 Emily Stewart, "Elizabeth Warren Wants Ceos to Go to Jail When Their Companies Behave Badly," *Vox* 2019.
applicable to the entire internet—not just for social media platforms. When assessing the adoption of this proposal in the US, developing a consistent standard for what constitutes ‘harmful’ content would require significant discussion. In addition, this law must be balanced against §230’s principle of ensuring that intermediary providers are not held liable for the publications of its users. Under the CI framework, this proposal creates a new exempt data category which would have rules separately prescribed. Assuming that platforms’ content identification systems sufficiently improve over time, this proposal would enable users to more freely express their thoughts on these platforms.

On a similar note, in April 2019, Australia enacted a new law that amends the country’s criminal code to hold internet infrastructure, hosting, and content providers criminally liable when they fail to remove records or streams of “abhorrent violent material” online.124 This law “applies to all parts of the [internet] stack”—regardless of a company’s involvement in spreading the information, it would be held liable.125 For instance, if a video stream of a terrorist act were watched by some user elsewhere, the ISP that enabled the connection would be one of many companies held criminally liable. While this law attempts to increase the cost of allowing harmful content to spread on the internet, practical implementation would likely be impossible. Similar proposals are also underway around the world, such as in France and Singapore.126

For several years, Yale Law School professor Jack Balkin has proposed to classify social media platforms as “information fiduciaries,” which would impose a duty of care for users’

---

personal information, much like how investment advisors have a fiduciary duty.\(^{127}\) While defining this reasonable duty of care would be left up to regulators, and must be done so in a way that does not spark preemptive censorship; Balkin’s proposal is broadly compatible with the current sectoral approach to data privacy in the United States. Under the CI framework, personal user information would be subject to a new data transmission principle with clear and codified consequences for violations. Social media platforms would likely agree on the principle of upholding user data, but would likely disagree on the enforcement mechanism, likely contending that their current system of self-policing is adequate. Rather the introducing a unique law that would classify platforms as fiduciaries, regulators should instead strengthen protections against unauthorized transfers or sales of data when drafting a first-party consent rule. A more comprehensive implementation may be possible after industry norms begin changing.

Similarly, in March 2019, Senator Warren proposed to classify many platform companies—not simply in social media—as “platform utilities,” barring them from becoming an active participant within its own platform which would grant an unfair financial advantage.\(^{128}\) For example, Warren’s policy would ban Apple from listing its own apps on the App Store because such apps would not be subject to its own commission rules. However, Facebook’s business model does not require users to pay for its services, which makes this proposal inapplicable for free-to-use social media platforms. However, regulators should recognize that the role of social media platforms are blurring. For instance, Facebook’s algorithms notably affect what content, advertisements, and recommendations are shown to a user’s News Feed—

---


\(^{128}\) Elizabeth Warren to Team Warren, 2019, https://medium.com/@teamwarren/heres-how-we-can-break-up-big-tech-9ad9e0da324c.
this would imply that Facebook’s role and influence in facilitating social connections are much greater than what it portrays as simply maintaining a “digital town square.”

c. Decrease incentives from aggregation

In March 2019, Senator Warren proposed to revoke and undo major technology M&A transactions. For example, she has called for Amazon and Whole Foods to be broken up, as well as Facebook and Instagram. Chris Hughes, a cofounder of Facebook, called for a similar breaking up of Facebook. While this approach has been historically effective in breaking up capital-intensive monopolies like telecommunications and oil, this approach fails to account for the network and aggregation effects previously discussed. Under the CI framework, this proposal seems to prevent companies from widening the data recipient attribute by acquiring other companies or developing new products. However, as noted previously, social media platforms are unique because both network and aggregation effects. In fact, by breaking up social media companies, society may lose benefits that arose from having insightful data sources interconnected. Moreover, the newly split entities would have the exact same economic incentive to collect and process personal information, which does not solve other problematic aspects of social media, like harmful content. However, one potential benefit of Senator Warren’s proposal may exist under a very limited circumstance: If the products are fundamentally incompatible. For instance, WhatsApp’s messaging platform is end-to-end encrypted, which

129 Statt.
130 Warren.
does not allow Facebook to gather nor retain any information about its users. In that context, WhatsApp could become an independent company again without much impact to Facebook.

In March 2019, Zuckerberg proposed that digital companies work to make user data interoperable.\textsuperscript{133} This effort is already underway: Several high-profile technology companies—including Google, Microsoft, and Facebook—have started The Data Transfer Project, whereby user data would be containerized and therefore easily transportable from one service provider to another.\textsuperscript{134} By doing so, the project aims to encourage industry-wide innovation: If users can freely pick their preferred platform, companies would succeed based on responsible innovation. This challenges the CI framework’s assumption that data is fixed in place: By granting users the power to transfer information between providers at any time, the proposal aims to increase users’ relative power against platforms. However, there is a major drawback: While the proposal outlines how data can be transferred from server to server, it does not address how existing information flow permissions are affected once the transfer occurs, or what happens to ML/AI algorithms once the input data is deleted. It remains unclear if the incumbent platforms like Google and Facebook would be materially affected by this project as their exiting pools of data enable superior ML algorithms. The result is an effective entrenchment of incumbents.

Lastly, while not a singular policy proposal, various privacy researchers have proposed modifications to data processing that would collectively decrease the ability for data to individually identify users. For instance, anonymization and differential privacy procedures ensure that ML/AI models are effective when analyzing aggregate data but ensures that no individual identity may be identified.\textsuperscript{135} Under the CI framework, these minor proposals do not

\textsuperscript{133} Zuckerberg Mark Zuckerberg: The Internet Needs New Rules. Let’s Start in These Four Areas.
\textsuperscript{134} “Data Transfer Project Overview and Fundamentals,” (Data Transfer Project, 2018).
influence any of the five attributes of information flow. However, such measures decrease the harms arising out of unintended data breaches like hacking. While regulators would face pushback when attempting to verify and audit that these statistical safeguards have been implemented into social media platforms’ proprietary systems, the requirement to obfuscate user data seems reasonable for future product developments. Moreover, such anonymization would better enable academic researchers to obtain data about online users.

d. Discussion

From this analysis, it seems that there is no single regulation that would perfectly address every problem of social media platforms. While some proposals suggest small but meaningful steps to ensure that users are more informed about how their digital experience is created, others suggest a structural overhaul that would disrupt the industry as a whole.

Moreover, not all proposals were specific to social media companies. Several proposals targeted digital companies generally, others were completely irrelevant to social media companies entirely.

And lastly, these proposals do not consider many ways in which social media platforms would oppose regulation. Ranging from reluctant agreement to vocal opposition, platforms would likely object to many of these proposals without a compelling reason to accept—or at least a promise that their financial stability is not threatened.
V. Recommendations

a. What elements are missing from current proposals?

In general, I believe many of the above-mentioned proposals aim to regulate internet companies with a sledgehammer-approach rather than recognizing that appropriate regulations are highly context-dependent, just like when defining privacy.\textsuperscript{136} Therefore, I posit regulators should further incorporate the following factors when drafting legislation: product-level differentiation, aggregation powers, and artificial intelligence & machine learning.

The first overlooked factor is product-level differentiation. The CI analysis revealed that users have specific expectations of privacy depending on the context. These context-specific expectations extend to social media, as well. For instance, users have a different expectation of Facebook when they are conducting a 1:1 private conversation compared to when posting a picture for friends to see. Regulations should incorporate the differences in the core conduct of these applications when drafting legislation. There are countless ways to create metrics in which social media platforms can be differentiated, but I contend Thompson’s two-axis model is sufficiently succinct: Companies should be classified according to (1) the intended audience size, between one-to-one and one-to-many; and (2) the intended duration of record, between ephemeral and permanent.\textsuperscript{137} While the exact placement of various services may vary, below is one adaption of Thompson’s idea:

\textsuperscript{136} Metaphorical comparison to a sledgehammer adapted from Ben Thompson and James Allworth, \textit{166 — Fence-Building Vs. Axe-Wielding, Exponent} (Stratechery, 2019).

This distinction is important because designing and enforcing the same regulation without regard for the conduct of various online applications may stall innovation. For instance, designating WhatsApp as a platform utility seems appropriate because the vast majority of communications occurring on the platform are intended to be 1:1 and private in nature—while the Blue App should be free to incorporate various features like Groups and Events into a user’s News Feed without regulatory hindrance.

The second overlooked factor is the power of aggregation. Like network effects, aggregation effects increase exponentially despite a linear increase in input data. Therefore, regulators should design regulations that explicitly increase scrutiny to firms that possess more data. The only proposal that assigns such weight is Senator Warren’s proposal to regulate firms with greater than $1 billion in annual revenue. However, revenue figures are, at best, loosely

---

138 For some hypothetical scenarios, see Lev Aretz and Strandburg, § VI-B.
139 Ibid.
140 Warren.
correlated with the amount of data a firm possesses. A more effective regulation may require internet companies with a specific threshold of users to report the volume of data that they possess on users. Such standards should also be regularly adjusted to account for macro-landscape changes: For example, ‘the top quartile of the number of internet users that connected to a social media service in the last year.’

The last overlooked factor is ML and AI. Even if proposals that allow data portability and data erasure are enacted, they do not sufficiently address the underlying algorithms that analyze user data. Essentially, no proposal addresses the fact that the underlying algorithms remain intact despite transfer or erasure of user data. Therefore, regulations should ensure that artificial intelligence algorithms are regularly adjusted or reconciled to account for users that have terminated their accounts.¹⁴¹

b. Policy recommendations

Because this a rapidly evolving field with little prior case studies, drafting an effective regulatory framework will involve extensive trial and error, including shifts in power that may disadvantage the companies themselves. However, these missing elements and policy goals are ultimately constrained by how effectively the government can coerce companies to implement changes. I therefore contend that an ideal regulatory transformation should combine ideas, implementation timelines, and cooperation from multiple proposals.

To that end, I present five recommendations, in increasing difficulty and implementation duration, for policymakers currently drafting regulations for social media platforms:

i. Increase fines

The first is to increase the magnitude of fines when privacy violations occur. Using Facebook as a reference point, its stock surged to add tens of billions of dollars in market capitalization despite announcing that it was expecting a $3–5 billion fine. This suggests that investors expected a higher fine.\textsuperscript{142} As a comparison, Facebook’s 2011 consent decree with the FTC regarding privacy violations has placed monetary damages at $40,000 per user per day.\textsuperscript{143} This ceiling should either be enforced in its entirety, or the ceiling should be further increased.

ii. Overhaul “notice and choice”

While the current implementation of notice and choice does not sufficiently protect user privacy, moderate reforms could significantly decrease information asymmetries between the user and the platform. I advocate for three immediate changes:

The first is to eliminate the “take or leave it” language when signing up. For instance, Facebook’s sign-up page explicitly notes that by signing up, users are agreeing to its policies wholesale. On the other hand, Twitter allows users to choose whether to allow the company to analyze their usage habits in exchange for customizing the user experience:

\textsuperscript{142} Jon Swartz, "Facebook Stock Is up Because Its Earnings Report Was Mostly Positive," \textit{Barron’s} 2019.
\textsuperscript{143} Marguerite Reardon, "Facebook's Ftc Consent Decree Deal: What You Need to Know," \textit{CNET} 2018.
Simply introducing a discrete stage where users must click “I agree” is insufficient in fixing the status quo. Instead, similar to visiting an optometrist, a clear visual comparison should be presented so users have a visual understanding of how their experience will change. Such graphical representations would overcome the human tendency to skip over written privacy policies.\textsuperscript{146}
The second is to eliminate vague descriptions on existing privacy controls. Many companies use vague language like ‘Provide, personalize and improve our Products’ to justify extensive data collection, much like how many application updates on Apple’s App Store simply state “we regularly update this app.”147 Privacy policies should be updated to include specific examples of what kind of information is collected and how it is specifically used—not merely the outcome that the company is attempting to achieve.

The third is to develop a standard format for presenting privacy policies across all websites. Much like what the Truth in Lending Act did for credit card disclosure statements, having a consistent format across every website will allow users to be more informed about where and why they are giving consent.148

As shown above, recent versions of Facebook’s Data Policy document has begun providing clearer examples in plain language of how data may be collected and why they are used—“to provide a more tailored and consistent experience”150—but does not include specific descriptions of what information is collected, such as the frequency of clicks, time spent on a particular post, or the relative weights of likes or comments. These collection parameters should be prominently featured when users begin using the service, rather than buried inside legal documents.

iii. Ban certain data mining activities

The third is to impose a blanket ban on certain data mining activities. Certain demographic attributes are already well-defined and legally protected in many local jurisdictions—e.g. age, race, sex—and thus can be easily implemented as such attributes can be excluded from ML algorithms. Moreover, sensitive user information must never be allowed to leave the social media platform’s server network without two conditions being present: (1) there

---

149 “Data Policy”.
150 Ibid.
is explicit knowledge and consent from the user consistent with Senator Warner’s proposal, and
(2) the third party also pledges to uphold the same standards consistent with Balkin’s proposals
of being a fiduciary to user data. Such approval process should be standardized at all social
media companies: Private application programming interface (API) access that Facebook created
for its preferred partners should be banned.

To help ensure that the company is in compliance with these rules, the government could
require that companies larger than a certain revenue or userbase threshold appoint a special
privacy-compliance officer to oversee all internal operations.

iv. Create a regulatory body around product-specific differences

As mentioned previously, almost every social media platform has differing privacy
norms. Therefore, the regulatory framework should incorporate these differences. To do this, the
FTC should establish an office where regulators would designate several permanent ‘categories’
where applications’ primary conduct would determine how they are regulated. For instance, no
data mining should occur for applications that facilitate 1:1 private conversations like WhatsApp,
while aggregation would be more permissible for News Feed posts which are intended for a large
audience. For instance, regulators could quickly fine Facebook if WhatsApp began somehow
reading conversation data and serving ads within conversations, while questionable violations
such as manipulating suggested friends lists could be escalated to a dispute resolution unit within
the FTC.

151 Balkin, "Information Fiduciaries and the First Amendment."; McCabe.
152 Appointing a privacy officer is not new. See e.g. Paul M. Barrett, "Tackling Domestic Disinformation: What the
Social Media Companies Need to Do," (NYU Stern Center for Business and Human Rights, 2019); Cecilia Kang,
Even Zuckerberg seems clearly aware of this product-specific privacy norm distinction: He has repeatedly described Facebook’s Blue App and Instagram as a “digital town square,” while describing Facebook Messenger and WhatsApp as a “digital living room.”\textsuperscript{153} To echo this distinction, this reform should especially be stringent when boundaries blur between applications, such as between Facebook’s ‘Blue App,’ Instagram, and WhatsApp. In fact, certain functions are already blurring: Despite being a one-to-one encrypted messenger, WhatsApp is facing increasing scrutiny because harmful content and misinformation are spreading to users within the platform.\textsuperscript{154} If the company aims to use user data from one application to influence the user experience of another, such activity should require active first-party consent, in addition to a graphical new prompt informing users of how data will be transferred between services to enable integration features.

\textit{Figure 11: Mockup of New Feature Permission Prompt}

---

\textsuperscript{153} Statt.
\textsuperscript{154} Williams and Kamra.
v. Help develop data portability and interoperability

As explained above, the introduction of a secure way to transfer user information between multiple platforms would uphold network and aggregation benefits while incentivizing companies to develop responsibly innovative products. The same principle has worked for telephone number portability, and implementing the same for user data may see the same benefits.155

To enable this, regulators should establish a task force which will help guide the development of a common data container. Once the standards have matured, small and big companies alike will be able to compete for user trust, which will act as a check against incumbents. Because this process is currently very undefined, regulators should examine the work of The Data Transfer Project to develop a complete vision for an interoperable future.

VI. Conclusion

Social media platforms have a privacy problem. Ever since The New York Times reported on the Cambridge Analytica scandal in March 2018, much public scrutiny has been focused on uncovering other ways where social media platforms have violated users’ privacy, with a particular emphasis on Facebook’s conduct.156

In light of various proposals by lawmakers to regulate social media platforms like Facebook, this paper aimed to answer three guiding questions:

• Defining privacy: What is the current state of privacy in the context of social media platforms?

---

156 Rosenberg, Confessore, and Cadwalladr.
Current proposals: What are the current proposals to regulate social media platforms, and what is missing?

Recommendations: How should lawmakers instead approach regulating social media companies?

A legal precedent analysis showed that the notion of privacy is ever-evolving. While initially defined as the “right to be let alone” against invasions of private spaces and activities, which is also a valid tort claim. However, this principle of privacy seems grossly inadequate for not only social media platforms, but also internet companies broadly. Internet companies enjoy much protection from legal liability arising out of privacy violations because they are considered a third party, §230 of the Communications Decency Act does not hold providers liable for the content of its users, and because there is no sectoral law related to digital privacy consistent with US legal traditions.

The paper further found that the current system of “notice and choice” for personal information disclosure online, while implemented in a similar spirit as HIPPA, GLBA, and COPPA, is severely inadequate in decreasing the information asymmetry that exists between the user and the company. These privacy policy documents are unnecessarily long, do not allow for partial acceptance (“take it or leave it”), use complicated language, and can change at any time. The net effect is that the vast majority of internet users do not consult the document, nullifying any conscious efforts to protect privacy.

---

157 Brandeis and Warren; Prosser.
158 Katz V. United States; United States V. Miller; Smith V. Maryland; "Section 230 of the Communications Decency Act"; Solove and Hartzog; Waldman, Privacy as Trust: Information Privacy for an Information Age.
159 Balkin, "Information Fiduciaries and the First Amendment."; Hautala; Hoffman; McDonald and Cranor; Osnos; Raphael; Solove and Hartzog; TechTalk; Waldman, Privacy as Trust: Information Privacy for an Information Age; "A Statistical Analysis of Privacy Policy Design."; "Privacy, Notice, and Design."
Moreover, social media platforms further undermine the historical understanding of privacy because they exhibit unique economic and noneconomic attributes. Platforms have strong network effects which create a “winner take most” competitive dynamic. Additionally, social media has strong aggregation effects which incentivize as much data collection as possible, particularly because the value of data as used as an input for machine learning & artificial intelligence algorithms increase exponentially. Platforms also operate multi-sided markets, which is further complicated for social media platforms because users do not pay at all. This creates an incentive mismatch for the platform to collect as much data as possible, aggregate and analyze them to derive behavioral insights, then sell them to advertisers for profit without consulting the user. Lastly, social media platforms also have a strong role in shaping the physical world, where Facebook was instrumental in influencing numerous high-profile elections in addition to being synonymous with the internet itself in some countries.\textsuperscript{160}

In light of these privacy-undermining characteristics, it is easy to declare that “privacy is dead.” However, an important insight comes from the fact that disclosing personal information is a fundamental part of using social media—i.e. a privacy tradeoff occurs “as a matter of course.” Thus, a new way to analyze privacy was necessary. In addition, privacy norms vary widely across different contexts. Therefore, this paper proposed the use of Helen Nissenbaum’s “contextual integrity” (CI) framework which posits that privacy is the “appropriate flow of information.”\textsuperscript{161}

\textsuperscript{160} “How Uber Star Ratings Work for Driver-Partners”; Eisenmann, Parker, and Van Alstyne; Fisher; Jorgenson; Lev Aretz and Strandburg; MacMurchy; Moon; Osnos; Parker, Van Alstyne, and Choudary; Roose; Thompson Defining Aggregators; Waldman, Privacy as Trust: Information Privacy for an Information Age; "Privacy, Sharing, and Trust: The Facebook Study," Case Western Reserve Law Review 67 (2016); Zuboff.

\textsuperscript{161} Mims; Nissenbaum; Oremus; Osnos; Selinger and Hartzog; Vaidhyanathan; Waldman, Privacy as Trust: Information Privacy for an Information Age.
Using the CI framework, approximately ten proposed regulations were assessed against how they would affect company operations and how users would experience change. For lawmakers, this is the first substantial chance to regulate a big, problematic industry. Case-by-case discretion is important, but many proposed policies seem to apply stringent, sledgehammer-style rules to all companies regardless of their business operations. The analysis showed that there was no single regulation that would address all problems inherent in social media platforms’ business models, nor any single regulation capable of quickly solving problems. Therefore, this paper presented five major recommendations with differing implementation timelines to ensure that social media platforms are acclimated into a robust regulatory framework.

The paper recommended that social network platforms should first face higher fines for breaking existing regulations. The paper then recommended that the current “notice and choice” system be overhauled to include explicit opt-in, visual comparisons, and clear language. The paper then recommended banning certain data mining activities which have varying legal statuses in multiple jurisdictions. The paper then recommended to establish a new regulatory framework for governance which incorporates product-specific privacy norms. The paper then concluded by recommending that the government assist private sector companies to develop an interoperable data containerization strategy, which would encourage smaller competitors to enter, while incumbents would face competition to innovate responsibly.

This topic is rapidly evolving. It is possible that this paper’s recommendations become outdated soon after publication. However, this paper contributes to the ongoing dialogue about privacy because it provides a detailed, analytical account of why social media platforms have an
incentive to collect, mine, and sell personal data; uses a novel way of privacy analysis into the realm of public policy; and recommends a series of steps to regulate social media platforms.
Appendices

Appendix A: Google Search for “Privacy Policy Generator.”

The search results in approximately 500 million results.

---

162 Google, "Search for “Privacy Policy Generator”.

---
## Appendix B: Tabularized Proposals

<table>
<thead>
<tr>
<th>Goal</th>
<th>Proposal</th>
<th>Positive</th>
<th>Negative</th>
</tr>
</thead>
</table>
| **Decrease information asymmetry between the user and the platform** | Disclose how data is used & how much it’s worth | • Increase opportunities to opt-out  
• Increase costs of modifying CI | • If done wrong, same as status quo |
| | Explicit first party consent (∴ no more 3rdParty DB’s) | • Substantially decreases other CI parties that data could transmit to  
• (No repeat of Cambridge Analytica) | • Concentrates first-party aggregation  
• Platform still has incentive to conduct first-party data mining & aggregation |
| **Increase liability for mistakes** | Jail time for federal violations | • N/A: More accountability(?) | • Preemptive censorship (§230 grants ‘right’ but not ‘responsibility to’) |
| | Information fiduciary | • Compatible with sectoral nature of US regulations  
• Transparent & clear punishments  
• Higher CI principle standard | • Corporate resistance: ‘Best practices are good enough’ |
| | Platform utilities | • Establish clear CI principle  
• Ban unfair corporate practices that discourage competition | • Not applicable to all forms of social media |
<table>
<thead>
<tr>
<th>Goal</th>
<th>Proposal</th>
<th>Positive</th>
<th>Negative</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Decrease incentives from aggregation</strong></td>
<td>Undo M&amp;A</td>
<td>• Prevent unauthorized widening of CI sender/recipient net through M&amp;A</td>
<td>• Could deter benefits of aggregation unique to digital technology</td>
</tr>
<tr>
<td></td>
<td>Interoperability</td>
<td>• Encourage responsible innovation • Economic incentive to uphold CI principles</td>
<td>• Underdeveloped framework on data deletion &amp; how ML/AI algorithms are affected • Requires fundamental re-engineering</td>
</tr>
<tr>
<td></td>
<td>Anonymization</td>
<td>• Eliminate ability for algorithms to individually identify users when aggregating data</td>
<td>• Does not eliminate incentive to aggregate • Requires fundamental re-engineering</td>
</tr>
</tbody>
</table>
References


"Data Transfer Project Overview and Fundamentals." Data Transfer Project, 2018.


"Differential Privacy." Harvard University Privacy Tools Project,


Facebook Q1 2019 Results. Facebook Investor Relations, 2019.


Knockel, Jeffrey, Masashi Crete-Nishihata, Jason Q Ng, Adam Senft, and Jedidiah R Crandall. "Every Rose Has Its Thorn: Censorship and Surveillance on Social Video Platforms in China." Paper presented at the 5th USENIX Workshop on Free and Open Communications on the Internet (FOCI 15), 2015.


Shu, Catherine. "New Facebook Tool Answers the Question ‘Why Am I Seeing This Post?’." TechCrunch, 2019.


Swartz, Jon. "Facebook Stock Is up Because Its Earnings Report Was Mostly Positive."

*Barron’s*, 2019.


TechTalk. "It Pays to Read License Agreements (7 Years Later)." PC Pitstop, 2012.


———. "Understanding Facebook’s Business Model." news release, 2019,