

Copyright

by

Brian Edward Shelley

2018

The Thesis committee for Brian Edward Shelley
Certifies that this is the approved version of the following report:

**The Ability of Surveillance Capitalist Technology Firms
to Resist U.S. Government Surveillance**

**APPROVED BY
SUPERVISING COMMITTEE:**

Supervisor: _____
Huseyin Tanriverdi

Philip Doty

The Ability of Surveillance Capitalist Technology Firms to Resist U.S. Government Surveillance

by

Brian Edward Shelley

Report

Presented to the Faculty of the Graduate School

of the University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Master of Science in Identity Management and Security

The University of Texas at Austin

May 2018

The Ability of Surveillance Capitalist Technology Firms to Resist U.S. Government Surveillance

by

Brian Edward Shelley, MSIMS

The University of Texas at Austin, 2018

SUPERVISOR: Huseyin Tanriverdi

This thesis reviewed and measured the methods employed by multinational U.S.-based technology firms to resist U.S. government surveillance. A political science adaptation of Affordance Theory was used to separate methods used to resist surveillance into four affordances: legal, political, technical, and market. Review of each firms' actions provided a more granular evaluation of the motivations and impact of their choices than has been explored in existing literature.

The results showed that firms had varying levels of success across all four affordances, and certainly less success than was assumed in existing literature given their resources and influence. The legal and political affordances were both constrained and enabled in part by the firms' reliance on the U.S. government to compromise. The technical affordance was hampered by protection of data exploitative business models. The market affordance casted doubt on the ability of users to influence change via market pressures. The actions firms chose were heavily influenced by their surveillance capitalist business models predicated on mass collection and exploitation of user data. This reliance on personal data assets to drive revenue inhibited the firms' capacity as surrogate defenders of individual privacy. When firms resisted surveillance, they were often motivated by conflict of law risks or protection of international markets. To effectively resist surveillance, current firms should begin to transition business models into new revenue streams and redirect public discontent to surveillance reform rather than surveillance resistance. New firms are at a disadvantaged position, with every option to resist surveillance being either cost prohibitive or with significant inherent risk.

TABLE OF CONTENTS

Chapter I: Introduction.....	1
Chapter II: Theoretical Background and Literature Review.....	6
a. History of Surveillance.....	6
b. The Current Landscape.....	7
c. What’s at Stake?	14
d. Authorizing Legislation.....	17
e. Existing Literature Review.....	23
f. Affordance Theory Framework.....	28
Chapter III: Application of Affordance Theory.....	31
a. Methodology.....	31
b. Legal Affordances.....	33
c. Political Affordances.....	44
d. Technical Affordances.....	59
e. Market Affordances.....	70
Chapter IV: Results.....	78
Chapter V: Discussion.....	89
a. Utility of Affordance Theory.....	89
b. Firm as Corporate Avatars.....	91
c. Contributions to Remaining Existing Literature.....	92
d. Suggestions for Further Research.....	94
Chapter VI: Conclusion.....	96
Bibliography.....	97

LIST OF TABLES

Table 1: Geographic Segmentation of Revenue for Alphabet (Google) (Dollars in Millions).....	15
Table 2: Geographic Segmentation of Revenue for Apple (Dollars in Millions).....	15
Table 3: Geographic Segmentation of Revenue for Facebook (Dollars in Millions).....	15
Table 4: Geographic Segmentation of Revenue for Microsoft (Dollars in Millions).....	15
Table 5: National Security Order Requests for Apple.....	19
Table 6: National Security Order Requests for Facebook.....	19
Table 7: National Security Order Requests for Google.....	20
Table 8: National Security Order Requests for Microsoft.....	21
Table 9: Legal Affordance Outcomes for Multiple Firms.....	33
Table 10: Legal Affordance Outcomes for Facebook.....	33
Table 11: Legal Affordance Outcomes for Microsoft.....	34
Table 12: Legal Affordance Outcomes for Google.....	34
Table 13: Lobbying Disclosure Spend for the Top Firms.....	46
Table 14: Lobbying Disclosure Spend for the Reform Government Surveillance Coalition.....	47
Table 15: Revolving Door Lobbyists.....	47
Table 16: Lobbied Legislation based on Lobbying Disclosures.....	56
Table 17: Outcomes of Affordance Theory - U.S. Citizens v. U.S.-based Firms.....	78
Table 18: Outcomes of Affordance Theory - Affordance Categorizations by Firm.....	80
Table 19: Apple as a Corporate Avatar	82
Table 20: Facebook as a Corporate Avatar.....	82
Table 21: Google as a Corporate Avatar.....	83
Table 22: Microsoft as a Corporate Avatar.....	83

Chapter I: Introduction

U.S.-based platform technology firms have established a market dominance built on the exploitation of personal data leveraged to create reinforcing network effects (Manjoo 2016). The global power and influence of these firms was supported by a largely unregulated free and open internet leading to a combined market capitalization in the trillions (Wilhelm 2017). Mass data collection drives the revenue of these firms, but the risks and responsibilities associated with the use of personal data threaten their business. In 2013, many of these firms were named as participants in clandestine surveillance operations executed by U.S. intelligence agencies (Welch 2013). Implicated firms took several steps to mitigate the fallout from the disclosures to both correct the exaggerated interpretation of their involvement and demonstrate their public commitment to privacy. Despite these efforts, the previously global internet has since begun to establish borders. International markets are implementing protectionist data protection laws that restrict collection, storage, and transfer of their citizens' personal information by firms. A bifurcated global internet increases operating burdens for firms and presents conflict of law scenarios that increase liability. U.S.-based firms can only hope to navigate and adapt to the emerging global trend that is national data protection.

Exposure of U.S. government access to global personal data collected by U.S.-based firms initiated this newfound emphasis on digital sovereignty. While these firms are forced to find a balance between stakeholders, the U.S. government continues to defend its access on the grounds of national security prioritization. Firms have taken measures to resist U.S. government surveillance but have achieved mixed results despite their prominence. Presumably, globally dominant U.S.-based firms would have sufficient resources and influence to impact legislation and surveillance practices, but change has not come easily. Firms have succeeded on the margins. The U.S. government has allowed for more transparency in reporting and limited the use of non-disclosure orders. Recently enacted law provides processes for firms to refuse certain government data requests due to conflict of law situations in select countries (Daskal 2018). Encryption has prevented surveillance of data in-transit. However, more substantive limitations on U.S. government surveillance authorities have been thwarted, leading to many questions this thesis will address. Have firms simply tried and failed to more effectively resist surveillance? What methods have yielded preferred results? What limitations, if any, are holding firms back?

Existing literature takes three angles when evaluating the role of firms concerning privacy and surveillance. The first angle emphasizes the impact of firms on the surveillance environment which supports calls for a proportionate inclusion of firms within the broader surveillance conversation (Kumar 2016). Mass data collection and the replacement of traditionally surveilled communications mediums have elevated the value of firms when conducting U.S. government surveillance. This places firms in a unique position where their business models simultaneously enhance the government's ability to conduct surveillance while enhancing their own abilities to limit that surveillance (Rozenshtein 2018). This private power afforded to firms to affect public operations creates positive and negative ripple effects for both U.S.-based firms and the U.S. government. The second angle is an ideological, privacy focused approach addressing surveillance resistance relative to the relationship between firms and individuals as both citizens and users. Privacy advocates expect firms to protect individual privacy by wielding the tremendous power and influence firms attained through the exploitation of personal data. This evaluation overvalues the ability of firms to resist surveillance, and when privacy is not protected, critics chastise firms for valuing business priorities over their users. The underlying expectation that firms are obligated to their users is too often framed with little consideration of other stakeholders. Again, privacy advocates emphasize the responsibility of firms to serve their users (Cover 2015) but they don't consider how competing demands limit the firms' ability to act as surrogate protectors of individual privacy. The third angle examines the structural reliance on firms to resist surveillance on behalf of users. Legal theory and precedent limit the rights of U.S. citizens to resist U.S. government surveillance when the government requests data directly from a firm. Individual citizens lack the resources, expertise, or collective action to leverage other forms of resistance, leaving them with little recourse to protect their own privacy (Calo 2015). At best users could use market pressure to force firms to implement privacy focused features (Soghoian 2015). If users wish to enhance their individual privacy, existing literature claims that success is dependent on the involvement of firms.

This thesis aims to combine aspects of each existing literature angle into a more comprehensive evaluation of firm surveillance resistance. The surveillance resistance methods of firms have been reviewed in existing works and many of those covered will overlap with the methods reviewed in this thesis. The goal of this thesis is to review previously explored methods and build on existing findings using a more granular evaluation of those methods with consideration of competing stakeholder interests. Existing literature firmly established the pivotal role firms play in government surveillance due to their pervasiveness in everyday life.

This thesis confirms that surveillance capitalism has made firms into valuable tools of surveillance and formidable resistors of surveillance, but contends that the power and influence established through surveillance capitalism complicates the motivations of firms if and when they choose to resist surveillance. This thesis tests the efficacy of surveillance resistance methods through a closer lens by reviewing the detailed actions of firms within those methods and recording the end results. Reviewing specific actions of firms in depth revealed not only *if* firms could resist surveillance, but in what circumstances they chose to resist, what motivated them to resist, and to what degree their business models limited their resistance. Privacy advocates may expect firms to serve as third party protectors of individual privacy based on ideological and structural dependencies, but the findings of this thesis cast doubt on the mantle of firms as corporate gatekeepers. Often, surveillance resistance was motivated by the protection of foreign markets or inhibited by the dependence on exploiting personal data assets to drive revenue. Privacy advocates may interpret these findings as an abdication of the responsibility of firms to protect individual privacy, but that conclusion grossly oversimplifies the firms' complex business environment. This thesis and existing literature acknowledge that firms are not devoid of privacy focused actions. Rather, this thesis emphasizes that the surveillance capitalist business models of firms create a dynamic of competing interests that complicate the perceived incentives, risks, and consequences of each action as interpreted by firms.

To review and rate the efficacy of surveillance resistance methods, this thesis applies an adaptation of James Gibson's Affordance Theory previously used by Ryan Calo to measure the ability of U.S. citizens when resisting surveillance. Calo segmented surveillance resistance into four affordances. The legal affordance covered litigious challenges. The political affordance covered appeals to lawmakers. The technical affordance covered privacy techniques like encryption. The market affordance covered the leveraging of external market forces to enhance resistance capabilities (Calo 2015, 6-15). Each affordance group will be rated after reviewing the methods and outcomes. By reviewing and rating the efforts U.S.-based firms have made to resist U.S. government surveillance since the Snowden disclosures, this thesis can address broader questions. First, the results will reveal the capacity of firms to resist surveillance and which methods were more or less effective. The presumption that firms are well equipped to resist surveillance will be reviewed on a per affordance basis and between affordances. Second, the presumption that any failures are the result of firms' unwillingness to jeopardize business models will be confirmed or denied based on the findings for each affordance. If self-

preservation precluded firms from committing to protect the individual privacy of their users, the skepticism of privacy advocates will be substantiated.

Chapter II of this thesis covers background and existing literature to provide context prior to the affordance reviews. The background section includes the history of U.S.-based firms with government surveillance and mass data collection; metrics establishing the dominance of U.S.-based firms; market segmentation demonstrating the importance of non-U.S. markets; relevant non-U.S. data protection regulations; and an overview of authorizing U.S. surveillance legislation. The existing literature section will review available evaluations of U.S.-based firms resisting surveillance from two angles. The first angle covers the manner in which firms have resisted surveillance and the critical role they play in the broader surveillance environment. The second angle covers not only how equipped firms are to resist surveillance, but also their role as gatekeepers of individual privacy. The latter angle includes Ryan Calo's "Can Americans Resist Surveillance" that not only supports the claims of other literature that firms are most suitable to resist surveillance, but also introduces the framework used as the methodology of this thesis (Calo 2015).

Chapter III explains the methodology of this thesis in more detail, including the methods measured within each affordance, which firms will be included in the study, and the hypotheses this thesis aims to answer. Following the methodology overview, each affordance is reviewed. At the end of each affordance section, the findings are rated to measure the success or failure of firm surveillance resistance. Based on those findings, firms will also be rated on their commitment to individual privacy relative to the demands of a data driven business model.

Chapter IV summarizes the results from all four affordances. These results are analyzed and discussed in Chapter V and the methodology as a whole will be critically reviewed. Chapter VI concludes this thesis and provides suggestions for follow up research.

This thesis focuses primarily on the U.S.-based technology platform firms with relation to U.S. government surveillance, but is relevant to macro conversations covering their global accumulation of power and the evolution of societal expectations of digital privacy. The competing dynamics that complicate surveillance resistance are a microcosm for the broader tradeoffs that global markets, governments, and citizens will have to navigate when determining what the future of privacy and surveillance should be in both the private sector and the public

sector. A future that demands privacy and digital sovereignty will force firms to make substantial changes. It may be a reckoning of the surveillance capitalism that built them.

Chapter II: Theoretical Background and Literature Review

A. History of Surveillance

Apple, Facebook, Google, and Microsoft are dominant U.S.-based multinational technology firms that wield tremendous power based on the number of users, data, and capital they possess. As these firms expand into other areas of daily life, they increase the network effects that drive user loyalty, engagement, and retention; so much that opting out of their services becomes cost prohibitive to consumers (Manjoo 2016). The data collected from users of a firm's platform have become intangible capital assets with long term value (Lo and Brynjolfsson 2016). Originally, firms extracted the value of collected data assets by iterating and improving their own platform to retain current users and attract new users based on the feedback the data assets revealed. Data collection resulted in a surplus of assets, so firms like Google redirected their data assets to a market exchange like digital advertising. The value of data, particularly data that can predict or manipulate future consumer behavior, has bred a new market dynamic described by Shoshanna Zuboff as "surveillance capitalism". This new form of commerce allows firms to utilize the troves of data collected from their users to either refine predictive analytics capabilities on their own platforms, or apply those capabilities to an external market, like advertising, thereby converting users from customers to sources of valuable data assets. Surveillance capitalism incentivizes firms to expand the channels of user data collection to maximize predictive capabilities sold on the market (Zuboff 2016). User data collection and retention is fundamental to their ability to generate revenue via surveillance capitalism.

In 2013, several technology firms were implicated in assisting U.S. government surveillance previously unbeknownst to the public. National Security Agency (NSA) contractor Edward Snowden leaked classified documents including a presentation detailing direct government access to platform technology firms' servers, naming firms like Apple, Facebook, Google, and Microsoft (Welch 2013). Over the last five years, these firms have employed a variety of methods to mitigate any residual costs of being named in the disclosures while continuing to expand their power and influence. Any perceived surreptitious access to user data by U.S.-intelligence agencies places firms in a quagmire. Demands for privacy by users or governments establishes an existential threat to firms that rely on surveillance capitalism. The willingness of users to exchange their data for platform services is based on users' fundamental misunderstandings

about the exchange of their data and/or the value of their data. Users overestimate government regulation over data sharing, lack understanding of how their data is exchanged, and underestimate the value of their own data (Turow, Hennessy, and Draper 2015, 16). An event like the Snowden disclosures, which exposes privacy failings and adversely impacts user sharing behaviors or the flow and control of data across borders, undermines surveillance capitalism. At the same time, the data troves that firms collect and retain to sustain a surveillance capitalism model can be invaluable sources of intelligence for U.S.-agencies charged with protecting national security. The U.S. government exploits the global market dominance of U.S.-based platform technology firms to serve as an extension of existing surveillance capabilities. This thesis will evaluate how Apple, Facebook, Google, and Microsoft have responded to the disclosures to assuage privacy concerns while simultaneously protecting a business model predicated on widespread surveillance.

B. The current landscape

As technology and data collection become increasingly ubiquitous in daily life, global dependence on the largest and most powerful consumer technology firms will necessitate an evolution in the intersection of society, government, and technology. The largest consumer technology firms, all based in the U.S., accounted for 37 percent of gains when the S&P 500 saw record growth in 2017 (Popper 2017). In June 2017, Facebook hit a record of 2 billion monthly active users (Constine 2017). In the final quarter of 2016, Apple's iOS and Google's Android made up 99.6 percent of new smartphone market share worldwide (Vincent 2017). These dominant platforms have entrenched their ability to thrive in surveillance capitalism by establishing powerful network effects. Network effects are prolific when users participate in value creation and add value to other users. When existing users attract new users to interact on the same platform, existing users avoid social cost caused by migrating to another platform; size begets size and growth begets growth, making the incumbent firms defensible against upstarts (Currier 2017). Additionally, firms with an external market can use their network effect as a competitive advantage based on their ability to reach and retain an outsized user base. For example, by July 2017, that year's projections saw that Google and Facebook accounted for more than 60 percent of domestic digital advertising revenue and over 50 percent of global advertising revenue (Ingram 2017).

Global market dominance of U.S.-based firms is instigating several forms of government scrutiny in markets around the world. In June 2017, the European Union (EU) levied Google with a record \$2.7 billion fine for violating antitrust regulations related to price comparison search results that favored Google's own service ("The European Union" 2017). A \$122 million fine was levied on Facebook in May 2017 by EU antitrust regulators for matching identities between Facebook users and users of the newly acquired firm Whatsapp (Bendix 2017). In 2016, the EU commission ruled that Ireland provided illegal state aid to Apple in the form of a 1% corporation tax rate and forced Ireland to collect \$15 billion in back taxes ("Ireland forced" 2017). These actions demonstrate a willingness to hold prominent U.S.-based technology firms to high data protection and antitrust standards. However, regional accountability of multinational firms can also create complex conflict of law situations when applying governance to a global internet. In June 2017, the Canadian Supreme Court demanded that Google remove search results for Datalink Technology Gateways, a distributor accused of repackaging pirated equipment from the firm Equustek. Google has since filed an injunction with the U.S. District Court in Northern California claiming that removing the search results is a violation of the First Amendment (Alba 2017a). In *Google LLC, v. Equustek Solutions Inc.*, injunction relief was granted on the basis that extraterritorially forcing removal of third party content by Google violated Section 230 of the Communications Decency Act¹. Google is also resisting proposed application of the EU right to be forgotten beyond the borders of the EU. This would effectively apply EU law to non-EU countries and require the suppression of content that would otherwise be lawful (Fleischer 2017).

Concerns about U.S. government surveillance and surveillance capitalist U.S.-based firms have prompted non-U.S. governments to implement privacy focused frameworks and regulations that focus on the global nature of the internet. The EU's Privacy Shield and the General Data Protection Regulation (GDPR) address both U.S. government surveillance and surveillance capitalism. Privacy Shield is the successor to the prior Safe Harbor agreement that was invalidated following the Snowden disclosures based on U.S.-based firms' inability to protect EU citizen data from mass surveillance. The invalidation of Safe Harbor created uncertainty for firms, threatening transatlantic data flows that tech firms rely on to conduct business in the EU (Pfeifle 2015). As with the Safe Harbor predecessor, U.S.-based firms use Privacy Shield to self-certify as adequately protecting privacy under applicable EU privacy law –

¹ *Google LLC, v Equustek Solutions Inc.*, Case No. 17-cv-04207 (N.D. Cal. Nov. 2, 2017).

either the Data Protection Directive or the GDPR starting May 2018. Facebook, Google, and Microsoft utilize Privacy Shield to self-certify.

Privacy Shield improves on Safe Harbor by offering EU residents recourse to hold U.S.-based firms accountable for any non-compliance including complaint submission and reply within 45 days, cost free independent dispute resolution, and available binding arbitration if necessary (“Privacy Shield List” n.d.). When related to National Security Access, EU residents can submit complaints to their Data Protection Authority and the complaint will be reviewed and handed off to the appointed U.S. Privacy Shield Ombudsperson (“EU – U.S. Privacy Shield Ombudsman” 2017). In September 2017, the EU Commission and U.S. authorities conducted the first annual review of Privacy Shield. The commission affirmed that the regulation ensures adequate levels of protection and offered recommendations for improvement, including added protections for non-U.S. citizens when reforming U.S.-surveillance law and permanent appointments of vacant U.S. positions integral to the agreement (“EU – U.S. Privacy Shield: First review” 2017). However, Privacy Shield still faces several challenges. The Working Party 29 (WP29) representing the Data Protection Authorities of each EU member state published similar Privacy Shield concerns as the EU Commission but added a deadline of May 25, 2018 - the effective date for GDPR - for the filling of permanent Privacy Shield ombudsperson and remaining Privacy and Civil Liberties Oversight Board (PCLOB) vacancies. If the vacancies are not filled, WP29 will challenge the adequacy of Privacy Shield in national courts (Article 29 Data Protection Working Party 2017). In October 2017 the Irish High Court ruled to escalate the Irish Data Protection Commissioner’s request to Court of Justice of the European Union (CJEU) to determine if existing transatlantic data transfer mechanisms adequately protect EU citizen data from U.S. government surveillance. The mechanisms in question were Privacy Shield and the use of standard contractual clauses (SCC). SCCs are alternative data transfer agreements used by firms like Facebook and Apple that are reviewed and approved by the EU Commission (“Privacy Policy” 2018a) in lieu of, or in addition to, Privacy Shield self-certification (Meyer 2017). If the CJEU affirms the claims of the Irish Data Protection Commissioner, the use of SCCs, and potentially Privacy Shield, could be invalidated. The absence of these cross-border data transfer mechanisms may leave firms like Facebook, Google, Microsoft, and Apple with no legal mechanism for transatlantic data transfers. Five years after the Snowden disclosures, the threat of U.S. government surveillance continues to put firm operations in EU markets at risk.

The vulnerability of Privacy Shield and SCCs is further complicated by the impending EU GDPR. The GDPR replaces the Data Protection Directive ensuring EU resident rights over the access, portability, and erasure of their personal data. The GDPR also has stricter breach notification and informed consent requirements. Critically, the GDPR explicitly applies extraterritorially. Any firm controlling or processing personal data of data subjects within the EU at the time of collection are subject to GDPR compliance, even if the firm is based outside of the EU. Penalties for non-compliance are fees between 2 percent and 4 percent of global revenue, depending on the violation (“Guide to GDPR” n.d.). GDPR compliant transfer of data outside of the EU requires the use of safeguard mechanisms like Privacy Shield or SCCs. If those mechanisms are deemed inadequate and invalidated, there is a risk that transfer of EU resident personal data outside of the EU would constitute a violation of the GDPR (Determann, Hengesbaugh, and Weigl 2016). The GDPR provides EU residents consent and control protections that threaten both government surveillance and surveillance capitalist models. Informed specified use and consent requirements prohibit deceptive or ambiguous data collection and sharing practices. Disclosure, correction, erasure, and portability rights allow EU residents to control the valuable surveillance asset that is their personal data. Transfer mechanisms are required under the GDPR and current U.S. government surveillance threatens the viability of those mechanisms. The regulation’s punitive enforcement mechanisms paired with the willingness of EU regulators to hold firms like Google and Facebook accountable presents significant risk in operating surveillance based data collection in the EU.

U.S.-based tech platform multinationals are also facing operational changes in Asia. In 2017, China introduced the China Cybersecurity Law (CSL) that addresses data protection concerns that resulted from the Snowden disclosures (Gidda 2017). The CSL’s data protection requirements, like informed consent and data integrity requirements, align with other international data protection frameworks. However, the CSL is much more restrictive on cross-border data transfers. The CSL requires firms collecting Chinese citizen personal data to store data locally within China. If a firm requires transfer of personal data outside of China’s borders, the firm must undergo a security assessment prior to authorization. Although the law is currently in effect, it has not been fully implemented. A draft encryption law that is being considered would require firms using encryption technologies to provide decryption support for national security or criminal investigations (Bigg 2017). The compliance date for cross-border data transfer sections has been moved to December 31, 2018 and there are competing factions in China debating the practical application of the CSL’s broad guidelines. But as seen in the EU, the

global freedom of data movement that has benefited U.S.-based firms is being challenged. The importance of data protection in China is beyond the EU's focus on a fundamental right of privacy. China considers their citizen data as an asset akin to other natural resources and have linked data protection to national security to reflect that position (Sacks, Triolo, and Webster 2017).

China has been both an attractive market for growth and a difficult market to operate in. Firms have experienced different relationships with China. Chinese reliance on Microsoft's Windows operating system has been problematic for both China and Microsoft. Windows XP was widely used in China but highly pirated. Chinese authorities promoted Linux variants to mitigate reliance on the foreign OS. Following the Snowden disclosures, Windows 8 was banned for use by the Chinese government (Gallagher 2017). In 2014, Microsoft ended support for Windows XP to pressure users into upgrading their OS to Windows 10. This move exposed how dependent China was on an OS that was more than a decade old, resulting in public criticism and an anti-monopoly investigation by Chinese regulators that has yet to be resolved (Mozur, Wingfield 2016). Despite facing efforts to exploit or undermine Microsoft's success in China, the firm continues attempts to advance the relationship. In 2017, Microsoft partnered with a state-owned China Electronics Technology Group to develop a custom version of Windows 10 for the Chinese government (Dou, Jie, and Greene 2017).

Currently, neither Google or Facebook operate their core products in China. Facebook was blocked by the Chinese government following riots in 2009 when leaders claimed that the social media platform was used to sow unrest. Since then, Facebook has been working to regain access to China and demonstrates a willingness to make changes to appease and appeal to the Chinese government. Facebook has made several executive hires with experience in China to build relationships and navigate China's bureaucracy. CEO Mark Zuckerberg has joined Apple CEO Tim Cook and Microsoft CEO Satya Nadella on the board of Tsinghua University's School of Economics and Management, met directly with President Xi Jinping, and assigned Facebook engineers to work on tools to allow a third party, like China, to block content. Zuckerberg has described Facebook's mission as connecting the world and publicly expressed the futility of that mission without China (Abkowitz, Seetharaman, and Dou 2017).

Google has a more adversarial relationship with China. In 2010, Google discovered a cyberattack and phishing scheme originating in China that stole intellectual property and

accessed the Google accounts of human rights activists (Drummond 2010a). Following the incident, Google decided to reroute uncensored Google.cn traffic to servers in Hong Kong after four years of operating in compliance with China's censorship requirements for search (Drummond 2010b). In response, the Chinese government blocked Google's services. Google has continued to be resistant to Chinese demands. Google's mobile operating system Android exists on smartphones in China, but Google has not been able to introduce their native Play Store because the firm refuses to censor apps. The only progress Google has made in China is an introduction of its Tensorflow AI tools to attract Chinese developers. Google has devoted resources to attracting Chinese talent and establish some presence in China. However, there will still be barriers to success. Developers must host data on servers within China rather than depending on blocked Google cloud services and the Chinese government may limit the use of Chinese datasets (Minter 2017). Facebook and Google's business models (social media and search, respectively) have prevented access to a population whose active online users are twice the entire population of the United States (McKirby 2015). China has made it clear that if U.S.-based tech platforms want access to their prospective users, China will be the one to dictate the terms.

Apple's relationship with China has been deferential. The Chinese government forced Apple to shut down the iTunes and iBooks stores six months after each launched with no public explanation offered by Apple or Chinese officials (Whittaker 2016). In 2017, Apple removed the New York Times app from the App store. The New York Times website, as with sites of other western publications like the Wall Street Journal and the Guardian, were already blocked in China to restrict information that is perceived as rumor or a threat to national security (Mickle and Alpert 2017). Conceivably, users in China could access New York Times content by changing their perceived geolocation. Later that year, Apple removed 674 virtual private network (VPN) apps that Chinese citizens could use to circumvent the state firewall and censorship restrictions. In 2018, Apple moved all Chinese user iCloud data and the encryption keys for that data to a local data center run by state owned Guizhou - Cloud Big Data Industry Co Ltd. to comply with recently enacted Cybersecurity and National Security laws (Nellis and Cadell 2018). Apple's cooperation with China has drawn criticism from human rights groups and congressional scrutiny from Senators Ted Cruz and Patrick Leahy (Reisinger 2017). In response, CEO Tim Cook has espoused two rationales for Apple's cooperation with Chinese authorities. First, when operating within a country, a firm is subject to the laws of that government even if they do not

always agree. Second, it is better to participate and attempt change from the inside (Strumpf 2017).

The United States has historically been hands-off when regulating U.S.-based tech firms. The last significant U.S. data protection ruling against a U.S.-based platform technology firm was in 2011 when the Federal Trade Commission (FTC) settled an eight-count complaint with Facebook, requiring the firm to make improvements to informed user consent, changes to data sharing practices including with third parties, and obtain independently audited privacy assessments. The FTC found that Facebook had been deceptive about their controls over access to user data by third parties like advertisers or app developers. Examples of deceptive practices included allowing third party apps more access than the stated limits of data required for the app to operate, allowing access to supposedly inaccessible deleted or deactivated account content, and sharing user data with advertisers while claiming otherwise (“Facebook Settles FTC” 2011). The FTC has the ability to fine Facebook for violations but has yet to do so even though Facebook had uncovered third party access to user data without consent that prompted Facebook to restrict access allowances. Based on FTC comments on controversial third party access to up to 50 million user accounts, Facebook’s discovery of non-consensual access to data belonging to friends of consenting users was unreported and highlights the inadequacy of even the strongest example of U.S. data protection (Dolven, Thompson 2018).

In 2013, FTC staff suggested that the commission file a lawsuit against Google practices that were considered anti-competitive, but FTC commissioners voted unanimously against it (Mullins, Winkler, and Kendall 2015). The FTC’s investigation included the same search preference practices that resulted in the \$2.7 billion fine levied by the EU. Where the EU determined Google’s search practices stifled competition, the FTC determined that the same practices improved the user experience (Arthur 2013).

In 2015, President Obama described the European Union’s comparatively punitive regulations as being largely protectionist. Obama surmised that EU regulations, purportedly based on values like privacy and security, were actually roadblocks designed to minimize U.S.-based tech sector dominance (Swisher 2015).

Data protection authorities are being established around the globe, but the U.S. uses a sectoral approach to data protection that only regulates what has been prescribed as the most

sensitive data. The existing data protection laws are too focused on protecting exposure of sensitive data and less considerate of individual agency over one's own data (O'Connor 2018). The U.S.'s current approach to data protection is an ideal environment for surveillance capitalist firms to thrive. Google's Eric Schmidt once described the "online world" as "the world's largest ungoverned space" (Zuboff 2016), but the freedom that has allowed U.S.-based firms to become globally dominant is diminishing. Foreign governments recognize that their citizens' data are valuable assets necessitating modern regulations in the name of privacy, protectionism, and national security. The U.S. government was exposed as having leveraged the global market dominance of U.S.-based firms as an arm of surveillance providing foreign governments with additional urgency and legitimacy to protect their citizens' data.

C. What's at stake?

Globally, U.S.-based technology platform firms rank highly when measuring global public perception of the top 100 firms by market capitalization. Apple and Microsoft ranked numbers one and two respectively, with Facebook at number six, and Google's parent organization Alphabet at number twenty-one ("How Global Top 100" n.d.). The high financial and reputational rankings of the largest platform technology firms is not coincidental. Popularity is a reflection of the data-network-effect where firms collect as much user data as possible. This in turn helps firms refine and improve services, leading to more users, which generates additional data for improvement, and leading to even more users. Data has replaced oil as a driver for growth, incentivizing ever increasing data collection ("Data is giving" 2017). These data driven U.S.-based technology platform firms offer governments and law enforcement a rich pool of data collected globally.

The top five U.S.-based technology firms (Google, Facebook, Amazon, Apple, and Microsoft) are worth an aggregated \$3 Trillion in market capitalization (Wilhelm 2017). Fifteen of the world's top twenty-five largest technology firms are based in the U.S., with eight included in the top ten. In 2016, U.S.-based technology firms sold over \$300 billion in technology goods and services to international customers (Hodgkins III and Kallmer 2017). Apple, Alphabet (Google), Microsoft, and Facebook segment their revenue by geography in their annual Securities and Exchange Commission (SEC) filings, as seen in Tables 1 through 4.

Table 1: Geographic Segmentation of Revenue for Alphabet (Google) (Dollars in Millions):

Domestic '16	EMEA '16	APAC '16	Domestic '17	EMEA '17	APAC '17
\$42,781 (47%)	\$30,304 (34%)	\$12,559 (14%)	\$52,449 (47%)	\$36,046 (33%)	\$16,235 (15%)

Source: Form 10-K Period Ending December 31, 2017

Table 2: Geographic Segmentation of Revenue for Apple (Dollars in Millions):

America's '16	Europe '16	China '16	America's '17	Europe '17	China '17
\$86,613 (40%)	\$49,952 (23%)	\$48,492 (22%)	\$96,600 (42%)	\$54,938 (24%)	\$44,764 (20%)

Source: Form 10-K Period Ending September 30, 2017

Table 3: Geographic Segmentation of Revenue for Facebook (Dollars in Millions):

U.S. '16	Foreign '16	U.S. '17	Foreign '17
\$12,579 (46%)	\$15,059 (54%)	\$17,734 (44%)	\$22,919 (56%)

Source: Form 10-K Period Ending December 31, 2017

Table 4: Geographic Segmentation of Revenue for Microsoft (Dollars in Millions):

U.S. '16	Other Countries '16	U.S. '17	Other Countries '17
\$40,578 (48%)	\$44,742 (52%)	\$45,248 (50%)	\$44,702 (50%)

Source: Form 10-K Period Ending June 30, 2017

Based on annual 10-K SEC filings for Apple, Facebook, Google, and Microsoft, at least 50 percent of revenue for each firm was generated outside of the U.S. in both 2016 and 2017. In 2017, a combined 48 percent of Google's revenue came from the Europe, Middle East, Africa (EMEA) and Asia-Pacific (APAC) segments and a combined 44 percent of Apple's revenue came from Europe and China. U.S. government surveillance reduces trust and incentivizes strong data protection regulation - as seen in the EU, Japan, and China - that threaten the viability of significant foreign markets.

Market dominance and popularity offer a lot for firms to lose when firms are implicated in U.S. government surveillance. Apple, Facebook, Google, and Microsoft deny that the U.S.

government was ever given direct access to servers (Welch 2013a). However, the perception that the U.S. government was granted any privileged access to user data forced multiple stakeholders to respond. Non-U.S. governments threatened new regulations and penalties that could increase operating costs or loss of business (Sargsyan 2016, 2223-2225). Non-U.S. competitors leveraged public distrust to encroach on U.S. technology firm market dominance. In 2013, the Information Technology & Innovation Foundation (ITIF) projected losses to the technology industry resulting from the Snowden disclosures as high as \$35 billion by 2016. In a 2015 article revisiting the impact of government surveillance on the technology industry, ITIF predicts that the losses will far exceed those initial estimates (Castro and McQuinn 2015).

The costs incurred by U.S.-based platform technology firms are being administered internationally but changes to U.S. government surveillance is reliant on public and political will domestically. Following the Snowden disclosures, Americans expressed concern over privacy and surveillance. PEW research conducted from 2014 to 2015 showed that 52 percent of Americans were concerned about surveillance and 34 percent of those who knew anything about the disclosures had changed their communications or online activities (Rainie and Madden 2015, 3). Sixty-five percent of respondents believed there were inadequate limits to government collection of telephone or internet data. If respondents had heard a lot about the disclosures, the percentage of respondents who felt limits were inadequate increased to 74 percent. Ninety-three percent of respondents felt it was important to control who can get information about them (Madden and Rainie 2015, 4). An Anzalone Liszt Grove poll from 2014 found that 63 percent of respondents wanted more oversight over surveillance programs (Byers 2014). Concern of government surveillance from constituents inspired bipartisan support for surveillance reform (Weisman 2013) culminating in the USA Freedom Act of 2015 which reformed telephony surveillance and added requirements for additional transparency (Samee Ali and Abdullah 2016).

In the years since, the Snowden disclosures public sentiment has dissipated. Surveys conducted in late 2017 by Lawfare showed that Americans had neither strong feelings in favor or opposition to U.S. government surveillance at a time when Congress was debating the surveillance law that authorizes intelligence community access to electronic communications. Sixty-seven percent of respondents chose 'I don't know/No opinion' when asked if they favored continued authorization of the NSA and FBI to spy on overseas targets without a warrant. When asked about concern over NSA collection authorities, a majority 30.5 percent of respondents

chose the neutral '3' on a five-point scale with '1' being not concerned and '5' being very concerned. The same question replacing the NSA with the FBI yielded a majority 28.8 percent choosing the neutral '3' (Eoyang, Freeman, and Wittes 2018). Domestic apathy may have relieved political pressure to reform sun setting surveillance authorization. In January 2018 Congress voted to extend the law that authorizes NSA warrantless surveillance of electronic communications and warrantless FBI querying of the collected data without proposed reforms. The reauthorization extended the surveillance authority for six years and potentially revived the use of controversial 'about' collection that increases the potential for domestic and foreign persons to be targeted for surveillance (Matsakis 2018).

D. Authorizing legislation

U.S. government access to data collected by platform technology firms is executed through upstream and downstream collection. Upstream collection refers to collection of data in transit via the internet backbone. Downstream collection refers to government requests compelling the disclosure of consumer data from companies like Apple, Facebook, Google, and Microsoft ("End 702" n.d.). U.S. government surveillance is authorized by two statutes: Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008 and Title II of the Electronic Communications Privacy Act (ECPA). FISA 702 authorizes both upstream and downstream collection of data, requiring that the surveillance target be a foreign national located outside the United States. In addition, it requires that a significant purpose of the surveillance be for foreign intelligence information. Once collected and stored, the NSA, CIA, and FBI can query the data ("Section 702: What it is" 2017). FISA 702 does not limit the type of data collected and allows for non-content and content of communications collection. Targeting of communications is not authorized on a per target basis. The Foreign Intelligence Surveillance Court (FISC) approves the targeting procedures (Rosenzweig, Stimson, and Shedd 2016). The FISC is a sealed court which hears challenges to FISA requests and accompanying non-disclosure orders that prohibit recipients from publicly disclosing any information related to the orders. Because the court is sealed, the outcome of any challenges, or even whether or not a challenge has been attempted, are not publicly available ("Are they allowed" n.d.).

The Electronic Communications Privacy Act (ECPA) was created to protect wired, oral, and electronic communications during creation, transmission, and storage. Title I of the ECPA, known as the Wiretap Act, requires a warrant for interception of in-transit communications,

with the exception of FISA (“Electronic Communications Privacy Act of 1986” n.d.). Title II, known as the Stored Communications Act (SCA), permits government access to stored communications held by a service provider, like Google, requiring a warrant, subpoena, or court order depending on the age of information sought (Brill 2016). The SCA authorizes the use of delayed notice or non-disclosure orders that prohibit electronic communications providers from notifying the target of the request and, where applicable, the target’s home country (Crusco 2017). The ECPA also authorizes an FBI administrative subpoena known as a National Security Letter (NSL). NSLs are executed by the FBI and do not require judicial oversight. NSLs are also accompanied with non-disclosure orders prohibiting recipients from disclosing the receipt and contents of the NSL except to seek legal advice. Unlike FISA requests, NSLs have undergone some reform. The USA Freedom Act granted recipients of NSLs the ability to challenge the NSL’s non-disclosure order, prompting judicial review (“National Security Letters FAQ” n.d.). When requesting electronic communications data, NSLs can be used to obtain email addresses, screen names, billing records, and subscriber data without judicial review, but NSLs cannot be used to obtain contents of communications (“National Security Letters” n.d.).

The ECPA also restricts firms from disclosing personal data to foreign governments. If a non-U.S. government requires data from a U.S.-based firm, the foreign government cannot go directly to the firm but must instead use Mutual Legal Assistance Treaties (MLAT). The MLAT process requires review and approval by the Department of Justice. The current MLAT system is not efficient enough to reliably handle the increasing amount of requests necessitated by the ECPA restriction on disclosure (Woods 2015). This blocking provision turns U.S.-based platform technology firms’ global dominance into a surveillance advantage for the U.S. government over non-U.S. governments. All requests for data from non-U.S. governments require U.S. warrant approval from a judge, thus turning the U.S. government into a “middle man” for foreign requests when the U.S. government has no such restrictions.

FISA requests and National Security Letters are at times lumped into one categorization called “National Security Orders” (NSO) (“U.S. National Security Orders Report” n.d.). Through litigation, the U.S. government has allowed firms like Apple, Facebook, Google, and Microsoft to release transparency reports that include NSO request statistics. Tables 5 through 8 show the number of NSO received and the number of impacted accounts from the NSO requests. The U.S. government allows for two disclosure methods. Facebook, Microsoft, and Google opted to break NSO into types - FISA requests and National Security Letters - which restrict the data into larger

reporting blocks of 0 – 499. Apple opted to report NSO as a single category which allows for smaller reporting blocks of 0 – 249. Reporting is on a six-month delay.

Table 5: National Security Order Requests for Apple

Year - Half	NSO Requests	Accounts Affected	Declassified NSL
2014 - H1	0 - 249	0 - 249	0
2014 - H2	250 - 499	0 - 249	0
2015 - H1	750 - 999	250 - 499	0
2015 - H2	13,250 - 13,499	1,000 - 1,249	0
2016 - H1	2,750 - 2,999	2,000 - 2,249	0
2016 - H2	5,750 - 5,999	4,750 - 4,999	1
2017 - H1	13,250 - 13,499	9,000 - 9,249	0

Data Source: "Report History" Privacy Accessed on 2017 Sept 28

<https://www.apple.com/privacy/transparency-reports/>

Table 6: National Security Order Requests for Facebook

Year - Half	NSL Requests	Accounts Requested
2014 - H1	0 - 499	0 - 499
2014 - H2	0 - 499	0 - 499
2015 - H1	0 - 499	0 - 499
2015 - H2	1 - 499	1 - 499
2016 - H1	0 - 499	0 - 499
2016 - H2	0 - 499	0 - 499
2017 - H1	0 - 499	500 - 999

Table 6: National Security Order Requests for Facebook (continued)

Year - Half	FISA Content Req.	Accounts Req.	FISA Non-Con Req.	Accounts Req.
2014 - H1	0 - 499	7,000 - 7,499	0 - 499	0 - 499
2014 - H2	0 - 499	7,000 - 7,499	0 - 499	0 - 499
2015 - H1	500 - 999	13,500 - 13,999	0 - 499	0 - 499
2015 - H2	500 - 999	13,500 - 13,999	0 - 499	0 - 499
2016 - H1	500 - 999	13,000 - 13,499	0 - 499	0 - 499
2016 - H2	500 - 999	12,500 - 12,999	0 - 499	0 - 499
2017 - H1	Not Yet Reported	Not Yet Reported	Not Yet Reported	Not Yet Reported

“Req.” = Requested

Data Source: “National Security Requests for Data” Government Requests Report Accessed on 2017 Sept 28 <https://govtrequests.facebook.com/country/United%20States/2013-H2/>

Table 7: National Security Order Requests for Google

Year - Half	NSL Requests	Accounts Requested
2014 - H1	500 - 999	500 - 999
2014 - H2	0 - 499	500 - 999
2015 - H1	0 - 499	500 - 999
2015 - H2	1 - 499	500 - 999
2016 - H1	0 - 499	500 - 999
2016 - H2	0 - 499	1,000 - 1,499
2017 - H1	0 - 499	1,000 - 1,499

Table 7: National Security Order Requests for Google (continued)

Year - Half	FISA Content Req.	Accounts Req.	FISA Non-Con Req.	Accounts Req.
2014 - H1	500 - 999	17,000 - 17,499	0 - 499	0 - 499
2014 - H2	500 - 999	18,500 - 18,999	0 - 499	0 - 499
2015 - H1	500 - 999	19,000 - 19,499	0 - 499	0 - 499
2015 - H2	500 - 999	22,500 - 22,999	0 - 499	0 - 499
2016 - H1	500 - 999	25,000 - 25,499	0 - 499	0 - 499
2016 - H2	500 - 999	35,000 - 35,499	0 - 499	0 - 499
2017 - H1	Not Yet Reported	Not Yet Reported	Not Yet Reported	Not Yet Reported

“Req.” = Requested

Data Source: “United States national security requests” Transparency Report

Accessed on 2017 Sept 28

https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US

Table 8: National Security Order Requests for Microsoft

Year - Half	NSL Requests	Accounts Requested
2014 - H1	0 - 999	0 - 999
2014 - H2	0 - 999	0 - 999
2015 - H1	0 - 999	0 - 999
2015 - H2	0 - 499	0 - 499
2016 - H1	0 - 499	0 - 499
2016 - H2	0 - 499	0 - 499
2017 - H1	0 - 499	0 - 499

Table 8: National Security Order Requests for Microsoft (continued)

Year - Half	FISA Content Req.	Accounts Req.	FISA Non-Con Req.	Accounts Req.
2014 - H1	0 - 999	19,000 - 19,999	0 - 999	0 - 999
2014 - H2	0 - 999	18,000 - 18,999	0 - 999	0 - 999
2015 - H1	0 - 499	15,500 - 15,999	0 - 499	0 - 499
2015 - H2	0 - 499	17,500 - 17,999	0 - 499	0 - 499
2016 - H1	0 - 499	12,000 - 12,499	0 - 499	1000 - 1999
2016 - H2	0 - 499	13,000 - 13,499	0 - 499	0 - 499
2017 - H1	Not Yet Reported	Not Yet Reported	Not Yet Reported	Not Yet Reported
2017 - H2	Not Yet Reported	Not Yet Reported	Not Yet Reported	Not Yet Reported

“Req.” = Requested

Data Source: “U.S. National Security Orders Report” Corporate Social Responsibility”

Accessed on 2017 Sept 28

<https://www.microsoft.com/en-us/about/corporate-responsibility/fisa>

Reporting in blocks was a compromise firms made due to the government’s concern that reporting requests to the individual would threaten national security. Compromise aside, reporting in blocks still benefits firms because it provides observers with a more informed perspective on the U.S. government’s access compared to the speculation that followed the Snowden disclosures. The above reporting dispels the notion that the U.S. government was offered unfettered, clandestine backdoor access to user information. Even at their highest volume, the blocks of data requests are infinitesimal compared to the user totals of these four dominant firms.

From an individual privacy perspective there are two aspects of the reporting that are notable. First, the 0 - 249 and 0 - 499 block ranges could reflect that a firm received zero NSO requests or up to 499 requests. These block ranges may contain the same amounts of requests as the higher block ranges, but their inclusion of zero means it is impossible for observers to know if a firm went six months without receiving a single NSO. Second, the growth in reporting data over the three and a half years covered is significant. Using the top end of each block, firms saw tremendous increases in NSO surveillance in the years since the Snowden disclosures. Apple’s NSO requests increased from 249 to 13,499 as seen in Table 5. The number of accounts impacted by Facebook’s FISA requests increased from 7,499 to 12,999 as seen in Table 6. The

number of accounts impacted by Google’s FISA requests increased from 17,499 to 35,499 as seen in Table 7. Microsoft was the only firm whose reporting decreased as seen in Table 8.

The growth in NSO requests, lack of judicial oversight, and the frequent use of non-disclosure orders with NSO has resulted in increased scrutiny from privacy advocates, including calls for reform and legal challenges. As the dominant platform technology firms increase their market control and fortify their network effects to collect more and more data, there is an expectation that the use of personal information as an asset obligates firms to protect the source of that valuable resource. The Electronic Frontier Foundation publishes an annual review titled “Who Has Your Back”. The review grades technology firms’ policies and actions concerning government data requests with the expectation that firms “stand up for user privacy” (Reitman 2017a). But as powerful as Apple, Facebook, Google, and Microsoft may be, their ability to resist U.S. government surveillance to protect user privacy is not as simple as choosing to “have their user’s back”. Multinational firms have multiple stakeholders, often with competing interests, to consider. The power and influence of firms is built on mass collection and exploitation of the very data that privacy advocates and users feel deserve protection. It may be presumptuous for privacy advocates and users to appoint technology platform firms as guardians of privacy. The ability of U.S.-based platform technology firms to operate in international markets has been jeopardized by U.S. government surveillance. Foreign governments have recognized that firms fueled by surveillance capitalism require constraining laws with significant penalties to protect the privacy of their citizens. The threat of increasingly restrictive international regulations is a potentially major motivating factor when firms establish policies and positions on U.S. government surveillance, especially considering that more than 50 percent of annual revenue for Apple, Facebook, Google, and Microsoft is generated from international markets. The motivations of firms are central to this thesis. Is the ability of firms to resist surveillance driven by an ideological obligation to users or is it due to pressure from outside stakeholders holding firms accountable for the protection of user privacy?

E. Existing Literature Review

In the years since the Snowden disclosures, existing literature has covered the role of technology firms when resisting surveillance from various angles.

In Corporate Privacy Policy Changes during PRISM and the Rise of Surveillance Capitalism Priya Kumar focused on the nine firms that were named in the leaked NSA PRISM documents, plus Twitter, to examine how firms adapted after their involvement in U.S. government surveillance was made public. Kumar studied the changes made to each firm's public privacy policy since the disclosures to determine if firms were becoming more privacy focused to resist surveillance or inadvertently enhancing government surveillance capabilities by expanding surveillance capitalist capabilities. Based on the changes between pre-Snowden and post-Snowden privacy policies, Kumar found that firms expanded their collection and use of personal data assets. This prompted Kumar to call for more involvement of firms in public conversations over U.S. government surveillance given their power and role as an implicit arm of U.S. government surveillance (Kumar 2016, 63-69).

Alan Z. Rozenshtein's *Surveillance Intermediaries* answered Kumar's call by comprehensively evaluating the role that U.S.-based platform technology firms play as third party participants in government surveillance described by Rozenshtein as "surveillance intermediaries." Rozenshtein emphasized the centrality of surveillance intermediaries to modern day surveillance based both on the digital replacement of traditionally surveilled communications and the enhanced capabilities that ubiquitous mass data collection offers the government. Traditional communications, like postage mail and telephone calls, have given way to the rise of email, chat, and social media that is controlled and operated by surveillance intermediaries like Apple, Facebook, and Google. To Rozenshtein, these surveillance intermediaries are not only uniquely equipped to resist surveillance, but unlike legacy communications firms, have proven willing to do so. Rozenshtein covered a broad range of techniques used by surveillance intermediaries described as "proceduralism," litigiousness, technological unilateralism, and policy mobilization. These techniques demonstrated the multifaceted capabilities at the disposal of surveillance intermediaries that systematically alter the surveillance environment and reinforce the centrality of firms to U.S. government surveillance. Throughout his evaluation, Rozenshtein focused on the impact surveillance intermediaries had on the broader surveillance environment, including intragovernmental checks on surveillance and an ideological discussion of the power held by surveillance intermediaries. Ultimately, Rozenshtein assessed the quasi-sovereignty of surveillance intermediaries and the duality of their influence both enhancing and limiting U.S. government surveillance (Rozenshtein 2018, 99-189).

In *Corporate Avatars and the Erosion of the Populist Fourth Amendment*, author Avidan Cover explored the capacity of technology firms to serve as ‘corporate avatars’ for individuals. As ‘corporate avatars,’ firms would act as surrogate defenders of individual privacy by challenging U.S. government surveillance practices and asserting constitutionally protected rights on their users’ behalf. The necessity of a ‘corporate avatar’ is rooted in case law establishing the third party doctrine. The third party doctrine states that individuals who voluntarily provide their information to a third party are no longer entitled to Fourth Amendment protection because that information is no longer considered private. The gravity of the third party doctrine is elevated by an environment where access to essential electronic communications services necessitates the forfeiture of personal data. Mass data collection by firms paired with the third party doctrine forces firms into a position where they can be either a guardian of privacy rights or an agent of U.S. government surveillance. Cover was concerned that firms would be reluctant to challenge the U.S. government to protect their surveillance capitalist business models. Cover noted that taking a position that emphasized the rights of users over the access and use of their personal data could draw attention to technology platform firms’ own commodification of personal information and invite regulation. If the data collection that fuels surveillance capitalism is hindered in the service of being a corporate avatar, Cover’s concerns may be valid. Cover concluded that the corporate avatar dynamic is ineffective in practice and lamented that technology firms would only be worthy avatars if their financial priorities aligned with consumer demand for individual privacy (Cover 2015, 1444-1502). An illustrative example of this is the use of encryption. Unlike litigation or legislation, firms have the freedom to implement encryption without any reliance on a third party for permission or support. The use of in-transit encryption protects individual privacy by limiting the value of upstream surveillance without negatively impacting surveillance capitalism. In-transit encryption is an example of Cover’s conclusion that firms would only act on behalf of individual privacy when doing so does not threaten their business model. The implementation of end-to-end encryption would challenge Cover. End-to-end encryption would limit both U.S. government and firm access to personal data assets. If a surveillance capitalist firm implemented end-to-end encryption on their platform, the firm would be prioritizing individual privacy over the firm’s access to revenue driving personal data assets.

Christopher Soghoian’s article *An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government* calls for more engineering and policy decisions to limit the surveillance capabilities of the government. Soghoian viewed the

engineering and transparency policies of technology firms as methods to facilitate a competitive market where consumers would select firms based on corporate disclosure and privacy policy. Soghoian relies on the belief that user demand for privacy will be strong enough to create market incentives for firms to implement more privacy-by-design and limit disclosure to government. Suggested privacy-by-design methods include transport encryption to prevent network surveillance; end-to-end encryption where even the firm doesn't have a decryption key; and limited or zero data retention policies to reduce or eliminate the amount of data stored and available for disclosure. Soghoian believed that if firms implemented privacy-by-design, they could compete with one another over users who value privacy. By not taking a privacy-by-design approach, Soghoian believed firms were revealing that they did not value privacy as much as they have publicly expressed (Soghoian 2015). The methods Soghoian offers are so privacy focused that they potentially nullify the utility of firms as a source of data for U.S. government surveillance. However, the methods are also an impediment to surveillance capitalism. Even if users were motivated to choose firms based on privacy, the value of those users would be diminished because the lack of access to personal information limits the firm's ability to improve their own products or feed advertising models. Soghoian's belief that users would leverage market influence to promote implementation of privacy-by-design features conflicts with Cover's lack of confidence in corporate avatars. As long as firms depend on user assets to drive revenue, diminished data access is as much a threat to business as losing users. Firm needs and user needs would not be in alignment, leading to Cover's skepticism that privacy protective features would actually be utilized.

Ryan Calo's essay *Can Americans Resist Surveillance* repurposes James Gibson's Affordance Theory for legal application. Gibson's theory was originally applied to ecological psychology to study the complementarity between organisms and their environment. To Gibson, observing affordances requires understanding the relative relationship between an organism and the environment grounded in the ability of the organism to take an action, or have an action happen to the organism. Critically, Gibson felt the relationship must be observed empirically and not theoretically (Scarantino 2003, 949-955). Calo's essay applies this ecological framework as a legal framework by studying the observed affordances of U.S. citizens in their ability to resist surveillance through four affordance methods - legal, political, technical, and market. The U.S. citizen serves as the organism operating in an environment of surveillance governed by existing U.S. legal structures. Calo's essay concludes that U.S. citizens have available affordances to theoretically resist surveillance, but his empirically backed observations reveal these

affordances to be ineffective. Legal affordance challenges to surveillance via litigation are stymied by established precedent on standing and the third-party doctrine. Political affordance challenges to surveillance are limited by public choice theory where diffuse opinions of surveillance are not compelling enough for citizens to act as passionately as special interest groups. Technical affordance challenges to surveillance are available, but are not readily usable to the average citizen, creating both barriers to entry and a high risk of error when attempted by the layperson. Finally, market affordance challenges require citizens to collectively pressure firms to resist surveillance through market forces. Calo even references Cover's concept of 'corporate avatars' and expressed similar skepticism as Cover that firms would sufficiently serve in an avatar role. Reliance on firms was a consistent theme of Calo's essay and he even states, "Against a background of corporate and other law, and given access to enormous resources, large firms are well positioned to push back against government surveillance if properly motivated. The motivation appears to be mounting in the form of domestic and, to a large degree, international pressure on American firms to put citizen-consumer privacy first" (Calo 2015, 1-15). Although firms are not organisms like citizens, the use of a formerly ecological theory is appropriate because firms and the environment they occupy are analogous to complex adaptive systems (CAS) that organisms occupy in the natural world. Natural CAS are shaped by organisms as individual agents responding to feedback through the property of emergence. Emergence occurs when interactions between individual agents and the environment result in feedback that reshapes the system which then trickles down to influence agents and perpetuate emergence feedback loops. In a CAS, individual agents within their system must balance their own needs with the needs of other agents to benefit the broader natural environment. A firm's environment is a CAS. While firms must protect themselves, their choices impact the other firms in their business ecosystem that they compete with and/or depend on. The choices of all these firms impact the business environment at large - which includes outside stakeholders like government entities and civil society - creating an emergence loop. Firms that do not create value to outside stakeholders risk marginalization. In an increasingly volatile business environment where U.S.-based public companies are delisting at a rate six times the rate forty years prior, firms must navigate emergence loops with long term goals in mind to avoid extinction. Planning for long term goals is difficult in a CAS due to the system's inherent unpredictability. Firms must expect surprise to reduce uncertainty, meaning that in an unpredictable environment firms must collect signals and plan for a variety of plausible desirable or undesirable outcomes. Predicting the future will fail in a CAS. Firms are better

served to prepare for many possible futures so that when surprise occurs, the firms can adapt to survive (Reeves, Levin, and Ueda 2016).

This thesis will test Calo's assertion that firms are well equipped to resist surveillance; Soghoian's assertion that privacy-by-design is advantageous to firms; and both Calo and Cover's assertions that firms are not worthy avatars for their users when resisting U.S. government surveillance. This thesis also recognizes that firms are resisting surveillance within a complex adaptive system that complicates the actions firms take to achieve desirable outcomes and mitigate undesirable outcomes. Calo's approach to Affordance Theory will be used to evaluate the ability of Apple, Facebook, Google, and Microsoft to resist U.S. government surveillance. Affordance Theory allows for an evaluation of the relationship between U.S.-based platform technology firms and U.S. government surveillance that is not grounded in a singular critique of a firm's ability, willingness, or obligation to defend individual privacy. This thesis will determine if firms are realistically equipped to resist U.S. government surveillance as privacy advocates assume. The results will also determine the capacity or willingness of firms to act as corporate avatars depending on how constrained firms are by their surveillance capitalism. Calo's application of Affordance Theory substituting U.S.-based firms for U.S. citizens works because both firms and citizens have the same affordances at their disposal. However, firms are not simply citizens with more power and resources, therefore treating them as such oversimplifies their relationship to their environment. The exposure of U.S. government surveillance served as an interaction that changed the dynamic within the broader business environment forcing firms to adjust in order to survive. Affordance Theory will assist in measuring the manner in which firms adjusted to achieve desired outcomes and avoid undesired outcomes. In a complex adaptive system like a business environment, the actions firms take not only impact their own survival but also the viability of other stakeholders within the environment. Firms must consider their relationships with government, users, shareholders, and other firms when taking actions. The next section explains how Calo's framework allows for the measuring of surveillance resistance methods executed by firms within their business environment.

F. Affordance Theory Framework

Affordances are measured as *negative* or *positive*, *perceptible* or *hidden*, and *true* or *false* from the perspective of the organism being evaluated (Calo 2015, 4). All affordances are contextual, so the same affordance is measured differently based on the firm. Here are some

examples. The legal affordance may be positive for a larger firm with a dedicated legal team and negative for a startup with limited legal representation. The political affordance may be perceptible to larger firms with teams of lobbyists and hidden to smaller firms that underestimate the ability of industry associations to amplify their voice. The technical affordance may be true when firms implement a platform that facilitates a zero data retention policy, making it impossible for firms to hand over data, and false when firms use strong encryption leading to demands by federal law enforcement to hand over decryption keys putting the security of the entire platform at risk. The contingent nature of affordances allows for comparison between firms and business models to draw more insights from each firm's actions.

The legal affordance is applied through litigation. Firms use litigation to challenge application of existing statutes in individual instances or facially challenge a statute's constitutionality. When the U.S. government requests consumer data from firms, the requests are often accompanied by a non-disclosure order preventing the firm from disclosing the details of the request or that the request was even received. Firms have used litigation to challenge for more transparency both in individual instances and in aggregate. Firms have also used litigation to challenge requests, primarily when the data is stored outside of the United States.

The political affordance is applied through political influence. Firms use political influence by lobbying politicians to influence legislation governing issues of value to the firm. Issues range from general concepts like surveillance reform to specific legislation like the Email Privacy Act. Influence is not simply a quid pro quo exchange. The growth of corporate lobbying is more systemic, creating a drain of expertise from public to private sectors and making Congress more dependent on lobbyist data. Highly technical issues exacerbate these dependencies and allow the industry to frame issues and tailor increasingly complex legislation to fit firms' needs. To counter adverse legislation that have legitimate support, firms participate in congressional committee hearings to influence legislation through testimony.

The technical affordance is applied through encryption of both metadata and content or anonymization. Firms use different forms and applications of encryption across platforms. Some firms have adopted anonymization techniques to retain the benefits of analytics and improve their products without the data used for insights being identifiable to the consumer or the consumer's device. The business models and exploitation of surveillance capitalism are determinant factors that influence how technical affordances are executed.

The market affordance is applied by leveraging the market pressure consumers place on firms to protect individual privacy. Calo's application of the market affordance was citizens using collective public sentiment to place market pressure on firms, forcing firms to resist U.S. government surveillance on citizens' behalf. This thesis will explore if loss of consumers could place shareholder pressure on firms to resist surveillance via the other affordances.

This thesis applies Affordance Theory to the most dominant firms - Apple, Facebook, Google, and Microsoft - as the individual agents within the broader business environment to review how effective firms have been at resisting U.S. government surveillance. Each of these four affordances will be categorized as a positive or negative affordance based on the methods employed by each firm and the outcomes of each method. Affordances are contingent to the firm and the surrounding environment, so differences between firms may lead to different affordance categorizations. At times, positive affordances can prove to be false affordances depending on the anticipated desired outcome and the eventual undesired outcome. The results will determine which affordances offer the most desired outcomes for firms balancing the demands of complex adaptive systems to expand their market dominance, protect their surveillance capitalist models, and mitigate potential risks.

Chapter III. Application of Affordance Theory

Methodology

To measure benefits and dangers of each affordance method, the below resources have been reviewed.

- *Legal Affordance*
 - *Litigation*
 - *Resisting Non-Disclosure Orders*
 - *Resisting Data Requests*
- *Political Affordance*
 - *Addressing Congressional Judiciary Committees*
 - *Coalition Letter*
 - *Congressional Hearing Testimony*
 - *Lobbying Disclosures*
 - *Apple, Facebook, Google, Microsoft, Resisting Government Surveillance*
 - *Public Sector/Private Sector Revolving Door*
 - *Lobbying Contributions to Applicable Bills*
 - *USA Freedom Act 2015*
 - *Law Enforcement Access to Data Stored Abroad (LEADS) Act*
 - *Email Privacy Act (EPA)*
 - *ECPA Amendments Act of 2015*
 - *Judicial Redress Act 2015*
 - *International Communications Privacy Act (ICPA)*
 - *Clarifying Lawful Overseas Use of Data (CLOUD) Act*
 - *USA Rights Act*
 - *USA Liberty Act*
 - *FISA Reauthorization*
- *Technical Affordance*
 - *Encryption & Anonymization*
 - *Surveillance Capitalist Business Models*
 - *Network Architecture & Localization*
- *Market Affordance*
 - *Review of Privacy Scandals*

- *Snowden Disclosures*
- *Facebook Cambridge Analytica*
- *Uber*
- *Apple v. FBI*

“Top Firms” refers specifically to Apple, Facebook, Google, and Microsoft. These consumer technology firms are four of the five top technology firms by market capitalization. In addition, all four were named as complicit to NSA surveillance in 2013, creating a cross section of current market dominance and an ongoing stake in U.S. government data access.

The legal actions reviewed were limited to publicly available filings or summaries that named one of the Top Firms. Publicly available filings may be limited because the FISC is a sealed court and NSLs often come with non-disclosure orders.

The lobbying disclosures reviewed include filings from Q1 2014 to Q4 2017 for the Top Firms and a coalition called Reform Government Surveillance (RGS) that includes all four Top Firms and members. Contributions were aggregated across all filings and each filing was reviewed for relevant issues.

Based on outcomes and expert opinion(s), each affordance will be categorized as a positive, negative, false, or contingent affordance for each firm. Once categorizations are measured, the following questions will be addressed:

1. *Which affordance(s) are most beneficial to which firms?*
2. *Are firms capable and/or willing to fill the role of a corporate avatar?*
3. *Does surveillance capitalism impact the methods firms choose to resist surveillance?*

PROPOSITION:

The legal affordance will be most beneficial because multiple stakeholders can be considered and involved in crafting actions based on anticipated outcomes. However, firms are limited by their surveillance capitalist business models and will prioritize defense of their access to revenue-driving user data over the protection of individual privacy. Firms are poor corporate avatars.

A. Legal Affordances

Legal affordances are leveraged through litigation. Non-disclosure orders and the third-party doctrine limit the legal affordances of citizens while elevating that of firms. The Top Firms have challenged both U.S. government requests for data and non-disclosure orders that prohibit firms from publicly acknowledging requests or alerting the subject of the requests that a request was received. Tables 9 - 12 represent a summary of the eleven cases reviewed to evaluate the effectiveness of litigation as a form of resistance. The tables list all the cases including the most recent case description details; the type of surveillance resisted; whether the ruling was favorable or unfavorable to the firm; and the potential desired and undesired outcomes resulting from firms taking legal action to resist surveillance. Following these tables, this section will explore the impact of these cases in more detail.

Table 9: Legal Affordance Outcomes for Multiple Firms

Date	Case No.	Latest Court	Type	Strategy	Outcome	Desirable	Undesirable
1/27/14	13-03 13-04 13-05 13-06 13-07	U.S. Foreign Intelligence Surveillance Court	ND	Prior Restraint	F	Transparency	PRISM Speculation

“ND” = Non-Disclosure, “DR” = Data Request, “F” = Favorable, “U” = Unfavorable

Table 10: Legal Affordance Outcomes for Facebook

Date	Case No.	Latest Court	Type	Strategy	Out-come	Desirable	Undesirable
7/21/15	132 AD 3d 11 30207/13, 30178/14	Appellate Division Of the Supreme Court of NY	ND	Open-Ended, Search & Seizure	U	Citizen Affordance Empowerment	Con’t Non-Disclosure Order Use
9/14/17	17-SS-388 17-SS-389 17-SS-390	D.C. Court of Appeals	ND, DR	Freedom of Association	F	Political Speech & Association Freedom	Surveillance of Political Dissidents

“ND” = Non-Disclosure, “DR” = Data Request, “F” = Favorable, “U” = Unfavorable

Table 11: Legal Affordance Outcomes for Microsoft

Date	Case No.	Latest Court	Type	Strategy	Out-come	Desirable	Undesirable
2/8/17	C16-0538JLR	U.S. Dist Ct. Western District WA	ND, DR	Prior Restraint	F	Revised D.O.J Non-Disclosure Guidance	Continued Non-Disclosure Use
2/27/18	No. 14-2985	U.S. Supreme Court	DR	Extra-territorial	N/A	Limits U.S. Gov't Reach Abroad	Localization, Protectionism

“ND” = Non-Disclosure, “DR” = Data Request, “F” = Favorable, “U” = Unfavorable, “N/A” = Not Applicable

Table 12: Legal Affordance Outcomes for Google

Date	Case No.	Latest Court	Type	Strategy	Out-come	Desirable	Undesirable
2/21/17	17-M-1235	U.S. Dist Ct. Eastern District WI	DR	Cites MS v U.S.	U	Limits U.S. Gov't Reach Abroad	Localization, Protectionism
4/19/17	16-mc-80263-LB	U.S. Dist Ct. Northern District CA	DR	Cites MS v U.S.	U	Limits U.S. Gov't Reach Abroad	Localization, Protectionism
7/10/17	16-4116	U.S. Dist Ct. NJ	DR	Cites MS v U.S.	U	Limits U.S. Gov't Reach Abroad	Localization, Protectionism
7/31/17	16-mj-00757	U.S. Dist Ct. D.C.	DR	Cites MS v U.S.	U	Limits U.S. Gov't Reach Abroad	Localization, Protectionism
8/17/17	2:16-mj-01061-TJR	U.S. Dist Ct. Eastern District PA	DR	Cites MS v U.S.	U	Limits U.S. Gov't Reach Abroad	Localization, Protectionism
9/1/17	5:17-mj-532-HNJ	U.S. Dist Ct. Northeastern District AL	DR	Cites MS v U.S.	U	Limits U.S. Gov't Reach Abroad	Localization, Protectionism

“ND” = Non-Disclosure, “DR” = Data Request, “F” = Favorable, “U” = Unfavorable

Immediately following the Snowden disclosures, the Top Firms called on the government for increased transparency. The secrecy of FISA 702 resulted in increased public distrust and

allowed a presentation slide from the disclosures to generate accusations of backdoor access to firm servers. Firms used litigation to challenge for more transparency allowances. There are two forms of non-disclosure orders.

The first form is a prohibition of disclosing aggregate data relevant to National Security Orders (NSO). NSO requests are typically accompanied by non-disclosure orders because of the sensitivity of national security investigations. FISA requests and National Security Letters are NSO. The Snowden disclosures implied that technology firms were providing the U.S. government direct access to their servers, so five technology firms (Google, Microsoft, Facebook, Yahoo, and LinkedIn) filed motions for declaratory judgement to allow the firms to disclose aggregate statistics². Apple served as an Amicus on this filing³. This filing is reflected above in Table 9. Google's motion stated that its "reputation and business has and continues to be harmed by the false or misleading reports in the media" and that "transparency is critical to advancing public debate in a thoughtful and democratic manner"⁴. An accompanying letter sent from Google's Chief Legal Officer to then Attorney General Eric Holder and FBI Director Robert Mueller states that the non-disclosure orders prohibiting disclosure of the number of NSO requests fuel public speculation that the U.S. government had "unfettered" access to Google servers (Drummond 2013). The motivation of firms for fighting non-disclosure orders was directly related to the public perception that firms were complicit in allowing the U.S. government privileged access to global user data (Kopfstein 2013). That perception was leveraged by international competitors to dissuade non-U.S. markets into more protectionist policies, even incorporating U.S. surveillance into marketing campaigns (Castro and McQuinn 2015). Challenging the non-disclosure orders was necessary to fight negative perceptions held by other relevant stakeholders like domestic consumers, non-U.S. governments, non-U.S. consumers, and global competitors.

The five firms that initiated litigation for more transparent disclosure allowances described the non-disclosure orders as a prior restraint on speech. The prior restraint claim was based on the non-disclosure orders prohibition of communication of U.S. government requests for data in advance of any opportunity of communication to occur. Prior restraints on

² Op. at 13-03, 13-04, 13-05, 13-06, 13-07 (*In Re Motion for Declaratory Judgement of a First Amendment Right to Publish Aggregate Information About FISA Orders*), (FISA Ct. 2014).

³ Op. at (*In re Motions for Declaratory Judgement to Disclose Aggregate Data Regarding FISA Orders and Directives*), Case Nos. 13-03, 13-04, 13-05, 13-06, 13-07 (FISA Ct. 2013) (amicus curiae brief).

⁴ Op. at 13-03 (*In re Amended Motion for Declaratory Judgement of Google, Inc.'s First Amendment Right to Publish Information About FISA Orders*), (FISA Ct. 2013).

expression, like communications, come with a presumption against constitutional validity especially when the suppressed speech is of [political and social] issues of public interest⁵. The lawsuit never reached a judgement. Instead, the five firms eventually agreed with the government to dismiss the actions in exchange for guidelines offered by the Attorney General allowing for aggregated disclosure (“Dear General Counsels” 2014). The agreement demonstrated the balance between the firms and the government and each party’s willingness to compromise in a way that allowed firms to claim that the government does not have unchecked access to data and still allowed for a level of opacity for the government given the national security implications of the NSO. It was mutually beneficial for firms and the U.S. government to demonstrate some measure of change to address public concerns. For firms, transparency would prevent a chilling effect on their users, who are necessary to fuel their surveillance capitalism. If many users are reluctant to use a firm’s service for fear of U.S. government surveillance, there is no incentive for new users to join. This demonstrates an example of negative network effects. Although transparency reporting could only reveal large aggregated blocks of requests, the reports show that requests were limited to a fraction of total users and that any access required the U.S. government to make a request to the firm. The U.S. government did not have uninhibited access to user data.

The second form of non-disclosure order prohibits firms from alerting users when the U.S. government requests user data. Notifying users of data requests gives users the opportunity to defend themselves as the subjects of an investigation. Facebook has challenged law enforcement requests for data and, although the requests were not NSO, the warrants used were authorized by the SCA and Facebook’s challenges were constitutional in nature. Facebook challenged non-disclosure orders in two instances. The first case concerned the warrants issued for subscriber information and content of 381 Facebook accounts believed to be linked to a disability fraud investigation. This case is reflected in the top row of Table 10. In the New York Supreme Court, Facebook challenged the non-disclosure order, asserting Facebook’s First Amendment rights against an open-ended ban on speech. Facebook added that an open-ended ban ensures that the owners of the Facebook accounts would never be able to advocate for their Fourth Amendment right against an unreasonably secret search and seizure. Facebook was denied because the court felt the firm had no legal standing to challenge the constitutionality because Facebook was “simply an online repository of data and not the target of the criminal

⁵ *Id.*

investigation”⁶. The court also felt that the disclosure of the warrants would risk an ongoing investigation⁷. The second case was also constitutionally focused and is reflected in the bottom row of Table 10. In a District of Columbia Appeals Court, Facebook moved to vacate the indefinite non-disclosure provisions of three warrants linked to protests that occurred on President Trump’s inauguration day. Facebook claimed that users were entitled to notice when their First Amendment rights to anonymous political speech and association were at stake. The motion was denied but the court amended the non-disclosure orders to expire thirty days after the government received the requested⁸. Eventually, the three warrants were jointly dismissed since the investigation had progressed while the orders waited appeal from Facebook⁹. In the first instance, Facebook’s challenge was summarily dismissed as Facebook was out of bounds advocating for constitutional rights of the individual consumer. In the second instance Facebook’s challenge advocating for the consumer’s First Amendment rights, while not completely successful, at least resulted in the court amending the order.

In April 2016, Microsoft submitted a complaint for declaratory judgement asking the U.S. District Court of Washington at Seattle to declare Section 2705(b) of Stored Communications Act (SCA), which authorizes non-disclosure orders, facially unconstitutional. This case is reflected in the top row of Table 11. Microsoft stated that in a twenty-month period, federal courts had issued 3,250 non-disclosure orders with an indefinite timeline for two-thirds of them. Microsoft claimed that the non-disclosure orders violated the firm’s First Amendment rights to speak with their customers about government investigations in addition to failing strict scrutiny. To Microsoft, indefinite non-disclosure orders were a prior restraint on speech putting the onus on Microsoft to check with the court for relief with no expectation of resolution. Microsoft also claimed that the firm could vindicate the Fourth Amendment rights of their users since indefinite non-disclosure orders prevent users from knowing that their rights need defending. Then in February 2017, the government motioned to dismiss Microsoft’s challenges resulting in a grant in part and a denial in part. The court granted the motion to dismiss the Fourth Amendment challenge ruling that firms could not assert Fourth Amendment rights on behalf of another person, as with the Facebook case. However, the court denied the motion to

⁶ Op. at 132 A.D.3d 11 (*In the Matter of 381 Search Warrants Directed to Facebook Inc.*), 14 N.Y.S.3d 23 (N.Y. App. 2015).

⁷ *Facebook, Inc v. N.Y. County Dist. Attorney’s Office*, No. 16 (N.Y. App. 2015).

⁸ *Facebook, Inc. v. United States*, Nos. 17-SS-388, 17-SS-389, 17-SS-390 (D.C. App. 2017) (notice to potential amici curiae).

⁹ *Facebook, Inc. v. United States*, Nos. 17-SS-388, 17-SS-389, 17-SS-390 (D.C. App. 2017) (joint motion to dismiss).

dismiss the First Amendment challenge, ruling that indefinite non-disclosure orders were both prior restraints and prohibitions of content-based speech with both requiring strict scrutiny that the orders failed to meet¹⁰. Microsoft's challenge was successful in part. In October 2017, Deputy Attorney General Rod Rosenstein approved new guidance issued by the Justice Department that limits non-disclosure orders to less than a year with limited exceptions. Non-disclosure orders also need to be narrowly tailored and applied only when necessary. While Microsoft still advocates for new legislation, the new guidance is considered a win for technology firms which led Microsoft to drop the lawsuit. This guidance may be exactly what a Justice Department spokesperson described as a balance where the department can still protect the rights of citizens while allowing technology firms to maintain relationships with users (Nakashima 2017).

Increased transparency helps refute any perceptions that the U.S. government has unbridled access to the Top Firms' user data. Challenging excessive non-disclosure orders signals to users that the Top Firms are on their side and potentially offers users the ability to challenge the data requests themselves. Facebook's mixed results across district courts will become a theme for the legal affordance. However, both the litigation for more aggregated transparency and Microsoft's facial challenge to SCA's non-disclosure provision resulted in a compromise between the Top Firms and the U.S. government. Litigation of non-disclosure orders resulted in desirable outcomes. The Top Firms have had far less success challenging the actual data requests through legal affordance methods.

In September 2015, a 2nd Circuit Court of Appeals decision made *Microsoft v. U.S* a pivotal case concerning government requests for user data. This case is reflected in the bottom row of Table 11. Microsoft submitted a motion to quash an SCA authorized warrant issued for data located in a Dublin datacenter based on the user's submitted country code. After the data is transferred to Dublin, almost all content and non-content data is deleted from U.S. data centers. Section 2703 of the SCA authorizes U.S. government warrants for data collected and stored by Electronic Communications Services (ECS), such as technology firms. Microsoft disclosed responsive information that was still being stored in the U.S., but the contents of the emails were stored in Ireland. Because the contents were stored outside of the U.S., Microsoft motioned to quash the warrant. However, the magistrate judge denied the motion, claiming that warrants issued under SCA authority operated more like a subpoena. The magistrate judge noted that the

¹⁰ *Microsoft Corp. v. United States Dep't of Justice*, No.16-0538 (W.D. Wash. Feb. 8, 2017) (order on motion to dismiss).

warrant was served on Microsoft and not law enforcement, and that Congress intended the warrant to obligate the recipient to “produce information in its possession, custody, or control regardless of the location of information”¹¹.

The 2nd Circuit Court of Appeals disagreed with the magistrate judge and reversed the order, returning the case back to district court to execute Microsoft’s motion to quash. The 2nd Circuit Court of Appeals believed that a warrant requesting data from a server outside of the United States is an extraterritorial application of domestic law. Unless explicitly contrary, interpretation of U.S. law presumes an application within the territorial district of the U.S. to avoid conflict of law scenarios and international discord. Testing laws for extraterritorial reach requires two steps. First, the law is reviewed to determine if the SCA permits extraterritorial reach, which the government conceded was not the case. The second step is to determine if there was an extraterritorial application of domestic law. The 2nd Circuit Court of Appeals believed the focus of the SCA was on privacy and not to aid law enforcement, therefore invasion of the customer’s privacy takes place when the customer’s protected content is accessed in Ireland. Microsoft’s role in retrieving the data from the Ireland server meant that Microsoft was acting as an agent of the government which is an extraterritorial application. The 2nd Circuit rejected the theory that “foreign sovereign interests are unaffected” when a U.S. judge orders a service provider to ‘collect’ data, possibly belonging to a foreign citizen, and ‘import’ it into the United States from a foreign server simply because the service provider has a base of operations within the United States¹².

The 2nd Circuit’s decision could have had a profound impact on U.S. government access to data. If upheld, the SCA statute that authorizes electronic communication warrants would not be able to compel disclosure of personal data located outside of the United States, making surveillance of foreign actors very difficult for the U.S. government. Any requests for data stored by U.S.-based firms outside of the U.S. would require use of the MLAT system, nullifying the advanced position the U.S. government has over multinational U.S.-based firms. Dissatisfied with the 2nd Circuit’s decision, the U.S. government requested an en banc review. The review was denied 4-4, but dissenting opinions from the decision would subsequently influence lower court rulings in cases that cited the 2nd Circuit’s decision (Jacobs 2017).

¹¹ Op at. 14-2985, *Microsoft Corp. v. United States*, (In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation), Case No.14-2985 (2d Cir. Jul. 14, 2016).

¹² *Id.*

Emboldened by Microsoft’s favorable 2nd Circuit ruling, Google challenged several requests for data stored outside the United States claiming that they were extraterritorial. Google cited the Microsoft decision in six separate districts, but *none* of the districts agreed with the 2nd Circuit decision. All six cases are reflected in Table 12. The district courts *agreed* in part with the 2nd Circuit that the SCA does not have extraterritorial jurisdiction. However, all six districts *disagreed* with the 2nd Circuit and ruled that both the querying of data at Google’s headquarters in California and exchange of data for review by law enforcement occurred in the United States. Therefore, execution of the warrants were domestic applications of the authorizing statute. In the Alabama and California districts, Google’s network architecture undercut any argument that copying or transferring data stored abroad to the U.S. impacted sovereignty. Google’s network shards data and distributes the shards globally for efficiency rather than storing data statically based on locality. Microsoft stored the user’s data in Ireland because that was the perceived location or nationality of the user¹³. A U.S. District Court in Wisconsin ruled on two cases challenging SCA warrants citing Microsoft, one of which had Google serving as the claimant. In its decision to issue the warrants, the court cited dissenting opinions from the U.S. v. Microsoft en banc request as persuasive analysis. The Wisconsin decision stated, “it should not matter where the ones-and-zeroes are stored” and that “what matters is the location of the service provider”¹⁴. A district court in the District of Columbia vehemently disagreed with the 2nd Circuit. The court described the 2nd Circuit decision as “erroneous” and “based on flawed reasoning.” The court went on further stating “...the Microsoft decision does little to protect customer privacy and succeeds only in pouring molasses on the ability of the government to conduct lawful criminal investigations to protect the public”¹⁵.

Relying on the Microsoft decision has made Google’s success rate so poor that the company informed the Justice Department that it would no longer challenge Section 2703 authorized

¹³ Op. at (*In the Matter of the Search of Content that is Stored at Premises Controlled by Google (No.45)*), Case No. 16-mc-80263 (N.D. Cal. 2017).; Op. at (*In Re Search Warrant Issued to Google, Inc.*), Case No. 17-mj-532 (N.D. Ala. 2017).; Op. at (*In Re Search Warrant to Google, Inc.*), Case No. 16-4116 (D. N.J. 2017).; Op. at (*In re Search Warrant No. 16-960-M-1 to Google, In re Search Warrant No. 16-1061-M to Google (No.13)*), Case No. 16-mj-1061 (E.D. Penn. 2017).

¹⁴ Op. at (*In re: Information Associated with One Yahoo email address that is stored at premises controlled by Yahoo, In re: Two email accounts stored at Google, Inc.*), Case Nos.17-M-234, 17-M-1235 (E.D. Wis. 2017).

¹⁵ Op. at (*In re Search of Information Associated with [Redacted]@gmail.com That is Stored at Premises Controlled by Google, Inc.*), Case No. 16-mj-757 (D. D.C. 2017).

warrants (Kravets 2017). The 2nd Circuit ruling initially appeared to be a success for the Top Firms, but since the ruling is not binding in other courts, citing the 2nd Circuit has proven to be unreliable.

The government petitioned the U.S. Supreme Court to hear the 2nd Circuit Microsoft case. The court accepted and heard oral arguments on February 27, 2018 (“United States v. Microsoft Corp.” n.d.). Depending on the decision of the U.S. Supreme Court, this affordance method could have resulted in both desirable outcomes and hidden undesirable outcomes. Microsoft’s Chief Legal Officer Brad Smith expressed concern in a blog post that if the Supreme Court reversed the 2nd Circuit decision and granted U.S. government access to data and content of foreign citizens regardless where the data is stored, non-U.S. governments may make reciprocal requests to the data and content of Americans, eroding privacy as each nation demands the same level of access. Smith also suggested that a reversal decision could result in more protectionist policies by non-U.S. governments given that their fears of preferential U.S. government access to their citizens’ data would be confirmed (Smith 2017c). At the same time, if the Supreme Court upheld the 2nd Circuit’s decision, non-U.S. governments may be incentivized to enact data localization policies. Data localization would have impacted firms and their stakeholders in desirable and undesirable ways. Non-U.S. users would have been able to avoid their data being reached by the U.S. government, but if their country has less restrictive privacy or surveillance regulation, localization would benefit the non-U.S. government with increased access (Granick 2016). Through localization, non-U.S. governments would publicly appear to be protecting their citizens from U.S. overreach while simultaneously making it easier to surveil their own citizens. Localization also favored Microsoft and other firms that have structured their network along country lines.

Google’s challenges to warrants citing the 2nd Circuit Microsoft decision failed in part due to the difference in network architecture. Localization favors a data-location-centric approach. Since Google’s data is sharded and constantly moving from server to server all around the world, a favorable Microsoft ruling incentivizing localization may have actually been undesirable for Google (Woods 2017). Resisting data requests within the legal affordance presents potential undesirable outcomes for both favorable and unfavorable rulings. In his concurring opinion from the Microsoft v. United States judgement, 2nd Circuit Judge Gerard Lynch called for Congress to act because courts are ruling based on statutes that do not adequately address the issues presented to the court. Congress is not bound to binary

decisions¹⁶. In March 2018, the Department of Justice and Microsoft mutually agreed that the enactment of the CLOUD Act rendered Microsoft's lawsuit moot (Jeong 2018). The CLOUD Act will be discussed further in the next section covering the political affordance.

The legal affordance yielded mixed results for the Top Firms. Desirable outcomes were achieved when firms litigated for more transparency allowances, but not to the extent that the Top Firms initially anticipated. Even during the public distrust of government surveillance immediately following the Snowden disclosures, the Top Firms dropped their lawsuit and compromised with the U.S. government to limit NSO reporting to large blocks of request figures and reporting updates every six months on a six-month delay. The compromised transparency still achieves the desired outcomes for the Top Firms. Other stakeholders like U.S. citizens, non-U.S. citizens, and non-U.S. governments have more visibility to data that was previously undisclosed. The request data and approval by the U.S. government to publicize relieves the firms of speculation that the U.S. government had unfettered backdoor access to user data. Similarly, Microsoft's facial challenge to indefinite non-disclosure orders led to new guidance from the Department of Justice, leading Microsoft to drop their litigation. Again, the Top Firms compromised by accepting more restrictive guidance in lieu of legislative restrictions. The concessions made in both cases reflect the need to consider all stakeholders in a complex adaptive system. The Top Firms were still able to achieve their desired outcomes. Actions that may have started using litigation forced the U.S. government to propose compromised solutions. The Top Firms adapted to the feedback rather than force their initial path and risk an undesirable outcome.

The limits of the legal affordance are most prominent when the Top Firms litigated to resist data requests. Litigation is highly dependent on existing law and established precedent restricting the available actions and outcomes using the legal affordance. The third party doctrine prevents the Top Firms' users from asserting Fourth Amendment rights, making users dependent on firms to protect their privacy. However, the above cases demonstrate that firms do not have third party standing to assert Fourth Amendment rights on behalf of their users either, so firms are simultaneously relied upon and prevented from challenging data requests based on Fourth Amendment constitutional protections. When the Top Firms resisted U.S. government data requests of data stored outside U.S. borders, the limitations of the legal affordance presented the risk of it becoming a false affordance and resulting in undesirable outcomes. The

¹⁶ *Microsoft Corp. v. United States*, No.14-2985 (2d Cir. Jul. 14, 2016) (concurring in the judgement).

legal affordance cannot consider the updated demands of multiple stakeholders, making litigation of decades old legislation fraught with unintended undesirable outcomes if pursued to completion. If the U.S. Supreme Court had ruled on the 2nd Circuit Microsoft appeal, regardless of the ruling's favorability, there would have been many potential undesirable outcomes including increased localization demands or reciprocal laws granting non-U.S. governments access to data stored within the United States. Although the litigious action of Microsoft, and subsequently Google, was executed with a desirable outcome in mind, the complex adaptive nature of the business environment may have turned a seemingly positive affordance into a false affordance. By resisting data requests, the actions of firms under the legal affordance threatened other firms within their business ecosystem and outside stakeholders, such as non-U.S. citizens, within the broader business environment.

The unpredictable and potentially undesirable outcomes of the rigid legal affordance may have actually been a net positive for the Top Firms' business ecosystem and environment because of the high stakes for both U.S.-based firms and the U.S. government. Transparency resistance cases resulted in compromises which ended litigation prior to a ruling. Data request resistance cases were mostly unsuccessful in lower courts, but the Microsoft U.S. Supreme Court case had such high stakes that firms and lower courts advocated for a legislative solution. Passage of the CLOUD Act is the culmination of multiple stakeholders planning for a variety of plausible outcomes in a complex adaptive system. Despite the risks inherent to the legal affordance, desirable outcomes may be unintended feedback from litigious actions on the part of the Top Firms and the U.S. government.

The Top Firms served as sufficient corporate avatars even if, at times, their capacity as corporate avatars occurred only when the needs of the firms were aligned with actions that supported individual privacy. Litigation for increased transparency and challenges to requests for data stored overseas were motivated by access to international markets and non-U.S. personal data assets. U.S. government surveillance access to foreign user data was utilized by non-U.S. competitors to threaten the global dominance of the Top Firms. Increased transparency allowances allowed firms to address and correct international speculation of backdoor government access. Conflict of law situations and protectionism were stated as motivating factors when resisting data requests. Microsoft's U.S. Supreme Court case would have prevented conflict of law issues for Top Firms while other outcomes would have been detrimental to U.S. citizen and non-U.S. citizen privacy. Both forms of surveillance resistance

had surveillance capitalist motivations, but they also had desirable outcomes for individual privacy even if being a corporate avatar was a tangential outcome. The legal affordance actions that are less clearly defined are the data request refusals based on constitutional challenges. These First and Fourth Amendment challenges support the rights of users to defend their constitutional rights or the ability of Top Firms to defend constitutional rights on the user's behalf. In these cases, the Top Firms appeared more altruistic with fewer obvious benefits to surveillance capitalism beyond gaining or retaining users based on a public commitment to privacy.

B. Political Affordances

The political affordance offers more benefits for firms because it lacks the constraints that complicated the legal affordance. When technology firms challenge data requests via litigation, the firms are limited by the existing governing statutes. The statute authorizing almost all requests is the Electronic Communications Privacy Act (ECPA) which was passed in 1986, predating the iPhone by over twenty years. Applying outdated legislation to a rapidly changing industry with global reach is impractical. The day that the government petitioned the U.S. Supreme Court to consider the Microsoft 2nd Circuit decision, Microsoft's Chief Legal Officer Brad Smith wrote a blog post advocating for legislative solutions because a legislative process would involve "incorporating input from multiple stakeholders," resulting in solutions that "consider the needs of law enforcement, the realities of modern technology, and the application of people's traditional rights in today's world" (Smith 2017a).

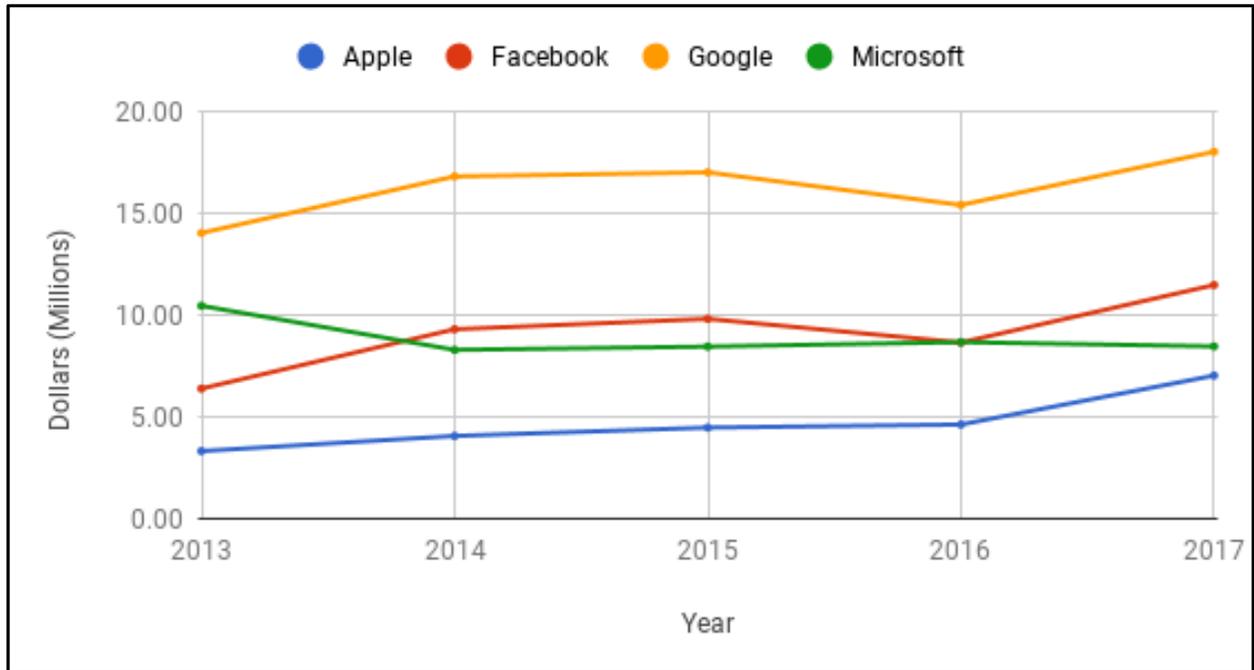
Firms leverage political affordances by influencing legislators to write new laws or revise existing laws. Actions of political influence are exerted through lobbying or addressing relevant congressional committees on the issues with current legislation and suggesting reforms. The levers of influence possessed by firms set them apart from diffuse individual citizens when leveraging political affordances. Lobbying is more than presumptive quid pro quo transactions between firms and lawmakers. Political scientist Lee Drutman describes modern lobbying as being far more systemic. Corporate lobbying accounts for three quarters of lobbying activity. As firms invest more into lobbying expenses, they attract experienced staffers from the government to the private sector. Lobbyists with government experience can earn as much as double that of a member of Congress. Public to private migration leaves congressional staffers with little experience, making them highly dependent on information from experienced lobbyists who have

brought expertise from government to firms. Complex policy topics covering technology and globalization increase the knowledge gap between government and firm lobbyists. Congressional staff sizes have been the same since 1979, leaving lawmakers with less experienced staffers covering increasingly complex policy issues with the same number of staffers as their predecessors had almost forty years ago. The complexity of policy further advantages firms by allowing for small provisions that benefit individual firms and make the overall policy even more complex. More complex policy benefits the most resourced stakeholders, likely firms, leading to less investment and resistance from the public. Firms also shape the knowledge base around Washington by funding think tanks and participating in associations that produce studies used by government staffers to support policy decisions (Drutman 2015, 3-34).

Overall, the Top Firms have greatly increased lobbying spending over the past five years. Apple has more than doubled annual spending between 2013 and 2017. Facebook increased annual spending by almost 80 percent between 2013 and 2017. Google increased annual spending by only 28 percent between 2013 and 2017 but consistently spent twice that of the other Top Firms. Microsoft was the only firm that decreased spending between 2013 and 2017 but still consistently spent more than Apple. Table 13 represent the Top Firms' spend based on mandated lobbying disclosures since 2013, demonstrating the level of investment between firms and the increased perceived value of lobbying over time. The high investment in lobbying spend presumes a return on investment for firms indicating power and influence on lawmakers. Also, the more firms invest in lobbying, the more likely they will be able to attract top talent away from government to represent their interests.

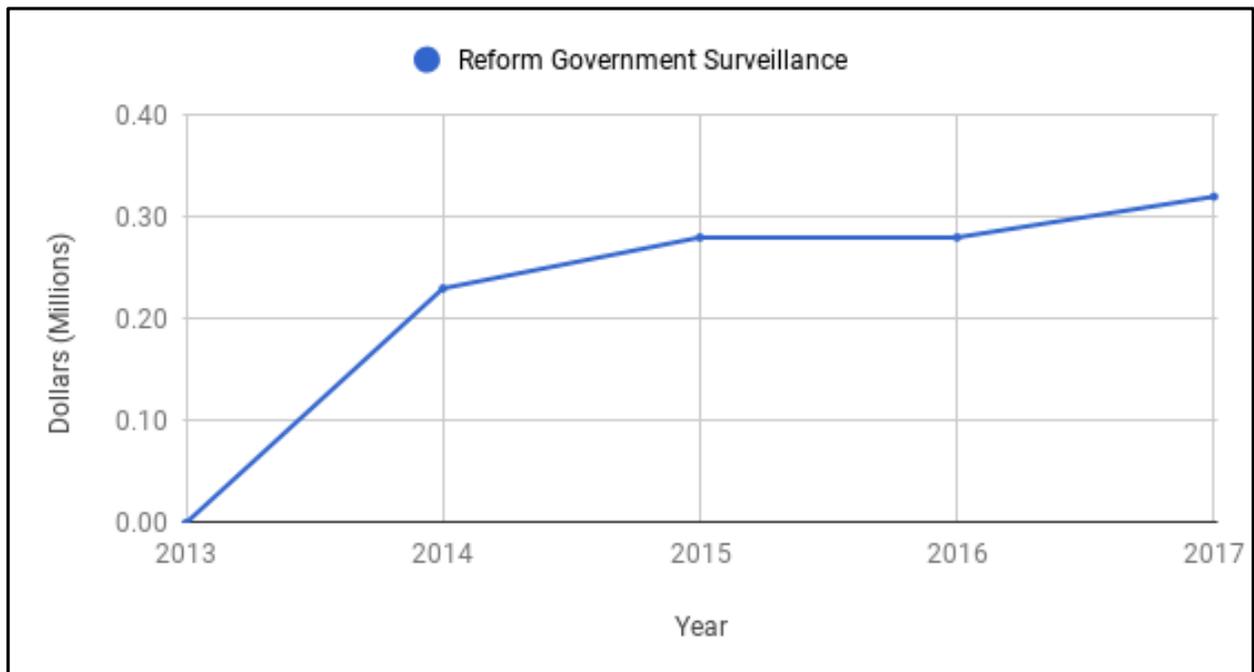
Table 13: Lobbying Disclosure Spend for the Top Firms

Source: “Lobbying Disclosure”. Office of the Clerk US House of Representatives, Accessed on 2017 Sep 15



After the Snowden disclosures, several U.S.-based technology companies formed an industry coalition called Reform Government Surveillance (RGS). This coalition includes all four of the Top Firms and is used to collectively express the types of surveillance reform these firms support. The coalition advocates for five reform measures. First, RGS suggests limitations of surveillance, including the end of bulk collection and requiring requests be targeted to specific, known users. Second, RGS suggests increased oversight, including an independent and adversarial court review, and public availability to significant court decisions (“Global Government Surveillance Reform” n.d.). The third RGS suggestion has been partially executed; RGS suggested transparency allowances for firms to disclose the number of requests received and suggested transparency reports for the government. Transparency allowances were earned via the legal affordance. Fourth, RGS advocates for the free flow of information, requiring a prohibition on localization requirements and other protectionist policies. Lastly, RGS suggested reforms to avoid conflict of laws situations and, if unavoidable, resolution on the part of the relevant governments. Table 14 demonstrates the RGS coalition’s lobbying spend that augments the spend of individual firms.

Table 14: Lobbying Disclosure Spend for the Reform Government Surveillance Coalition



The Top Firms all have lobbyists with prior government experience, and Table 15 helps demonstrate how firms value prior government experience. All four firms have greater than 57 percent revolving door lobbyists. One of Google’s lobbyists, Susan Molinari, was a member of the House of Representatives from 1991 - 1997. The investments summarized in Tables 13 and 14 contribute to the Top Firms’ abilities to hire lobbyists with government experience in order to maximize their impact on lawmakers. Table 15 also demonstrates that the lobbying firm representing the Reform Government Surveillance Coalition, Monument Policy Group, is also heavily staffed with revolving door lobbyists at 64 percent.

Table 15: Revolving Door Lobbyists

Firm	Ratio of Revolving Door Lobbyists
Apple	6 of 9 total internal lobbyists
Facebook	4 of 7 total internal lobbyists
Google	8 of 13 total internal lobbyists (Includes former Congressperson)
Microsoft	10 of 16 total internal lobbyists
Monument Policy Group*	9 of 14 total hired lobbyists

*Representing Reform Government Surveillance, Source: Open Secrets, Accessed on 2018 Mar 20

The Top Firms have invested significantly into lobbying to address a range of issues like copyright law, immigration, and surveillance. In October 2013, a coalition of technology firms, including the Top Firms, sent a letter to both the House Judiciary Committee and Senate Judiciary Committee calling for increased transparency to correct what firms consider speculation about government access following the Snowden disclosures. The firms advocated for better privacy protections and reforms for more accountability and oversight of surveillance programs. The USA Freedom Act was specifically endorsed as a positive step in a public conversation about privacy and security, and the firms offered to work with the committees and co-sponsor bills to support the effort (“An Open Letter to Washington” 2013).

Executives prioritized surveillance reform and appeared before congressional committees to advocate for new legislation. In March 2013, Google’s Director of Law Enforcement and Information Security Richard Salgado testified in a House Judiciary Subcommittee hearing on “ECPA Part 1: Lawful Access to Stored Content.” Google’s testimony represented the concerns of the Digital Due Process Coalition created to push for ECPA reform. Members of this coalition include other Top Firms Apple, Facebook, and Microsoft as well as trade organizations and smaller firms (“Who We Are” n.d.). Salgado’s testimony introduces the problems created when a dynamic industry is governed by a statute that predates modern technologies by decades. The 2013 hearing focuses on privacy concerns of U.S. citizens. Salgado calls for reforms that offer more constitutionally protected privacy for users and clear guidance for firm compliance when faced with requests from law enforcement. Salgado emphasizes that applying an antiquated law to current technology and business practices creates confusion and uncertainty for law enforcement, firms, and courts alike (Salgado 2013).

In June 2017, Salgado testified before the House Judiciary Committee again, but with two major additions to the 2013 testimony. First, the ECPA was a major focus of the more recent testimony, but Salgado drew attention to how the ECPA complicates cross-border data access. Salgado commended the House Representatives for unanimously passing the Email Privacy Act the previous year which addressed domestic concerns that were raised during his 2013 testimony. However, the ECPA, now more than thirty years old, required additional reform to address global implications of the statute’s antiquated provisions. Second, when suggesting underlying principles that should be considered in legislation reforming the ECPA, Salgado pointed to recently introduced legislation that shared the same goals outlined in his own

testimony. During the testimony, Salgado described how the ECPA adversely affects the international markets of technology firms. In the same way the statute was unable to anticipate advances in technology, the writers of the ECPA could not anticipate the significant global reach of U.S.-based technology firms. To emphasize the inadequacy of litigation as a solution to address ECPA complications, Salgado states, “All of these courts are being asked to resolve individual disputes in ways that are divorced from sound policy decisions, without the robust opportunity for debate among a variety of stakeholders, and indeed potentially entirely in closed courtrooms” (Salgado 2017a, 4). Remember that Google fared poorly when resisting government data requests through the legal affordance. Salgado’s testimony envisions a path to reform as a path that considers and strives for equity between users, law enforcement, technology firms, and foreign sovereigns alike. Salgado acknowledged the potential of the bipartisan International Communications Privacy Act (ICPA), introduced in 2016 in both the House and the Senate, as a promising framework to update ECPA in a fashion that considers the needs of all relevant stakeholders. Salgado then proposed four refinements to improve the ICPA that addressed threats to cross-border data transfer, which is critical to Google’s Cloud Infrastructure (Hölzle 2018). The first refinement proposed that data location be excluded as a determining factor governing access. The second proposed that notice be provided to countries when another country requests data belonging to a national or current resident of the former country. The third proposed redress and potential comity analysis should a country receive notice that another country is requesting data belonging to one of its nationals. Lastly, the fourth refinement proposes reciprocity agreements between countries who prescribe to the first three refinements (Salgado 2017a). All four refinements were foundational talking points when ICPA sponsor Senator Orrin Hatch spoke on the Senate floor less than a month after the House Judiciary Hearing (Hatch 2017b).

Microsoft’s President and Chief Legal Officer Brad Smith also testified before the House Judiciary Committee on two occasions to address cross-border data requests. In February 2016 and May 2017, Smith’s testimony also called for new legislation to replace the outdated ECPA but emphasized the costs at stake should Congress neglect to act or neglect to consider global data protection laws. Smith frames the international situation describing how application of outdated laws are resulting in unilateral and extraterritorial claims of legal authority creating a conflict of laws “on steroids.” Overreaching laws lead to other countries responding with data localization and retention requirements that leave technology firms in the middle choosing which country’s law to break. Smith offers the GDPR as a relevant example. The GDPR requires

that decisions made by courts or other administrative authorities requiring firms to disclose personal data to a requesting third country, like the United States, to be conducted via international agreement. Requests made by the U.S. government - like the request being reviewed by the U.S. Supreme Court in the Microsoft Ireland case - would present a situation where Microsoft could only comply to U.S. demands by violating the EU law and face penalties of up to 4 percent of their global revenue. A Mutual Legal Assistance Treaty (MLAT) is an existing international agreement mechanism that is GDPR compliant, but has not been updated with technology advancements. MLATs are still completed on paper and lack standardization across agreements. In the testimony, Smith calls for modernization and standardization of the MLAT process as part of a complete overhaul of U.S. law and international agreements (Smith 2016). Smith warned that inaction could threaten multiple stakeholders. U.S. firms are placed in conflict of law situations risking significant fines or encouraging protectionist policies that disadvantage U.S. firms internationally. Individual privacy is threatened globally as countries reciprocate unilateral and extraterritorial claims that ignore sovereignty. Legitimate law enforcement efforts are undermined by overbroad blocking statutes, like the ECPA, that disadvantage foreign law enforcement by forcing them to rely on inadequate international agreements (Smith 2017b). Smith's testimony appears to focus much more on conceptual changes and emphasizes the risks of congressional inaction, which compliments Salgado's reform suggestions.

Salgado and Smith emphasized that the ECPA is outdated legislation, particularly with regards to the Stored Communications Act (SCA). The provisions of the statute indicate that the legislators in 1986 did not anticipate how pervasive stored communications would be three decades later, particularly with the advent of cloud services. The age of the ECPA is felt in two ways. First, the statute's provisions govern access to remotely stored communications based on the age and status of the communication. For example, if an email is stored in the cloud and has been opened or is older than 180 days, the U.S. government only needs a subpoena to request the provider for those communications. A warrant is only required for un-opened communications less than 180 days old ("Electronic Communications Privacy Act (ECPA)" n.d.). These provisions reflect a pre-cloud computing era when storage was expensive and users stored communications locally. The result is electronically stored communications being more accessible to law enforcement than physical communications when the former has become the dominant method. The original privacy provisions of the ECPA were not protecting individual

privacy as intended because they still reflected an antiquated understanding of electronic communications.

Second, pre-cloud computing ECPA legislators did not anticipate the global nature of electronic communications. Provisions intended to protect the privacy of U.S. citizens were written with insufficient specificity distinguishing domestic users of U.S.-based electronic communications providers and non-U.S. users. Interpretation of the provisions prohibits U.S.-based providers from disclosing user data to non-U.S. governments even when law enforcement is investigating a crime committed outside of the U.S. with all parties being foreign nationals. This interpretation amounts to a blocking provision that requires non-U.S. governments to rely on diplomatic processes like Mutual Legal Assistance Treaties (MLAT) (Daskal 2016). The MLAT process is inefficient. Fulfillment can take up to ten months to complete and the U.S. receives three times as many requests as is filed with foreign governments (Nojeim 2015). The combination of global cloud computing market dominance of U.S. providers and the blocking statute nature of the ECPA provisions exacerbated the need for ECPA reform. Firms were caught between U.S. legislation that advantaged the U.S. government's reach to obtain foreign personal data while disadvantaging the ability for non-U.S. governments to access data belonging to their own citizens that happened to be collected and stored by U.S.-based firms.

The Top Firms have expressed frustration with existing legislation and have used their lobbying resources to advocate for specific reforms of surveillance and cross-border data transfers. The enacted USA Freedom Act of 2015 was present as an issue on lobbying disclosures for Apple, Facebook, Google, and Microsoft. The USA Freedom Act primarily addressed FISA Section 215 telephony surveillance but also reformed electronic communications surveillance by requiring more transparency from the Foreign Intelligence Surveillance Court and requiring amici curiae to advise the court. Recipients of non-disclosure orders were also offered more allowances for reporting transparency (Lovells 2015). The Law Enforcement Access to Data Stored Abroad (LEADS) Act was present as an issue on lobbying disclosures for Facebook, Google, and Microsoft. The LEADS Act would have reformed the ECPA by preventing the U.S. government from accessing data from U.S.-based "Internet Services" if the data is stored abroad and access violates the law of the country the data is located or the data is owned by a non-U.S. person. This would have required more U.S. government reliance on an inefficient MLAT process, so improvements to MLATs were included in the LEADS Act as well (Nojeim 2014). The ECPA Amendments Act was present as an issue on lobbying disclosures for Facebook, Google,

and Microsoft. The ECPA Amendments Act was more privacy focused than the cross-border access focused ECPA reform bill. This act would have prohibited voluntary disclosure of personal data to law enforcement by firms, eliminated the 180-day distinction for warrants, reformed delayed notice procedures to limit the use of non-disclosure orders, and established comptroller transparency and accountability. Notably, the ECPA Amendments Act would not have applied to the Wiretap Act or FISA (“Summary of Electronic Communications” n.d.). The Email Privacy Act (EPA) was present as an issue on lobbying disclosures for Apple, Facebook, Google, and Microsoft. The EPA amends the ECPA by eliminating the 180-day distinction between communications, essentially requiring a warrant for communications regardless of their age. The EPA passed unanimously in the House in 2016 but the Senate version was stalled when amendments that would broaden warrantless access in emergency requests and expand the power of National Security Letters were introduced (Myers 2017). The enacted Judicial Redress Act of 2015 (JRA) was present as an issue on lobbying disclosures for Apple, Facebook, Google, and Microsoft. JRA offers citizens of the EU rights of civil action and the same redress that U.S. citizens are provided under the Privacy Act of 1974 (Bender 2015). The JRA was an essential part of the Privacy Shield agreement which replaced the Safe Harbor agreement that was invalidated after the Snowden disclosures. Privacy Shield allows companies to self-certify compliance for transatlantic data flows and is utilized by Facebook, Google, and Microsoft (“Privacy Shield List” n.d.). The International Communications Privacy Act (ICPA) was present on lobbying disclosures for Facebook, Google, and Microsoft. ICPA was introduced in both the House and the Senate in May 2016 (“S.2986” n.d.). The ICPA provided access to data of U.S. persons regardless of where the personal data was stored. If the personal data belonged to a non-U.S. person, the requesting law enforcement agency would be required to contact the data subject’s country of citizenship to offer the opportunity to object, prompting a comity analysis. To address the inadequacies of the MLAT process, the ICPA uses two strategies. The first strategy involved bilateral agreements between the U.S. government and a foreign government committing to reciprocal rights of access, notice, and challenge when each government requests data belonging to a citizen of the other government’s country. One such agreement has already been established with the United Kingdom (Hatch 2017b). Second, ICPA has provisions to update and improve the MLAT process, including the creation of an online docketing system for increased accessibility, transparency, and accountability (Hatch 2017a).

The ICPA has recently been supplanted by the CLOUD Act introduced in February 2018 by Senator Orrin Hatch and Representative Doug Collins. Senator Hatch sponsored the ICPA

and the LEADS Act, making the CLOUD Act the most recent iteration of legislation addressing cross-border data access by law enforcement. The CLOUD Act was present as an issue on lobbying disclosures for Apple, Facebook, Google, and Microsoft but has some notable differences from the ICPA. The CLOUD Act is similar to the ICPA in that both bills choose not to rely on the location of data to determine U.S. government access to data. The CLOUD Act places more responsibility on the firm. The firm can move to quash a warrant if the firm believes that complying with a data request would result in a conflict of laws, but explicit language of the bill restricts comity claims to non-U.S. governments who have established a bilateral agreement with the U.S. executive branch. Non-U.S. governments without a bilateral agreement are still eligible for common law comity motions to quash, but it remains to be seen how those will be handled differently. As with the ICPA, the CLOUD Act attempts to make non-U.S. government requests for data held by U.S.-based firms more efficient by allowing non-U.S. governments, who have an established bilateral agreement, to circumvent the MLAT process and request data directly from firms like the U.S. government is able to do. The exception being that U.S. citizens are offered more protections from non-U.S. governments requesting data than non-U.S. citizens are offered from U.S. government requests. The ICPA had provisions to improve the MLAT process where the CLOUD Act does not (Daskal 2018). The lack of MLAT reform could incentivize non-U.S. governments to agree to bilateral agreements with the executive branch that offer more expeditious data disclosure.

The CLOUD Act may be supported by all four of the Top Firms, but the bill has faced opposition by several privacy and human rights advocacy groups including the ACLU, the Electronic Frontier Foundation, and Amnesty International. In a coalition letter, twenty-four organizations expressed their disagreement with “technology companies” who stated the CLOUD Act was progress in protecting human rights. The groups’ objections highlight the power given to the executive branch when choosing countries for bilateral agreements; the enhanced access to data by foreign governments that are considered more lenient than current U.S. law; and the power to challenge data requests to be solely at the discretion of firms with no resource for individual users (“Coalition Letter Opposing” 2018). Despite opposition from privacy and human rights advocacy groups, the CLOUD Act was included in a 2018 Omnibus spending bill passed by Congress and signed into law by President Trump to avoid a government shutdown. Privacy focused members of Congress, like Senators Ron Wyden and Rand Paul, objected to the inclusion because doing so precluded meaningful debate (Hatmaker 2018).

In 2017, thirty-one firms co-signed a letter to Representative Bob Goodlatte calling for reform of FISA Section 702. Suggested reforms included codifying limitations on “about” collection in the Upstream program, judicial oversight of government queries of Section 702 collected data, narrowing the definition of “foreign intelligence information,” and increases in transparency and oversight (“Dear Chairman Goodlatte” 2017).

After co-signing the May 2017 letter to Representative Goodlatte that suggested preferred reform measures for Section 702, the Top Firms were largely absent from the FISA reauthorization debate. The Top Firms were not invited as witnesses to testify at a Senate Committee on the Judiciary hearing in June 2017 or a House Judiciary Committee hearing in March 2017 covering FISA Section 702 expiration, reform, and reauthorization (“FISA Amendments Act” 2017; “Section 702 of the Foreign Intelligence Surveillance Act” 2017). Panel two of each hearing witnessed testimony from think tanks, law schools, private law practices, a former general counsel at NSA and former Director of the National Counterterrorism Center, a professor at the U.S. Naval Academy, and Privacy and Civil Liberties Oversight Board member. Some witnesses advocated for privacy focused reforms, but the absence of the Top Firms leaves out the testimony of key stakeholders. The Top Firms transmit communications that are caught in upstream collection and collect and store data that is requested via PRISM. Because their mass data collection makes them valuable targets, the Top Firms’ business reputations were called into question after the Snowden disclosures and the ramifications of perceived complicity with U.S. government surveillance continues to impact their ability to operate in non-U.S. countries. The inclusion of testimony from Top Firms would not have been unprecedented. Microsoft and Google testified in ECPA reform hearings covering similar subject matter - U.S. government access to data belonging to non-U.S. citizens. Apple testified as a witness at a House Judiciary Committee hearing covering encryption and the balance between privacy and security (“The Encryption Tightrope” 2016).

In October 2017, the USA Rights Act and the USA Liberty Act were introduced to reform FISA 702 prior to reauthorization. The former bill included the U.S.-based firms’ suggestions to codify “about” collection restrictions, required warrants for backdoor searches of Section 702 collected data and reverse targeting of Americans with exceptions only for emergencies, and increased transparency and oversight (“The USA Rights Act” 2018). As with the USA Rights Act, the latter bill also codifies the end of “about” collection and adds additional transparency and oversight mechanisms. Unlike the USA Rights Act, the USA Liberty Act adds less restrictive

limits on intelligence agency queries by exempting non-content data and queries that are not looking for evidence of a crime, which is considered a broad exemption (Reitman 2017b). Both the USA Rights Act and the USA Liberty Act included reforms that the Top Firms have publicly supported but neither was explicitly named in 2017 Q4 lobbying disclosures for any of the Top Firms. Rather, lobbying disclosures listed broader references to FISA 702. Apple's lobbying disclosure listed "Issues related to government requests for data" ("Apple, Inc." 2017). Facebook's lobbying disclosure listed "reform government surveillance programs" and "Foreign Intelligence Surveillance Act of 1978, Section 702" ("Facebook, Inc." 2017). Google's lobbying disclosure listed "Transparency related to Foreign Intelligence Surveillance Act" ("Google, Inc." 2017). Microsoft's lobbying disclosure listed "Legislative proposals related to government surveillance and data collection, including issues of transparency and FISA reform" ("Microsoft Corporation" 2017).

The Top Firms may not have lobbied for either the USA Rights Act or the USA Liberty Act explicitly, but they did support reforms within the bills. In October 2017, the coalition Reform Government Surveillance publicly expressed support for the USA Liberty Act but did not explicitly express support for the USA Rights Act ("Reform Government Surveillance Statement" 2017). A month later, the coalition expressed "significant concerns" with the FISA Amendments Reauthorization Act of 2017 and its lack of meaningful restrictions on queries of Section 702 collected data; lack of codifying the end of "about" collection; and an expansion of targeting allowances for U.S. government surveillance ("Statement on FISA Amendments" 2017). In January 2018, the FISA Amendments Reauthorization Act of 2017 was passed by Congress and signed into law by President Trump extending authorization until 2023 (Liptak 2018).

Table 16 summarizes significant bills related to surveillance reform and cross-border data access that have been explored in more detail throughout this section.

Table 16: Lobbied Legislation based on Lobbying Disclosures

Bill	Current State	Lobbying Firms
USA Freedom Act	Became Law 2015	Apple, Facebook, Google, Microsoft
LEADS Act	Introduced 2015	Facebook, Google, Microsoft
ECPA Amendments Act	Introduced 2015	Facebook, Google, Microsoft
Email Privacy Act	Passed House, Stalled Senate	Apple, Facebook, Google, Microsoft
Judicial Redress Act	Became Law 2016	Apple, Google, Microsoft
Int'l Comm. Privacy Act	Introduced 2017	Facebook, Google, Microsoft
CLOUD Act	Became Law 2018	Apple, Facebook, Google, Microsoft
USA Rights Act	Introduced 2017, Attempted Amendment to Replace S.139 FISA Reauthorization Act '17	N/A <i>*Facebook, Google, Microsoft have supported similar reforms but not explicitly this bill</i>
USA Liberty Act	Introduced 2017	N/A <i>*Facebook, Google, Microsoft have supported similar reforms but not explicitly this bill</i> <i>*RGS publicly supports</i>

Sources: "Congress.gov." Library of Congress, Accessed on 2018 Mar 21;

"Lobbying Disclosure." Office of the Clerk US House of Representatives, Accessed on 2017 Sep 15

The political affordance has been a predominately positive affordance resulting in more desirable outcomes to the Top Firms than the legal affordance. The Top Firms have invested millions into lobbying Washington and have recruited experienced former U.S. government staffers - including a former Congressperson - to staff the majority of their lobbying personnel. Investment in the political affordance has been a success. Issues and legislation lobbied for by the Top Firms have been enacted or progressed in Congress. Addressing congressional committees through letters and testimony has heavily influenced the framing and passage of legislation. The enactment of the CLOUD Act not only represented years of lobbying for ECPA reform, but also directly addressed the issue raised by the United States v. Microsoft case formerly before the U.S. Supreme Court. Political affordance actions can avoid the undesirable outcomes of the legal affordance because crafting legislation allows for a dialogue and consideration of multiple stakeholder needs in a complex adaptive business environment. Where the legal affordance is a more adversarial, zero-sum process with the U.S. government,

the political affordance includes multiple voices from the business ecosystem to find a balanced solution for the business environment as a whole.

FISA 702 reform was difficult to rate. Compared to the investment in ECPA reform, the Top Firms were not active participants in FISA reform measures. This absence is more poignant when one considers that FISA 702 is the surveillance authority that was linked to the Top Firms in the Snowden disclosures and that FISA reform was explicitly suggested by both the EU Commission and the Working Party 29 to continue cross-border data transfers. It would be false to say that the Top Firms fully abdicated resistance to FISA 702 surveillance. FISA reform was listed on lobbying disclosures and the coalition Reform Government Surveillance (RGS) was actively representing the positions of the Top Firms and influencing the language in the FISA reform acts. However, these actions did not result in desirable outcomes. FISA 702 reform efforts lacked invitations to hearings on Capitol Hill and FISA 702 reauthorization lacked reform. Not only were none of the reform suggestions from RGS included in FISA reauthorization, but FISA 702 surveillance authorities actually expanded. The root cause of these outcomes is unclear. Was the power and influence of the Top Firms simply not enough to affect FISA 702 reform the same way the Top Firms influenced ECPA reform? Or did the Top Firms withhold that power and influence for a strategic reason? The Top Firms may have avoided drawing attention to FISA reform because of what is at stake in Europe. If the firms had little faith that Congress would enact reform measures that limit U.S. government surveillance allowances, they may have opted not to draw specific attention to FISA Section 702 flaws only to have those flaws continue without reform (O'Brien 2017). If avoiding attention was the motivating factor behind limited FISA 702 reform engagement, the Top Firms opted for a high risk strategy that ignores the principles of complex adaptive systems. Since 2012, 2017 was the first opportunity for debate, reform, or expiration of Section 702 (Richardson 2017). Presuming that FISA 702 reform efforts would fail and then choosing not to act in hopes that regulators would overlook the FISA reauthorization indicates that the Top Firms were not expecting surprise, limiting their ability to adapt. Instead, the Top Firms have allowed FISA 702 surveillance to expand without another opportunity for reform for another five years, all while relying on EU regulators to act less punitive than if the Top Firms actually tried and failed at reform efforts. If the already undesirable FISA 702 reauthorization outcomes lead to more undesirable regulatory outcomes, it is hard to pin those failures on the political affordance given the desirable outcomes achieved in ECPA reform. The Top Firms failed to take advantage of a positive affordance.

Under the political affordance, the Top Firms served as poor corporate avatars. Support for privacy-focused reform bills like the USA Freedom Act, the ECPA Amendments Act, and the Email Privacy Act may reflect some commitment to individual privacy. However, at best those bills are beneficial to both the firms and individual citizens, reinforcing the belief that firms will only serve as corporate avatars when it suits them. Advocating for more restrictions to U.S. government surveillance benefits firms by establishing a public foundation of privacy advocacy while limiting the U.S. government's reach, which has threatened the surveillance capitalist model. After the Snowden disclosures, firms were caught in between U.S. government security priorities and individual privacy rights. Laws that restrict the ability of U.S. government surveillance to request data remove firms from what had been a highly compromised position. When privacy is negotiated and informed through lobbying and public hearings, firms can enjoy the benefits of advocating for privacy while avoiding the hidden dangers or risks faced through the legal affordance. Low risk, high reward actions do not make for a true corporate avatar.

The Top Firms' support for the LEADS Act, the Judicial Redress Act, the International Communications Privacy Act, and the CLOUD Act has been less about individual privacy and more about cross-border data transfers. These bills limit U.S. government access to personal data either stored outside of the U.S. or belonging to a non-U.S. citizen and provide non-U.S. citizens with similar rights afforded to U.S. citizens under the Privacy Act of 1974. However, these bills are prioritized by the Top Firms because they resolve global issues that led to increased regulation, localization demands, and the potential for conflict of law situations. The Top Firms frame these changes as privacy focused because they are improvements to the existing issues created by an outdated ECPA. These improvements do more to relieve international state level tensions concerning data protection that have been troublesome for firms. Advocates of privacy and human rights believe the firms have fallen short in their role as corporate avatars. Twenty-four privacy and human rights advocacy groups strongly opposed the CLOUD Act despite the Top Firms saying the bill was privacy conscious. These groups claimed that the ability to circumvent the MLAT process as written in the CLOUD Act puts the privacy of non-U.S. citizens at risk. They also disagree with the reliance on firms to challenge data requests of non-U.S. citizens and believe recourse should be granted to the individuals targeted. Privacy and human rights advocacy groups agree that the ECPA is inadequate and have expressed support for ECPA reform (Turner 2017). They have publicly favored the more privacy focused Email Privacy Act (Cope 2017). With such prominent privacy and human rights groups strongly

opposing the CLOUD Act in ways never expressed about the LEADS Act or the ICPA, it is difficult to trust that the Top Firms truly had privacy in mind all along when they expressed unwavering support for the CLOUD Act's provisions that are more focused on avoiding conflicts of law and easing international tensions than individual privacy rights.

C. Technical Affordances

Technical affordances are leveraged through engineering changes that limit or prohibit surveillance, specifically the use of encryption and anonymization. The Top Firms have the capacity to resist surveillance through technical means that impacts the legal affordance and the political affordance. When evaluating their role as corporate avatars, the approach toward the Top Firms will be more instructive than previous affordances because firms have more agency via the technical affordance. The ability of firms to resist surveillance via the legal affordance is highly dependent on existing law and applicable precedent. The ability of firms to resist surveillance via the political affordance is highly dependent on their ability to influence the political will of lawmakers. Being the Top Firms in the platform technology sector puts Apple, Facebook, Google, and Microsoft in a well-resourced position to unilaterally engineer surveillance resistant privacy technology into their platforms. However, privacy-by-design engineering may restrict both U.S. government surveillance and surveillance capitalism. Are firms willing to adapt their own business practices to stifle surveillance? How do differences between firms inform their approach to privacy? The technical affordance presents a unique situation where the surveillance capitalist models of firms is executed differently between firms depending on how each firm generates revenue.

After the Snowden disclosures, the Top Firms used the technical affordance to respond quickly. To assure users the Top Firms would protect them, firms explained how encryption can protect privacy against upstream and downstream surveillance. Apple posted a message for their customers in June 2013 emphasizing that communication services like iMessage and Facetime are end-to-end encrypted, meaning Apple cannot decrypt the data and only the sender and recipient have the decryption keys ("Apple's Commitment to Customer Privacy" 2013). Apple's Mac OS and iOS support full disk encryption to protect the data on consumer devices. Apple iCloud data like photos, contacts, notes, and backups are encrypted in transit and all but mail are encrypted at rest ("This is How We Protect" n.d.). End-to-end encryption is available for iCloud services handling the most sensitive personal data such as payment information,

passwords stored in keychain, and Siri information as long as two-factor authentication is enabled (“iCloud Security Overview” n.d.).

Microsoft announced expanded use of encryption and referred to government surveillance as an advanced persistent threat akin to malware or cyber-attacks. Microsoft’s changes included encrypting customer content in-transit between customers and Microsoft and between Microsoft’s data centers. These data in-transit changes were announced late in 2013 and were promised to be completed by the end of 2014. Data at rest stored by Microsoft was also encrypted and Microsoft discussed partnering with other companies to protect data going from one email communications service to the other (Smith 2013). Partnering with other email providers to encourage the use of encryption is beneficial for the Top Firms because if only one provider in email exchange is encrypting the communication in-transit, the email is vulnerable to surveillance (“Email encryption in transit” 2018). In 2018 Microsoft announced that end-to-end encryption would be available for Skype calls and chats as a feature called “Private Conversations” using the same encryption system as a top secure messaging app called Signal. Note that unlike Apple’s Facetime, Microsoft’s end-to-end encryption is not the default and is designed as an additional feature. Microsoft will still have access to metadata from the conversation including when the conversation occurred and the duration, but the content will be inaccessible to Microsoft (Newman 2018b). Voice calls and chat in Skype were already encrypted in-transit although voice calls are stored unencrypted (“Does Skype use encryption” n.d.).

In 2014, Google committed to always using HTTPS encryption in-transit when users send or receive emails and when Gmail data travels internally between Google servers (“Staying at the Forefront” 2014). Google was also the first major cloud service provider to use Perfect Forward Secrecy (PFS) encrypting data in transit between Google servers and other providers (“Security”, n.d.). PFS is even more surveillance resistant than other in-transit encryptions because PFS uses ephemeral session keys. With other forms of encryption, the same key can decrypt a great deal of the encrypted communication. In those cases, any encrypted data collected during upstream surveillance could potentially be decrypted if the key were ever compromised in the future. With PFS, those with access to the PFS keys cannot generate the same key used to initially encrypt the original session making collection of PFS encrypted data even less useful (Higgins 2013).

Facebook set connections between users and Facebook to be encrypted by default using HTTPS. Facebook also forced their third-party developers to support HTTPS within a ninety-

day period and committed to implement the same PFS encryption as Google (“Secure Browsing” 2013). For the Facebook Messenger app, Facebook added an option to enable the same end-to-end encryption system used in Signal that would eventually be incorporated into Skype. As with Skype, end-to-end encryption is not enabled by default, but the added privacy options still make the enhanced encryption accessible to the general public, giving users the option for stronger privacy protection (Greenberg 2016b).

With the exception of Apple’s use of end-to-end encryption for iMessage and FaceTime, the Top Firms’ expanded uses of encryption were applied to in-transit data, at rest data that the firm can decrypt, or encryption requiring the user to opt in. None of these three encryption implementations materially limit the Top Firms’ access to valuable personal data assets. Encryption at rest protects data from unauthorized access, but if the firm controls the key management then the firm has access to the underlying encrypted data. Google positioned server side encryption of Google Cloud as a service that “frees you from the hassle and risk of managing your own encryption and decryption keys” (“Google Cloud Storage” 2013). If the firm controls the cryptographic keys protecting user data, it is vulnerable to National Security Letters or PRISM surveillance. Encrypting data in-transit diminishes the value of FISA Section 702 upstream collection that monitors the internet backbone because it protects communications traveling between the user’s device and the firm’s servers (“HTTPS encryption” n.d.). The Top Firms can implement encryption in-transit and become more resistant to upstream surveillance without any negative impact on their surveillance capitalist business models, making it easier to implement encryption by default.

It is noteworthy that Facebook, Microsoft, and Apple offered end-to-end encryption for services but required either opt in to the encryption itself or two-factor authentication. Requiring users to opt in to privacy settings rather than setting privacy as a default requires users to be informed and invested enough to opt in. This is an advantageous position for firms because the privacy features are available for the users most concerned about surveillance without locking the firm out of all user data that firms use to improve their platform and serve advertisements on behalf of clients. Most users do not opt in to privacy features that are not the default. According to a Google engineer speaking at a conference in January 2018, 90 percent of active Gmail accounts do not have two-factor authentication enabled (Ong 2018). By offering privacy features that only the most privacy conscious or informed users utilize, firms can

position themselves as privacy conscious without losing broad access to valuable personal data assets.

All four of the Top Firms exploit personal data and behaviors to maintain and expand their market position. Apple's approach is different because, unlike Google or Facebook, Apple's revenue is not driven by an advertising model. Instead, Apple leverages user data to build network effects that incentivize users to stay within a walled garden of only Apple hardware and services (Murphy 2017). Apple's business model allows the firm to market privacy as a competitive advantage. A prominent section on Apple's site is dedicated to privacy and states that Apple believes "privacy is a fundamental human right" and "great experiences don't have to come at the expense of privacy and security" ("Apple Products are designed" 2018). The two Apple services that offer private end-to-end encryption by default - iMessage and FaceTime - are communication services that are only available within Apple's iOS and OS X operating systems on Apple hardware. iMessage is one of Apple's most effective walled garden services that incentivizes users and the people users communicate with to use only Apple products (Goode 2016). The importance of using Apple services to drive hardware sales is evident in an interview where Apple CEO Tim Cook identifies Google, and not Samsung, as their primary competitor because Google's Android operating system "enables" hardware firms like Samsung to compete with Apple. Later in that same interview, Cook addresses questions about surveillance by emphasizing that users are not the product and that Apple's business is not based on having information about users (Colt 2014). Cook's statement does not mean that Apple does not collect or utilize user data. Apple acknowledges that user information is critical to improving its business, but user privacy is an imperative (Greenberg 2017). Apple does not benefit from indiscriminate mass data collection the same way other Top Firms do by using that data to drive their business. Apple is vertically integrated and controls the full stack - hardware, software, and services - allowing them to collect only the data they need to improve that stack and implement collection with a privacy conscious approach when fortifying their network effects.

In 2016, Apple began using a privacy focused technique called differential privacy. When both Mac OS or iOS users opt into sharing data with Apple to improve services, the data Apple uses to inform improvements undergo several steps to anonymize the data. First, device identifiers are dropped from the information. Next, statistical noise is added to cloud the user's contribution on device and metadata is dropped. Finally, the clouded data is sent to Apple where access to that data is limited. The aggregate data from many users allows Apple to remove the

noise and retain the valuable insights without being able to de-anonymize user contribution. On top of the sharing process, Apple sets a daily budget limiting the contributions a user can provide to Apple. This prevents an active user with a statistically high number of contributions from theoretically providing enough data that the removal of noise allows for revelation of aggregate insights into that single user (“Differential Privacy” n.d.). As with the other Top Firms, Apple exploits user data to broadly improve hardware, software, and services to reinforce network effects. Unlike the other Top Firms, targeting individual users is not necessary to Apple the same way it would be for advertising or search engine optimization. This difference allows Apple to experiment with privacy focused techniques that may not be usable for other Top Firms. User data is still critical to Apple’s market dominance; the difference is how that data is exploited.

Google and Facebook’s business models are based on leveraging user data for an advertising model, so their ability to implement privacy-by-design is more limited than Apple. For these firms, user information is used to optimize targeted advertising. Crucially, neither Facebook or Google sell user information to third parties (“Does Facebook sell my information” n.d.; “How Ads Work” n.d.). Selling a valuable asset like personal data would be counterproductive. Rather, Google and Facebook run their own ad networks that provide advertisers with tools for targeted advertising that are grounded in each firm’s collection of user data. For instance, Facebook’s ad targeting offers businesses the ability to target three types of audiences. First is a “core audience” that allows for targeting based on data like age, gender, location, and behaviors. Second is a “custom audience” of a business’s existing customers using data from customer relationship management (CRM) software like email addresses or phone numbers. Third is a “lookalike audience” that identifies personal data attributes and behaviors that match a business’s custom audience to reach new customers (“Choose Your Audience” n.d.). Facebook must be able to access their users’ identifiers in plain text to serve targeted advertising based on external plain text, making end-to-end encryption or even anonymization unworkable. According to Google’s Privacy Policy and User Terms, Google uses data points like location data, search terms, and advertising device identifiers to target ads for advertising clients. Server logs are “anonymized” by removing IP addresses and cookie information, but not until after nine to eighteen months (“Advertising” n.d.).

Mass collection and exploitation of user data is so critical to Google and Facebook’s business models that any claims of privacy prioritization are diminished not only by a lack of privacy-by-

design techniques, but also by each firm's own actions. In June 2014, Google announced a project to build end-to-end encryption into Gmail. After three years, Google seemingly abandoned the project and made the code open source with sources inside Google claiming that the project received little support over time (Greenberg 2017). In 2016, Google merged the personal data it collected with anonymous site tracking data it owned after purchasing the ad network DoubleClick in 2007. Initially Google chose to keep its own data and the purchased DoubleClick data separately. However, facing enhanced targeting capabilities from other firms like Facebook, Google reversed that position, essentially identifying the previously anonymous tracking data. New users were opted-in by default. Existing users were opted-out by default, but invited to opt-in with prompts that emphasized "new features" and not de-anonymization (Angwin 2016). In 2013, Facebook acquired the Virtual Private Network (VPN) app Onavo and since 2016 Facebook has encouraged Android Facebook users to use Onavo via a "Protect" prompt. In 2018, iOS Facebook users were also offered a "Protect" prompt and were encouraged to use Onavo as a VPN. Shortly after appearing on iOS, researchers noticed that the VPN monitors and tracks users as they visit websites and use apps collecting and sending the data back to Facebook. A VPN is typically considered a privacy tool designed to limit the observation of user traffic. Trust is usually placed in the VPN with many providers choosing not to keep any logs as a privacy feature (Newman 2018a). Marketing a VPN using a prompt titled "Protect" and then collecting browsing and app usage data to fuel Facebook is a misleading promotion of a false privacy tool. Facebook and Google's ad based surveillance capitalism limits both firms' ability to resist surveillance using the technical affordance. Abandoned end-to-end encryption, de-anonymization of data, and misleading privacy tools that collect user data highlights the limits of privacy when faced with the insatiable desire for personal data in a targeted advertising model.

Microsoft's business model is not as easily parsed as Apple, Facebook, and Google. Traditionally, Microsoft's revenue came from licensing its software to Original Equipment Manufacturers (OEM) who made the hardware. In 2015, Microsoft transitioned to a new strategy that competes on all technology fronts after falling behind Google and Apple in the mobile market. On one front, Microsoft is emulating Apple's model of free software installed on Microsoft branded hardware to bring in new users and create their own walled garden ecosystem. On another front, Microsoft diverges from Apple's model - using software and services to drive hardware sales - and leverages the user introduction to Microsoft's software to upsell more premium versions via a subscription model. Services like cloud versions of

Microsoft Office would compete with Google's productivity suite but with paid upgrades instead of a data for access exchange. Use of these services also exposes users to other Microsoft business lines like the Cortana voice assistant, Bing search, and Skype communications (Warren 2015). A third front for Microsoft adopts a Google/Facebook model with the Windows Bing search engine, serving targeted advertising that offers location and device targeting as well as custom targeting where the client uploads existing customer identifiers ("Ad solutions for internet advertising" n.d.). User data is critical for Microsoft as the firm takes on the other three Top Firms. The walled garden and subscription revenue models require user data to improve software and services to compete with an established platform like Apple or a free platform like Google. The advertising model requires personal data to target advertising and compete with Google and Facebook, both of whom have platforms that encourage users to share. However, as Windows 10 rolled out, Microsoft faced criticism for deceptive tactics like forcing OS upgrades that increased the amount of data being sent from the user's machine back to Microsoft if the user opted in to personalization via the voice assistant Cortana. After the forced OS upgrade process, users were prompted to opt-in to personalization that authorized location data, text input, voice input, and touch input to be sent back to Microsoft (Kalia 2016). Shortly after the initial rollout that caused the personal data controversy, Microsoft's Windows 10 Anniversary update escalated the forced data collection by opting-in to Cortana by default and removing Cortana's on/off button, thus forcing users to limit Cortana's data collection in settings or to edit the Windows registry as a hack workaround (Chacos 2017). Mining user data became such an integral part of building Microsoft's new business model to catch the other firms that it fractured user trust to obtain the data. Microsoft may make privacy claims by using industry standard encryption for data in-transit and at rest, but the means by which Microsoft chose to access user data calls their commitment to individual privacy into question ("Microsoft Trust Center" n.d.). By choosing both the Apple business model and the Google/Facebook business model, Microsoft put itself into a precarious competitive position. Microsoft will not be able to compete with Apple on privacy because their advertising component requires access to plain text personal data, but the subscription model and walled garden approaches limit the number of users Microsoft's advertising can target. This results in an inferior product to Facebook and Google. Considering Microsoft's disadvantaged market position and the deceptive methods employed to collect user data, it is difficult to trust that Microsoft will proactively implement more privacy-by-design techniques to resist surveillance. Even when Microsoft added end-to-end encryption to Skype, the announcement was at least five years after the Snowden disclosures and it was

offered as a tool and not by default. In contrast, Apple offered end-to-end encryption in its own messaging and video calling services by default prior to the Snowden disclosures.

Apple's business model and commitment to privacy may allow for implementation of proactive technical affordance methods to resist surveillance, but there is potential for the technical affordance to become a false affordance. In his 2011 paper, Christopher Soghoian discussed the choice firms had to implement more encryption technologies. Soghoian wrote that if the firm encrypts user data without the ability to decrypt the data, the firm is not legally obligated to ensure the government has the ability to decrypt the data (Soghoian 2015, 9). Five years later, the FBI was prepared to bring Apple to court when the firm refused to build a software tool the FBI could use to break iOS full disk encryption. In a testimony before the House Judiciary Committee, Apple's Senior Vice President and General Counsel Bruce Sewell defended the firm's refusal stating, "Weakening encryption will only hurt consumers and other well-meaning users who rely on companies like Apple to protect their personal information" (Sewell 2016). Commenting on Apple's refusal to comply, a former General Counsel of the NSA believed that if firms had the power to encrypt all user data, it comes with a responsibility to "do some of the work that had been done by the intelligence agencies" (Menn 2016). These two statements highlight the dilemma of privacy-by-design as both a strength and a weakness that protects the identity and communications of the public and bad actors alike. Techniques like encryption are ambiguous. Weakening encryption weakens it for everyone and strengthening encryption strengthens it for everyone (Rosen 2017). Privacy advocates like Soghoian can point to the Snowden disclosures and call on firms to implement better encryption in their products and services. However, if the balance between privacy and security swings too far to either side, the technical affordance can be revealed as a false affordance. Apple's use of end-to-end encryption for communications and full disk encryption on its devices forced the FBI to push for a more drastic solution, thus creating a national debate. The Director of the FBI framed their encryption demand of Apple as justice for fourteen slaughtered victims whom America owed a professional investigation (Comey 2016). The Top Firms may be able to unilaterally implement privacy focused technical affordance actions to resist surveillance, but doing so does not guarantee the U.S. government will simply move on. Building privacy-by-design into a platform may be an effective action to resist surveillance, but the emerging feedback may necessitate escalation from stakeholders throughout the business environment. The U.S. government has a national security mission that is hampered by privacy-by-design techniques. The potential of U.S.-based technology platforms to serve as a surveillance resource has proven to be a valuable

tool for intelligence agencies and law enforcement. The reaction of firms and non-U.S. governments to the Snowden disclosures is a threat to the existing valuable resources of U.S.-based electronic communications platforms. Additionally, surveillance resistant techniques like end-to-end encryption create potential safe havens for individuals who would otherwise have been surveilled. The U.S. government is unlikely to allow technology to become a net negative resource without some resistance.

Encryption and anonymization are methods the Top Firms have at their disposal to resist surveillance depending on their willingness to adapt their business model or self-impose limits to their surveillance capitalist incentive structures. However, the technical affordance includes a privacy-by-design technique that, rather than being a mode of resistance, may serve as its own incentive for resistance. The threat of U.S. government surveillance was used opportunistically by non-U.S. governments to make localization demands of the Top Firms. Localization is positioned by governments as a means to achieve privacy and security but the motivation is sovereignty and access control. Localizing data would not limit surveillance as suggested. If coupled with data protection laws limiting access by foreign governments, localization may prevent the Top Firms from complying with data requests, but that does not limit the totality of surveillance. Centralizing data into fewer locations increases the risk of hacking as the method of surveillance. Non-U.S. governments with poor human rights records exploit the façade of privacy and security to legislate localization that offers them more access to their own citizens' data (Sargsyan 2016, 2225-2230).

Google's distributed network architecture emphasizes security and efficiency to serve users at Google's scale, but protectionism like localization threatens Google's operations. Google's network breaks up data files into smaller pieces and then stores, replicates, and moves them to enhance the network performance. Since the data is broken into smaller pieces that constantly move, isolating locations for data becomes difficult, helping to prevent unauthorized access like hacking but is incompatible with protectionism (Hölzle 2018). Localization demands fundamentally challenge the benefits derived from Google's network. These threats have already appeared through the legal and political affordances. Google's citation of the 2nd Circuit Microsoft decision presented complications for lower courts because the distributed network was incompatible with a sovereignty decision predicated on location of data, leading to an unfavorable result in all six lower court challenges. Google's support for the CLOUD Act is

rooted in their desire to frame U.S. government access to data away from a location based approach (Hölzle 2018).

The exposed actions by both the U.S. government and the Top Firms forced reactionary responses from non-U.S. governments to push for localization, either for protectionist or exploitative reasons. Executing a distributed network architecture can be threatening to firms if protectionism persists or escalates, particularly in the largest international markets. For firms like Google, use of that architecture increases the stakes of resisting surveillance to prevent non-U.S. governments from enacting location based laws that are incompatible with the operation of their platforms. However, Google's network architecture also limits their ability to resist surveillance in the first place, as seen in the legal affordance. Microsoft leveraged the fact that they store user data based on the stated location of the user to appeal a government request for data to the U.S. Supreme Court. Google's architecture prevented them from successfully applying Microsoft's position when challenging U.S. government requests in several courts. Having more storage flexibility protects access to international markets. Apple has been compliant with localization demands in China to protect access to that market. For all the benefits, a distributed network architecture comes with tradeoffs and risk for multinational technology firms.

The technical affordance was a positive affordance for all firms when resisting upstream surveillance. All four Top Firms increased the use of encryption in-transit to limit the utility of monitoring the internet backbone. When the Top Firms implemented in-transit encryption like HTTPS, many of them set timelines for partners to implement HTTPS as well. The actions taken by the Top Firms can have desirable privacy outcomes throughout the business ecosystem. When the technical affordance was applied to resisting U.S. government requests for data through methods like National Security Letters or PRISM, the affordance was highly contingent on the surveillance capitalist business model of the firm. Apple's walled garden model allows for stronger privacy-by-design and the use of privacy as a competitive differentiator. Facebook and Google's targeted advertising models severely limited their ability to resist data requests using the technical affordance. Microsoft's aggressive mixed model led to undesirable outcomes for both their surveillance capitalism and their ability to resist U.S. government surveillance. End-to-end encryption and anonymization are inconsiderable for firms whose revenue is produced by selling access to users as the product. To offer the automated functionality of Facebook and Google's efficient ad network, the firms require access to plain text personal data to cultivate

advertising based direct and indirect identifiers. End-to-end encryption or anonymization techniques would have undesirable outcomes on ad-based revenue businesses. Encrypting the data at rest or in-transit is beneficial to security, but not privacy in the context of government requests. As long as the firms have cryptographic keys to access the encrypted data, their users' personal information is susceptible to government surveillance, thus making the technical affordance a net negative affordance for Facebook, Google, and Microsoft.

The capacity of the Top Firms as a corporate avatar was also directly correlated to each firm's surveillance capitalist business model. Technical affordance actions can be applied unilaterally, so any restrictions to the technical affordance are of the Top Firms' own making. Apple publicly touts its commitment to privacy, which may be a competitive differentiator and an example of a firm serving as a corporate avatar when business needs align with individual privacy. However, Apple's uses of technical affordance actions are the only examples across all affordances where the methods used to resist surveillance were at least partially out of line with the firm's business interests. Apple's use of encryption forced the firm into a public opposition with a federal intelligence agency making demands that legitimately threatened Apple's privacy advantage. In the face of litigation with the Department of Justice, Apple chose individual privacy even when a majority 47 percent of PEW survey respondents who were iPhone users believed that Apple should comply with FBI demands (Doherty and Jameson 2016, 2). Privacy is clearly core to Apple's business and platform when the firm is prepared to oppose both the U.S. government and its own users.

Apple has proactively invested in technical affordance actions well before the other Top Firms. Their use of end-to-end encryption in their communications services predated the Snowden disclosures. In addition, Apple has invested in new privacy techniques to maximize their surveillance capitalist needs while limiting the exposure and collection of user data. In comparison, Facebook, Google, and Microsoft minimally served as corporate avatars. These firms' targeted advertising models necessitate their access to user data, so any technical affordance actions implemented were either encryption that restricted only third party access to data or feature additions that were opt-in by default. Privacy conscious users were offered end-to-end encryption in communications services as a feature addition to compete with Apple and smaller platforms like Signal. However, the feature requires the user to opt-in, thus setting limitations on the use of the end-to-end encryption functionality and preventing an undesirable outcome on the larger pool of advertising targets. Facebook, Google, and Microsoft also

demonstrated a need for user data that fractured trust in Top Firms as capable corporate avatars. Targeted advertising is an arms race that escalates the methods firms will employ to build more and more detailed customer profiles. Targeted advertising models restrict the technical affordance thereby restricting the role ad-based surveillance capitalists can serve as corporate avatars if they wish to compete with the other ad driven firms in their ecosystem.

Evaluating the Top Firms as corporate avatars is difficult when considering network architecture. Distributed networks are more secure and private by design. On the other end of the spectrum, localization under more authoritarian governments may be presented as protective against foreign surveillance, but can often compromise the privacy rights of individuals at the hands of their own government. Google's use of a distributed network is beneficial to individual privacy, but is also necessitated by Google's needs at scale. Additionally, Google's support for the CLOUD Act seems to be driven by threats to its own architecture. As mentioned in the political affordance section, the CLOUD Act was not supported by human rights or privacy groups. Apple's willingness to abide by localization demands has been described as "Orwellian" by Amnesty International, but Apple believes that participation with China can influence privacy and human rights progress from the inside (Barron 2018; Strumpf 2017). As with the other affordances, labeling Top Firms as corporate avatars proves to be a futile exercise.

D. Market Affordances

When Calo studied U.S. citizen use of the market affordance, he suggested that citizens collectively place market pressure on firms to resist surveillance on their behalf. Calo referred to this as a nested affordance where the citizen leverages the market affordance to resist surveillance through the firm. This concept is essentially Cover's corporate avatar theory which Calo even cited in his paper. Although Calo was skeptical that the nested affordance would work in practice, the market affordance can be tested by observing how the business environment places market pressure on firms to prioritize privacy (Calo 2015, 13-15). Because all four Top Firms are publicly traded, if citizens left or boycotted a platform en masse, the cost of their loss may pressure shareholders to demand that firms resist surveillance. Unlike the prior three affordances, the market affordance will be measured primarily on anecdotal evidence that is tangentially related to a hypothetical scenario where U.S. government surveillance leads to privacy demands from citizens that warrant substantive action from the Top Firms. Considering

the current market dominance of the Top Firms, the Snowden disclosures had the opportunity to provide observable outcomes, but that scandal failed to provide market pressures strong enough to influence notable privacy changes. The first three affordances have demonstrated that firms are rarely sufficient corporate avatars, and are often influenced by their surveillance capitalist business models. In the absence of a real world example with observable outcomes, recent relevant controversies will be used throughout this section to provide context for a hypothetical situation.

The 2013 Snowden disclosures were a major controversy that named U.S.-based technology firms as active participants in U.S. government surveillance programs. As discussed throughout this thesis, the repercussions of the disclosures are still being felt five years later. Following the disclosures, thousands of protesters rallied in Washington, DC to protest U.S. government surveillance (Newell 2013). This citizen unrest was not a precursor to sustained distrust among citizens as consumers of technology. In late 2014, the PEW Research Center surveyed respondents about privacy strategies post-Snowden. A minority of those surveyed were concerned about the government monitoring them while using technology. Thirty-eight percent were concerned about the government monitoring their email; 39 percent were concerned about government monitoring of their searches; and 31 percent were concerned about government monitoring of their social media. Even fewer of those surveyed were willing to change the way they used technology platforms. Eighteen percent of respondents changed the way they used their email accounts; 17 percent of respondents changed the way they used search engines; and 15 percent of respondents changed the way they used social media (Rainie and Madden 2015, 4). Although the NSA documents implicated firms as arms of U.S. government surveillance, people's technology habits remained predominantly unchanged even if they were more concerned about surveillance. This is reflected in user engagement performance indicator metrics as well. After the disclosures, much of the financial risk to firms came from abroad through protectionist policies and increased regulations. Overall, the Top Firms' growth metrics and the value extracted from users were not negatively impacted. In 2013 Facebook recorded 1.19 billion monthly active users which was an 18 percent increase over 2012 (Protalinski 2013). In 2014 Facebook recorded 1.35 billion monthly active users which was a 14 percent increase over 2013 (Protalinski 2014). In 2013 Apple sold 150.2 million iPhones, a 20 percent increase over 2012 (Abbruzzese 2014). In 2014 Apple sold 169.2 million iPhones, up 13 percent over 2013 (Lowensohn 2013). The metric Average Revenue Per User (ARPU) reflects the monetization of users. Facebook's Q4 2013 to Q4 2014 ARPU grew 31 percent from \$2.14 to \$2.81 and Google's

Q1 2013 to Q1 2014 ARPU grew 7 percent from \$42 to \$45 (Garner 2015). Citizen distrust following the highest profile government surveillance scandal was not negatively reflected in user engagement. The emergence of the Snowden disclosures did not elicit feedback from consumers that would have potentially forced substantive change directed from shareholders to firms in response to diminished trust from consumers.

In 2018 Facebook announced the suspension of analytics firm Cambridge Analytica stating that the firm had improperly obtained information belonging to 87 million Facebook users (Prokop 2018). The scandal has invited discussion of potential regulation of the U.S.-based platform technology industry. After Facebook CEO Mark Zuckerberg testified before both chambers of Congress, two data protection laws were announced. First, Senators Richard Blumenthal and Ed Markey introduced the Customer Online Notification for Stopping Edge-provider Network Transgressions (CONSENT) Act. Markey framed the CONSENT Act as a U.S. response to the EU General Data Protection Regulation. The bill includes breach notification requirements, explicit opt-in consent requirements, and notifications if personal data is used. The FTC would handle enforcement (Brandom 2018). Second, Senators Amy Klobuchar and John Kennedy announced legislation that would allow users to opt-out of data tracking, require terms of service to be written in plain language, access already collected data, and have a privacy program (Deahl 2018). There is bipartisan support for data protection legislation reflective of a deterioration of trust with Facebook and technology platforms in general. However, there is skepticism that legislation will pass or that the final draft will be as protective as originally intended. Members of Congress expressed doubt that the current Republican-controlled Congress would be able to pass regulatory legislation with midterm elections at the end of the year (Timberg 2018). A former congressional staffer commented that even if the proposed laws made it to a vote, they may look very different once the Top Firms begin lobbying lawmakers. The Obama administration introduced the Consumer Data Privacy framework in 2012. Even after the Snowden disclosures, lobbyists for U.S.-based technology firms modified the bill so much that consumer privacy groups ultimately opposed the 2015 discussion draft (Bedoya 2018). Executives of the Top Firms have expressed openness to impending regulation, but they are already telegraphing their desire to frame it through caveats in their language. Apple CEO Tim Cook said “well-crafted” regulation was probably necessary (Welch 2018). During his testimonies, Facebook CEO Mark Zuckerberg said he would not oppose the “right” regulation and that he would work with Congress to “flesh it out” (Kelly 2018). It will be up to citizens to

prove to lawmakers that data protection legislation needs to be truly representative of consumer protection and is an issue they will vote on.

Loss of consumer trust has led to social movements to leave platforms. Facebook's Cambridge Analytica scandal has prompted a #deletefacebook campaign. It is too early to determine how impactful such a movement will be, so other movements could be instructive. In 2017, Uber's many controversies led to #deleteuber campaigns stemming from exploitation of protests, an internal culture of sexual harassment and assault, the CEO verbally abusing one of the firm's drivers, a tool used to evade regulators and law enforcement, and an executive who stole medical records of a rider who was a rape victim (Alba 2017a). Also, Uber suffered a data breach of 57 million driver and rider accounts that was hidden by paying off the hackers and making them sign non-disclosure agreements (Isaac, Benner, and Frenkel 2017). In January 2017, Uber received up to 500,000 account deletion requests in one week after the firm was accused of taking advantage of a New York City Taxi work stoppage related to protests of President Trump's Muslim ban (Isaac 2017). The weekend following the start of the #deleteuber campaign, Uber competitor Lyft's app was downloaded more than Uber for the first time in Lyft's history (Hawkins 2017). A consulting firm study showed 81 percent of respondents were aware of repeated Uber scandals with 27 percent, triple previous data, having negative perceptions of Uber (Siddiqui 2017). All these issues point to a consumer backlash for Uber's negative public image. However, even with multiple controversies and an anti-Uber movement, only 4 percent of respondents switched ride hail apps even though the respondents felt all ride hail apps were the same (Siddiqui 2017). Uber went on to record 4 billion rides during 2017 alone after having just recorded the milestone 5 billion all time rides in May 2017. In January 2018 Uber reported 75 million monthly active users with 15 million rides per day (Bhuiyan 2018). Lyft ended up benefitting from Uber's 2017 scandals to a degree, doubling rides over the previous year. However, even at that milestone, Lyft recorded 375.5 million rides in 2017 which is 9 percent of Uber's 2017 ride total (Carson 2018). For Uber, the social movement boycott amounted to minimal damage despite an entire year worth of negative media coverage.

So far, this section has focused on the costs of not prioritizing privacy, but perhaps there are benefits to being privacy focused. In 2016 Apple refused to cooperate with the FBI's request to access the iPhone of a San Bernardino shooter. The Department of Justice claimed that Apple's refusal to comply was motivated out of concern for Apple's business model and public image. CEO Tim Cook describes privacy as a "key value" for Apple (Benner and Mozur 2016). Former

CEO and co-founder Steve Jobs had been vocal about privacy before his death in 2011 having said:

Privacy means people know what they're signing up for in plain English and repeatedly. That's what it means. I'm an optimist. I believe people are smart and some people want to share more data than other people do. Ask them. Ask them every time. Make them tell you to stop asking them if they get tired of you asking them. Let them know precisely what you're going to do with their data (Farnsworth 2018).

Cook has confronted shareholders when questioned about Apple acting on their values. At a 2014 shareholder meeting, a member of the National Center for Public Policy Research (NCPPI) challenged Cook after a NCPPI resolution was voted down, suggesting that investment in environmental measures should be driven by return on investment (ROI) only. Cook replied saying that shareholders that wanted Cook to make decisions purely for ROI reasons should get out of their stock (Shankleman 2014). During the public debate with the FBI, Cook addressed shareholders saying, "We've been in the news lately, and some of you may have some questions on that. We do these because these are the right things to do. Being hard doesn't scare us" (Lien and Dave 2016). Apple's decision to defy the FBI may not be the hard stance that Cook perceived. Opinion polls published within a week of each other in February 2016 showed majority opinions for and against Apple. One of the polls returned that 20 percent of respondents did not know what to think (Carmen 2016). Throughout 2016, Apple's share prices did not reflect their strong privacy stance. At one point in the first half of 2016, Apple's shares were 30 percent below the high from the year before. Market analysts linked this decline to underperforming iPhone sales at the end of 2015 (La Monica 2016). The shares recovered in the second half of 2016, reaching its highest level since December 2015. The boost to share prices was credited to rival Samsung Galaxy Note 7 phones having battery explosion issues (Balakrishnan 2016). Apple's commitment to privacy is a core part of their brand. The dispute with the FBI was a highly publicized privacy stance that denied the U.S. government a tool that could allegedly threaten the privacy of every iPhone user. However, as much public debate and coverage as this issue has garnered, the public appears to be highly conflicted over Apple's position. Because Apple's share value appears to be far more reliant on iPhone sales than controversy, consumers would have to drastically modify their purchase behaviors in favor of, or opposed to, Apple's privacy values.

From the examples above, determining if consumers could apply market pressure to force firms to resist government surveillance has proven to be a difficult task. The complex adaptive nature of the business environment makes it difficult to even find trends between scandals. Apple's privacy stance did not appear to have an impact on the short term, reflected either through public opinion or in share prices. The counterfactual of this dispute may have been more illustrative of how privacy could impact share prices forcing investors to pressure Apple. What if Apple had eventually ceded to the FBI or lost the litigation and were forced to provide an unlocking tool? After all the rhetoric from Apple claiming that such a tool would compromise every iPhone, would iPhone sale projections be low enough to dramatically drop the value of Apple's shares? This scenario is even more compelling knowing that Samsung's battery explosion issues boosted Apple shares in anticipation for the 2016 holidays. What if consumers were forced to choose between an iPhone that had all of its privacy benefits stripped or a Samsung phone that could potentially explode? That scenario would demonstrate just how much consumers value Apple's culture of privacy.

It is too early in Facebook's current Cambridge Analytica scandal to glean much insight, but the parallels to Uber's many scandals may be informative. Like Facebook, Uber is a multinational U.S.-based technology platform firm that has built its business on disruption and operated with little to no regulation. Both firms demonstrated poor data governance and failed to publicly report the loss of data belonging to tens of millions of users. Both firms have a social movement boycott hashtag. Both have highly visible founder CEOs. However, that is where the similarities end. Although Uber does not have the size or stature of Facebook, the scandals involved were more salacious and were constant throughout an entire year. Uber ended up losing several executives who were active participants in the firm's scandals. Despite all the negative headlines, purported loss of consumer trust, chaotic internal leadership and governance, and notable competitors, Uber recorded milestone numbers for 2017. For a brief period, they lost a statistically small number of users who may have defected to their rival, but long term consumer unrest was not sustained. The inability to negatively impact firm revenue removes even the potential for shareholders to place pressure on firms to resist surveillance.

Facebook may be different. CEO Mark Zuckerberg was summoned to testify before Congress. None of Uber's executives were brought to Capitol Hill. Depending on how it is drafted, impending regulation is a legitimate risk to the Top Firms. However, if regulation is the only response to the Facebook scandal, then U.S. citizens benefited from the political affordance

and not the market affordance. It is unclear if the market affordance will place significant pressure on Facebook to change. Facebook's dominance likely contributes to the scrutiny of this scandal, but that dominance was established and fortified by network effects built on surveilling users. Facebook has potentially years of communications with large networks of family and friends. Facebook's network effects are designed to make the decision to leave the platform come at tremendous personal cost. There are also few alternatives. Potential social media and communications competitors Instagram and Whatsapp were acquired by Facebook. The absence of direct competition makes it more difficult to #deletefacebook than it was to #deleteuber, and not many users deleted Uber.

In time, investor filings may reveal that Facebook lost a significant number of active users, and perhaps the share prices will reflect those losses. Facebook's shares have declined during the scandal, particularly when the FTC announced an investigation into Facebook to determine if the firm violated the consent decree from 2011 (Ortutay 2018). Some investors are suing Facebook to make up for these losses, claiming that the firm "made materially false and misleading statements" (Larson 2018). Fortunately for Facebook, the outrage may be dampened. After Zuckerberg's testimony before Congress, Facebook's share price improved 5 percent (Molla 2018). The price is still down 11 percent compared to before the scandal, but as time passes and Facebook drifts out of the news cycle, perhaps the share price will continue to improve. Some analysts are saying that investors can take advantage of irrational pessimism that is driving down Facebook share prices to purchase stock, which will rebound in a few news cycles, at a discount (Kam 2018). If Facebook does suffer significant user losses and no new data protection laws are enacted in the U.S., it would be interesting to see what steps Facebook would take on their own to restore user trust.

If the Top Firms were implicated in a Snowden level scandal involving U.S.-based surveillance, the business environment would produce a great deal of emergence and feedback. With the passage of the CLOUD Act and the spread of data protection laws around the world, U.S. government surveillance that requested data from U.S.-based firms belonging to a foreign national would likely produce legal and political conflicts that would preclude the necessity for consumers in that country to pressure shareholders. If the surveillance targets were in the EU but outside of the United Kingdom, the firm may be subject to a fine of 4 percent of global revenue and the business ecosystem would suffer from the de-authorization of transatlantic data transfer mechanisms required to operate businesses in the EU. If the surveillance targets were

in China, the penalties for the firm may be a ban from operating in the country and/or fines. Given the size of these two markets, both of these scenarios would achieve the goal of pressuring shareholders but to a greater extent that includes fines and a possible loss of entire markets, not just a critical mass of consumers boycotting as part of a movement. The movement would not be necessary. If the surveillance targets were U.S. citizens, there might need to be a critical mass of boycotting users. It is unlikely that the U.S. government would punish U.S.-based firms for complying with surveillance requests from their own government. If more than one firm is implicated, would that shift the public outrage to the government? If only one firm is implicated, and hypothetically another firm resisted surveillance, the complicit firm would likely be singled out under tremendous scrutiny. The nature of the targets would likely impact the boycott. If the surveillance was of a marginalized group or otherwise partisan in nature, the degree of outrage may be accelerated. However, as seen in the Apple FBI dispute, if the targets were proven to be nefarious actors, the public may have diverse reactions making it more difficult to build a critical mass.

If there were enough losses to pressure shareholders into forcing firms to resist surveillance, the firms could use the legal or political affordances, but those affordances are prolonged processes. The legal affordance may require challenges for every request and the results could vary among the lower courts. The political affordance may have support assuming that the government is also facing backlash, but because legislating considers all stakeholders, the final bill may take time to be enacted or may not be sufficient to prevent all types of surveillance. The most effective affordance would be the technical affordance. The technical affordance does not depend on other parties for implementation and the unilateral nature could be beneficial to convince users of a newfound commitment to resist surveillance. However, in the absence of the other affordances, the technical affordance would require encryption that prevented even the firm from accessing the data. For firms like Google or Facebook, the loss of users would become a willing tradeoff to protect the revenue stream that sustains the firm.

Chapter IV. Results

The following tables summarize the findings of this thesis covering the broader application of Calo’s modification of Affordance Theory to evaluate the utility of the four affordances - legal, political, technical, market - when resisting U.S. government surveillance.

Tables 17 - 18 summarize the outcomes of Affordance Theory applied to the resistance of surveillance. Table 17 compares the ability of U.S. citizens to the ability of U.S.-based technology platform firms to resist surveillance. The U.S. Citizens column reflects the conclusions from Calo’s original use of Affordance Theory. Calo believed that firms would be better equipped to resist surveillance. The U.S.-based Firms column reflects the findings of this thesis. Table 18 summarizes the outcomes achieved by firm and affordance.

Tables 19 - 20 summarize the capacity of each Top Firm to serve as a corporate avatar. Each table is broken down into the legal, political, technical, and market affordances. The market affordance row is generalized to the firm’s business model.

Table 17: Outcomes of Affordance Theory - U.S. Citizens v. U.S.-based Firms

Affordance	U.S. Citizens	U.S.-based Firms
Legal	Limited by the Third Party Doctrine and Non-Disclosure Orders	Challenges to Non-Disclosure Orders led to desirable outcomes. Challenges to data requests had high potential for false affordance and undesirable outcomes. Desirable outcomes
Political	Citizens are diffuse and less focused than special interest groups	ECPA reform led to desirable outcome. FISA reform unclear. Less risk than legal affordance.
Technical	High barrier to entry, lack of expertise	In-Transit Encryption led to desirable outcomes. Highly dependent on surveillance capitalist business model.
Market	Reliant on firm willingness to serve as corporate avatars	Low probability that consumer distrust leads to undesirable shareholder value and pressure from investors. Limited by business model.

The Top Firms were more resourced and influential than U.S. citizens, but the firms were operating in a more complex environment. Under the legal affordance, U.S. citizens are highly dependent on firms because of the third party doctrine and the use of non-disclosure orders. The Top Firms' legal challenges to the use of indefinite non-disclosure orders allowed U.S. citizens to at least be notified that their information had been requested by the U.S. government, regardless of whether the request led to a charge. The citizen may not be able to claim a Fourth Amendment violation because of the third party doctrine. Firms cannot do so on the citizen's behalf because they do not have third party standing. Both U.S. citizens and firms need to use the political affordance to resolve scenarios where legal restrictions limit the firm's ability to act on behalf of the user.

The political affordance illustrates the disparity between U.S. citizens and the Top Firms. There is not only an information asymmetry between firms and citizens, but also between firms and lawmakers. Firms have invested tens of millions in expenditure to recruit former government employees to lobby Capitol Hill. This poaching drains expertise from the government and transfers it to the firm, creating an information asymmetry that U.S. citizens typically do not have. Firms can also sustain legislative lobbying for years and through several iterations of bills where U.S. citizens may not.

Clearly, the Top Firms are far better equipped to leverage the technical affordance. In some instances, the effort may be required from both citizens and firms. Some firms added privacy focused features, but these features either required opt-in selection or action on the part of the user to achieve the desirable outcome. The addition of new features may reduce the barrier to entry citizens experience when trying to leverage the technical affordance on their own. If the firms are offering the tools, learning to use them may be more accessible to citizens.

The ability of consumers to put market pressure on firms to incentivize surveillance resistance has been aided by technology and has not produced results in past privacy focused scenarios. Threatening a firm's business model by deleting the app or otherwise opting out could force investors to pressure firms on the citizen's behalf. To date, there have been no examples of this occurring.

Table 18: Outcomes of Affordance Theory - Affordance Categorizations by Firm

Firm	Legal Affordance	Political Affordance	Technical Affordance	Market Affordance
Apple	N/A - Amicus Only	ECPA - Desirable, FISA - Undesirable	Upstream - Desirable. PRISM - Desirable	TBD
Facebook	ND - Desirable DR - Undesirable	ECPA - Desirable, FISA - Undesirable	Upstream - Desirable. PRISM - Undesirable	TBD
Google	DR - Undesirable	ECPA - Desirable, FISA - Negative	Upstream - Desirable. PRISM - Undesirable Network a Liability	TBD
Microsoft	ND - Desirable DR - TBD	ECPA - Desirable, FISA - Undesirable	Upstream - Desirable. PRISM - Undesirable	TBD

“ND” = *Non-Disclosure*, “DR” = *Data Request*, “N/A” = “*Not Applicable*”, “TBD” = “*To Be Determined*”

Firms achieved desirable outcomes resisting surveillance to limit U.S. government access to non-U.S. citizens. A combination of the legal affordances and the political affordances led to ECPA reform that limits the reach of the U.S. government outside of the United States and helps prevent conflict of law situations that produce undesirable outcomes.

ECPA reform demonstrated the complexity of the business environment that firms occupy. Years of lobbying and multiple iterations of ECPA reform bills progressed to varying extents in Congress, all while Microsoft continued challenging a request for data in Ireland that was appealed all the way to the U.S. Supreme Court. No matter the ruling, there would have been potential for undesirable outcomes across the business ecosystem because of the rigid nature of litigation. These undesirable outcomes were averted by the inclusion of the CLOUD Act in an omnibus spending bill that rendered the U.S. Supreme Court case moot. If the CLOUD Act had to go through normal procedure, would it have passed, and would it have done so without significant revisions? Firms and the U.S. government alike celebrated the passage of the CLOUD Act, but it is highly dependent on bilateral agreements between the executive branch and non-U.S. governments. At this point, there is only an agreement with the United Kingdom. The Top Firms should be lobbying the executive branch to push more agreements as data protection laws around the world are implemented.

The technical affordance most clearly demonstrated the impact of surveillance capitalist business models on the actions firms choose to resist surveillance. Google, Facebook, and, to an

extent, Microsoft's business models limit them when resisting surveillance. These firms rely on access to personal data as fuel for ad targeting revenue streams. Because Apple operates a completely different business model and is vertically integrated, Apple can find a balance between access to user data and the use of privacy-by-design functions like encryption and differential privacy. Apple's commitment to privacy and willingness to resist surveillance escalated a dispute with the FBI. Google, Facebook, and Microsoft may be limited in their ability to innovate on privacy, but if Apple pushes too far they risk another escalation either with the U.S. government or even a less human rights oriented country like China. Apple has been deferential to China, but if China demanded the same tool that the FBI wanted, either choice to comply or not would put Apple in a very precarious position. In a complex adaptive environment, Apple may not be able to predict, but it needs to prepare for a situation where strong resistance to surveillance leads to backdoor or encryption key demands enacted into law. Or Apple needs to prepare for the opposite scenario where an inaccessible iPhone could reasonably have prevented a major incident like a terror attack or mass shooting. Apple's willingness to comply with localization demands is in contrast to Google whose distributed network necessitates surveillance resistance to limit protectionism. Both firms are making business driven decisions based on access to international markets or scalable efficiency with privacy as a byproduct.

The market affordance served as a nested affordance for the other three affordances. There have not been examples to date that suggest that consumer distrust or dissatisfaction over privacy violations could lead to a critical mass of lost users to pressure firms into resisting U.S. government surveillance at the expense of their business model. This is not to say that public pressure has no impact on firms. Public outrage related to privacy issues like a breach or sale of data can lead to feature changes, public apologies, resignations, and policy changes. Resisting U.S. government surveillance adds another variable to the business environment. U.S. government surveillance is authorized by law and sometimes includes court orders requiring a firm's compliance. Resisting U.S. government surveillance to avoid loss of users and loss of shareholder value adds its own costs and firms risk undesirable outcomes that may require balancing with the threat of lost consumers. Firms whose business model is fueled by ad based surveillance capitalism are at greater risk because the same collection and exploitation of data to drive revenue is what makes the firm an attractive source of surveillance. Implementing more privacy-by-design techniques to protect users could inhibit the revenue fueling access to

personal data. These firms may be forced to play defensively through lobbying to limit overreaching or clandestine surveillance.

Table 19: Apple as a Corporate Avatar

Affordance	Capacity as a Corporate Avatar
Legal	Served amicus for increased transparency.
Political	Supported the CLOUD Act, not supported by privacy groups FISA reform efforts led to undesirable outcome.
Technical	Walled garden business model with control over stack allows for privacy focused techniques. Some end-to-end requires two factor enabled. Localization compliance risks privacy even with best intentions.
Market	Walled garden business model with control over stack allows for privacy focused techniques. Experience standing alone resisting surveillance against FBI.

Table 20: Facebook as a Corporate Avatar

Affordance	Capacity as a Corporate Avatar
Legal	Litigated on behalf of individual First and Fourth Amendment rights.
Political	Supported the CLOUD Act, not supported by privacy groups. FISA reform efforts led to undesirable outcome.
Technical	Targeted advertising business model limits to only in-transit encryption. End-to-end messaging requires opt-in. Demonstrated deceptive tactics to collect user data.
Market	Targeted advertising business model limits ability to resist surveillance.

Table 21: Google as a Corporate Avatar

Affordance	Capacity as a Corporate Avatar
Legal	Focus on cross-border data access and ECPA reform.
Political	Supported the CLOUD Act, not supported by privacy groups. FISA reform efforts led to undesirable outcome.
Technical	Targeted advertising business model limits to only in-transit encryption. Merged large datasets that de-anonymized the personal data. Distributed network architecture benefits individual privacy.
Market	Targeted advertising business model limits ability to resist surveillance.

Table 22: Microsoft as a Corporate Avatar

Affordance	Capacity as a Corporate Avatar
Legal	Litigated on behalf of individual Fourth Amendment rights. Non-disclosure order challenge resulted in desirable outcome. Focus on cross-border data access otherwise.
Political	Supported the CLOUD Act, not supported by privacy groups. FISA reform efforts led to undesirable outcome.
Technical	Combination walled garden, subscription, targeted advertising business model limited to in-transit encryption. End-to-end Skype limited feature that requires opt-in. Aggressive tactics to collect user data.
Market	Targeted advertising portion of business model limits ability to resist surveillance.

Apple was the most capable corporate avatar of all the Top Firms because of the walled garden business model. Apple was less engaged in the legal affordance, serving only as amicus on the multi-firm litigation for more transparent reporting after the Snowden disclosures. There were no publicly available cases where Apple challenged data requests authorized by ECPA or FISA. Apple was also less engaged using the political affordance. The technical affordance and the market affordance are where Apple stood apart from the other firms. Apple’s walled garden business model, privacy focused techniques, and marketing privacy as a core value is not coincidental. Apple’s vertical integration allows for privacy techniques that limit collection, retention, and storage of user data in a minimal and anonymized fashion. Because Apple can benefit from surveillance capitalism in a controlled fashion that limits collection based on only Apple’s needs, privacy can be marketed as a core value and used as a competitive differentiator. Apple *could* monetize their users’ data, but it appears Apple does not have to nor wants to.

Apple's business model would be beneficial should they ever be implicated in a U.S. government surveillance scandal again. If a mass collection of users were going to leave Apple's walled garden, Apple is not only equipped to technically resist surveillance, but they have also proven that they will stand alone against the FBI. The only scrutiny of Apple as a corporate avatar comes from their cooperation with non-U.S. government that have a track record of human rights and privacy violations. Apple seems to be much more willing to serve as a corporate avatar against the U.S. government as opposed to other firms.

Microsoft and Facebook are less capable as corporate avatars than Apple, but both were more capable than Google. Both firms used the legal affordance to litigate for constitutional rights of users. Facebook challenged warrants that they considered overbroad and potentially chilling to political speech and the right of assembly. Microsoft challenged the indefinite use of non-disclosure orders which allows individuals to be notified about being surveilled. Both firms attempted to protect the Fourth Amendment rights of their users but were denied third party standing. Both firms were also part of the multi-firm group that challenged for more transparency allowances. As with Apple, the technical affordance demonstrated how each firm's business model determines their capacity as corporate avatars. Microsoft's multi-faceted business model limited their ability to implement privacy-by-design techniques. The end-to-end encryption available in Skype was available years after the Snowden disclosures and only as a feature requiring user opt-in. Facebook's targeted advertising business model significantly limits their ability to implement privacy-by-design techniques and incentivizes indiscriminate mass data collection. Both firms used deceptive or aggressive tactics to collect data from users. The business models of both firms compromise their ability to adapt if a mass collection of users was going to leave their platforms after either firm was implicated in another U.S. government surveillance scandal. Facebook's current scandal with Cambridge Analytica could reveal more about Facebook's capability to adapt.

Google was the least capable corporate avatar. Google's use of the legal affordance was solely focused on protection of cross-border data transfers and ECPA reform to avoid conflict of laws scenarios. Like Facebook, Google's targeted advertising business model significantly limits their ability to implement privacy-by-design techniques and incentivizes indiscriminate mass data collection. Google also merged two large datasets after having stated that they would keep them separate, effectively de-anonymizing one of the datasets. Google's business model compromises their ability to adapt if a mass collection of users threatened to leave the platform

should Google be implicated in another U.S. government surveillance scandal. The one benefit to their willingness as a corporate avatar is Google's network architecture. Protecting against localization demands of non-U.S. governments requires resistance to U.S. government surveillance. The distributed network also has built-in privacy benefits.

The findings demonstrate how limited the current Top Firms are when resisting U.S. government surveillance. Operating in an unregulated industry for decades has allowed for tremendous growth that is built on business models that are largely antithetical to individual privacy. The importance of building network effects to establish and reinforce dominance places exponential value on personal data assets, thus limiting the ability of firms to adapt and better resist surveillance.

For firms whose revenue is generated by targeted advertising, transitioning to a subscription model where their revenue comes directly from the user offers more opportunities for resistance. Personal data assets would still be at a premium because network effects would be just as important to establish consistent subscription revenue, but because firms would only need to exploit personal data to improve their own platform they would have much more flexibility to implement privacy-by-design techniques and data governance. Focusing on their own platform may allow firms to iterate on their services in the same way that Apple's business model has allowed them to use differential privacy to anonymize data while retaining the ability to extract valuable insights, though they would be more limited than current insights. If firms are not selling an advertising platform used by a diverse client base to target individuals, there is less incentive for firms to indiscriminately collect data that is not directly relevant to product iterations. However, a transition to a subscription based model would still leave firms reliant on surveillance capitalism so even though gains would improve their overall privacy posture the impact on surveillance resistance may be minimal.

A transition to a subscription model as a way to implement more privacy-by-design features may not be feasible for firms that generate revenue primarily through services compared to Apple's vertically integrated business driven by hardware sales. The competitive advantage of firms like Google and Facebook is that the same data collection that fuels targeted advertising also differentiates their services from upstarts, establishing strong network effects. Unless data can be anonymized while still being tailored to an individual, the firms would sacrifice their competitive advantage while simultaneously limiting their user base to those who

are willing to pay subscription fees. If a new service emerged with a targeted advertising model, users may see more benefit to a more tailored service that is also free to use. This would essentially be the opposite of the market affordance findings. The current network effects of firms prevent users from impacting shareholder value enough to influence surveillance resistance at times of crisis. If firms proactively dismantle their network effects, they could be adversely impacting shareholder value to protect the privacy of users who have not demonstrated a willingness to protect their own privacy beyond voicing dissatisfaction. Google and Facebook have spent years establishing dominance in digital advertising that has led to their market capitalization. It would not make sense, from a business perspective, to dismantle their businesses to marginally resist surveillance.

If firms are to adapt to the changing privacy landscape and make privacy a dominant priority when resisting surveillance, they would have to diminish the reliance on any surveillance capitalist model. Firms could establish alternate revenue streams that operate independently and are not predicated on exploitation of personal data assets. Microsoft and Google are potentially setting themselves up for success in a privacy conscious world by investing in cloud infrastructure. Amazon has dominated the market by leveraging the internal infrastructure competencies necessitated by their business to offer those same services to external organizations and developers (Miller 2016). Google and Microsoft have followed Amazon's lead. At 10 percent, Microsoft has only a quarter of the public cloud market share as Amazon, but Q4 2017 reported a 97 percent increase year over year. Google is third in market share at close to 4 percent but had a Q4 2017 growth rate of 85 percent (Coles n.d.). Google has invested \$30 billion in cloud infrastructure over the past three years (Miller 2018). While it may take time in an increasingly competitive market, Google and Microsoft's diversification is establishing metaphorical insurance policies while surveillance capitalism invites increasing scrutiny. Diminishing the reliance on monetizing personal data assets may provide firms with more flexibility to resist U.S. government surveillance through the implementation of more privacy-by-design features that are enabled by default, thus significantly decreasing the collection and retention of personal data assets. Critically, if there were ever another U.S. government surveillance scandal or standoff, firms who transitioned their primary revenue source away from surveillance capitalism could respond to public scrutiny or stand up for public privacy by altering their privacy techniques in ways that would have previously threatened their revenue producing data collection.

To avoid risks to surveillance capitalism, firms could turn the public concern over U.S. government surveillance on the government itself. In the same way that Apple frames their relationship with China, firms could simply state that they are merely abiding by U.S. law while placing emphasis on digital sovereignty. Passage of the CLOUD Act has already provided some protection for firms against conflicts of law. When addressing domestic concerns over surveillance, public outcries could be redirected at the government in the same way that Apple framed the encryption debate as the FBI jeopardizing the privacy of everyone using an iPhone.

Firms that offer free services funded by targeted advertising could frame any surveillance resistance changes as a tradeoff that would require a subscription model to continue operating at the level users expect. For example, if Google adopted this approach, it would be a choice between the U.S. government legislatively constraining surveillance authorities and Google needing to transition to a subscription model where users would have to pay for what had been a free service. This method may absolve firms of an untenable role as a corporate avatar.

As surveillance capitalism is called into question by individuals and governments worldwide, new firms face difficult choices in markets that are currently dominated by surveillance capitalist firms. The emergence of privacy focused and punitive data protection regulations worldwide have increased the operating costs of compliance and the financial risk of non-compliance. If a new firm operates outside of the United States, any U.S. government surveillance requests may threaten critical cross-border data transfers or result in punitive fines that firms cannot absorb during growth stages. Resisting U.S. government requests to avoid regulatory risks is not a feasible alternative. New firms likely lack the resources for prolonged litigation or lobbying methods of the legal and political affordances. Not to mention that this thesis demonstrated that those affordances were by no means guaranteed, even with the resources and influence of a Top Firm like Apple or Google.

Technical affordances would be more accessible to new firms, but would come with their own limitations and risks. The security and efficiency benefits of a distributed network architecture may prove to be problematic if the firm was ever required to comply with localization demands, and refusal to comply could result in fines or litigation that new firms may not be able to facilitate. New firms could implement default end-to-end encryption, making compliance to U.S. government surveillance requests nearly impossible to accommodate. However, unilateral technical affordance methods can potentially escalate the demands of the

government, forcing firms into a standoff akin to Apple and the FBI. A standoff may necessitate defense in court where, again, new firms likely will not have the resources for prolonged litigation. If a new firm were to defend their privacy stance in court, failed litigation would not only completely upend the privacy protections the firms implemented to resist surveillance, but the precedent set in a loss could also threaten the entire business ecosystem. Even if a new firm avoided an escalated standoff with the U.S. government, operating as a privacy focused service where the firm has no access to decryption keys may attract the bad actors that U.S. government surveillance is targeting. A new firm may not be able to withstand public branding as a safe harbor for bad actors the same way the FBI attempted to frame the Apple debate over the San Bernardino shooting.

The only guaranteed method to resist surveillance would be to limit the collection and retention of personal data assets as much a new firm's business allows. If the data is not available to either the firm or the government there would be no opportunity for non-compliance with data protection laws or surveillance requests, but that option may not be realistic. Opting out of advertising based revenue models may inhibit user acquisition and diminish the ability of firms to establish their own network effects. Without strong network effects, new firms may not be able to retain users during potential scandals. The disadvantaged position of new firms to resist U.S. government surveillance, no matter the chosen method, further emphasizes the position of the Top Firms who established their dominance in a previously unregulated industry. The only choice new firms have may be to prioritize growth at all costs to build their own network effects. If they aren't capable of doing that, they won't be able to compete with the Top Firms regardless of U.S. government surveillance.

Chapter V. Discussion

A. Utility of Affordance Theory

Calo's initial application of Affordance Theory was to measure the ability of U.S. citizens to resist government surveillance. His findings demonstrated that individuals were systematically disadvantaged and that the technology firms would be better equipped to resist surveillance. This thesis applied Calo's Affordance Theory to U.S.-based technology firms to test if firms were actually better equipped, but with some modifications. Calo's research used the conceptual findings of other research to support his conclusions. This thesis applied Affordance Theory to the actual surveillance resistance that firms engaged in following the Snowden disclosures. Calo also treated U.S. citizens as a singular being with the same motivations and limitations. This thesis focused on four individual firms to make distinctions between firms and to observe how those differences affected the ability of each firm to resist surveillance. The four firms chosen were globally market dominant firms because the assumption made by Calo is that the influence and resources of firms would better equip them to resist surveillance.

While this thesis focused on firms, the findings have impacts on all stakeholders within the business environment. Generally, U.S.-based platform technology firms have benefitted from little to no regulation and the ability to build dominant businesses by exploiting personal data assets. But what built these companies is proving to be their greatest threat. The mass data collection of firms has made them targets for surveillance and regulation. Both government surveillance and surveillance capitalism have forced countries around the world to establish borders in the previously open internet that facilitated these firms' growth. The firms with business models reliant on targeted advertising are at even greater risk. Targeted advertising business models incentivize the exact opposite behaviors required by data protection laws around the world. Are these firms prepared to adjust if data protection diminished the viability of an ad model? Are users willing to pay for these services using a subscription model, and can the firms sustain the revenue per user and growth rates as the current ad model provides? Firms need to self-regulate and make the ad model worthwhile for users to exchange data. More user control over the what data is collected and what ads are displayed may make the exchange more palatable for users. If users help cultivate the ads they are shown, firms may not have to collect

such endless amounts of data to obtain the same insights as the actual user's contributions. Many of these concerns and recommendations apply to shareholders.

Users should be careful as well. Many of the services the Top Firms provide are free of charge on the ad based model. If privacy protections begin to diminish the value of ad based models, users may get a lesser version of what they had and may have to adjust to a subscription model. This is not meant to discourage calls for privacy. Users should understand that there will be tradeoffs.

With the exception of the CLOUD Act, the U.S. government appears committed to surveillance with little long term outlook for the future of data protection. This thesis has covered all the methods that firms engage in to limit the fallout of U.S. government surveillance. It is understood that the data collected by firms is an invaluable surveillance resource. However, if non-U.S. governments respond with stronger data protection laws or protectionist policies, it begins to diminish the value of the privileged access the U.S. government obtains from U.S.-based firms.

Dividing the methods of surveillance into four separate affordances allowed for initial clarity and review, but when applied to the practical methods used by firms, it became clear that the affordances were dependent on one another, thus making it more difficult to rate the efficacy of each affordance separately. Also, the outcomes of each method opened up the possibility for reverberations that could reframe whether an outcome was desirable or undesirable. An example of this is the enactment of the CLOUD Act. The CLOUD Act rendered the Microsoft Supreme Court litigation moot, making it difficult to determine if litigation was successful. The final bill was built on years of lobbying previous bills that were only partially incorporated. Firms hailed the bill as privacy protective but privacy advocates strongly disagreed. The bill is highly dependent on the executive branch establishing bilateral agreements that are yet to be initiated. How should Microsoft's use of the legal affordance be rated? Should the CLOUD Act's passage be considered when making that determination? What if the executive branch does not establish bilateral agreements with any new governments? All of this uncertainty and interdependence made it difficult to rate affordances as simply positive or negative.

Calo's use of Affordance Theory is not a preferred tool for measuring a firm's ability to resist surveillance. Bucketing and rating methods of resistance based on the existing affordance types

and the application of a binary rating is too restrictive. A better methodology would be to map emergence feedback within complex adaptive systems, accounting for all relevant stakeholders. It must include reverberations throughout nested affordances resulting from the initial action of individual agents. In a more comprehensive system, Microsoft's challenge of the Ireland warrant through litigation would be tracked, not only as the challenge progressed to higher courts, but also to lobbying and congressional hearings that called for legislative solutions to prevent undesirable legal outcomes that could not consider multiple stakeholders. Alternatives to Affordance Theory must be able to account for changes over time and the impact of outcomes across several resistance methods.

B. Firms as Corporate Avatars

The results of this thesis were also intended to measure the ability of firms to act as corporate avatars. Like Calo, Cover's perception was that citizens needed firms to protect their privacy because of systematic limitations applied to them individually as citizens, but Cover was skeptical that firms would serve effectively in this capacity. Cover believed that firms would put the needs of the business ahead of the privacy needs of individuals. So, while using Affordance Theory to measure the ability of firms to resist surveillance, this thesis also measured firms as corporate avatars when resisting surveillance. Often, the ability of a firm to resist surveillance was heavily influenced by the degree to which the firm was motivated or limited by business needs. The motivation to prevent protectionism and localization that threatened cross-border data flows may have motivated firms to resist surveillance of data stored outside of the United States. This would be an example of business needs making firms more effective at resisting surveillance. Another example is the use of end-to-end encryption by firms. This privacy technique would make firms very effective at resisting surveillance, but implementation negatively impacts the ability of firms to exploit personal data for surveillance capitalism. This would be an example of business needs limiting the ability of firms to resist surveillance.

The use of corporate avatar theory had been applied to test the ability and willingness of firms to serve as protectors of individual privacy, but rating firms as corporate avatars was more difficult than expected. At times, the motivations of firms can be unclear since there aren't explicit statements by firms that explain motivations. In those instances, rating a firm based on levels of self-interest becomes highly speculative. Other complications arose when firms were seemingly motivated by business needs, but the outcome was also desirable for individual

citizens. How should a firm be measured as a corporate avatar when the ability to resist surveillance is a byproduct of the firm protecting its own interests? Should a firm's capacity as a corporate avatar be determined by the outcome of their actions or the motivation for resisting surveillance? Does the outcome determine if a firm is a corporate avatar or does the motivation? A better method for measuring firms as corporate avatars would be a spectrum or scale rather than a binary choice between corporate avatar and not corporate avatar. Ideally a new mechanism could weigh outcome and motivation for an advanced measurement of firms as corporate avatars.

C. Contributions to Remaining Existing Literature

Ryan Calo's application of Affordance Theory and Avidan Cover's concept of the corporate avatar were both integral aspects of the methodology of this thesis. However, this thesis couples and augments other existing literature covering technology firm involvement with U.S. government surveillance. Priya Kumar asserted that inclusion of the firms named in the Snowden disclosures was critical to ongoing public debate over U.S. government surveillance (Kumar 2017, 69). The naming of Apple, Facebook, Google, and Microsoft as complicit participants in the disclosures contributed to them being the Top Firms in this thesis. Kumar analyzed the changes within firms' privacy policies to illustrate the continued growth of surveillance capitalism while firms were actively involved in PRISM surveillance. Her analysis focused on a period covering the firms' participation in PRISM up to the Snowden disclosures in 2013, and ended with a call to action to further scrutinize the involvement of PRISM associated firms (Kumar 2017). Although the Top Firms have resisted U.S. government surveillance since the disclosures, this thesis found that resistance has been least impactful as it pertains to PRISM. The political affordance failed to reign in PRISM surveillance. The reauthorization of FISA Section 702, which is the authorizing legislation for PRISM, expanded the capabilities of National Security Agency (NSA) surveillance and did not limit access to the collected data by other agencies. The value of surveillance capitalism has not waned following the period covered by Kumar's analysis. The Top Firms have exhibited more aggressive data collection behaviors through deceptive practices seen in the technical affordance, including the merging of large datasets that were previously said to be kept separate and the promotion of privacy focused software that monitors and collects user activity. The methods of resistance executed via the technical affordance were highly influenced by surveillance capitalism. The Top Firms implemented in-transit encryption that limited the value of the NSA's UPSTREAM surveillance

program. However, use of end-to-end encryption, which would have limited the value of PRISM, was used sparingly. By continuing the inclusion of the Top Firms in discussions of U.S. government surveillance, this thesis augments Kumar's findings only to determine that the actions of the Top Firms have had little impact on their continued involvement in PRISM surveillance, years after being named in the Snowden disclosures.

Just as this thesis progressed Kumar's emphasis on the importance of technology firms in surveillance conversations, so did Alan Z. Rozenshtein's research on the ability of technology firms to resist surveillance as "surveillance intermediaries" (Rozenshtein 2018, 107). On the surface, his research and this thesis have commonalities. His analysis of litigiousness, technical unilateralism, and policy mobilization are comparable to this thesis' analysis of legal, technical, and political affordances (122-149). The divergence with Rozenshtein's research is in the objectives of the underlying analysis. Rozenshtein explored the role of surveillance intermediaries in the surveillance environment whereas this thesis explored the role of the Top Firms in the business environment. Rozenshtein used his analysis to discuss two conceptual and ideological conversations. First was the concept of the "surveillance separation of powers" demonstrating how the resistance of surveillance intermediaries forced intragovernmental checks on executive branch surveillance operations (Rozenshtein 2018, 149-163). Second was the use of a new framework to determine how societal appetites for surveillance impact policy with consideration of societal tradeoffs (Rozenshtein 2018, 163-172). This thesis explored techniques of surveillance resistance in more depth and with consideration of emergence and feedback stemming from the Top Firms' actions throughout their business ecosystem and environment. For example, Rozenshtein briefly addresses localization and surveillance capitalism, which were both major aspects of this thesis. He mentions that localization could be an unintended consequence of litigation (Rozenshtein 2018, 169) and how different surveillance capitalist business models impact the implementation of encryption between firms (Rozenshtein 2018, 138). This thesis examined both of those topics in more granularity. The risk of localization influenced how firms advocated for legislation in congressional hearings and adversely impacted firms differently based on their network architecture. The variation of surveillance capitalist business models not only impacted their use of end-to-end encryption, but also the use of anonymization techniques and the aggressive lengths firms employed in a data collection arms race. Surveillance capitalism also served as an undercurrent throughout this thesis when evaluating the capacity of firms as corporate avatars. While Rozenshtein kept resistance techniques more compartmentalized, this thesis explored how actions or outcomes

within one affordance had downstream effects to other affordance methods. For example, Rozenshtein discussed the U.S. Supreme Court case *Microsoft v. U.S.* (130) but did not explore its relation to the legislative solutions like the International Communications Privacy Act (ICPA) or the Clarifying Lawful Overseas Use of Data (CLOUD) Act. However, it is worth mentioning that the CLOUD Act was not introduced until a month after Rozenshtein's article was published. This significant event, which rendered the *Microsoft v. U.S.* case moot once enacted, illustrates how just a few months of time can impact analysis of a dynamic topic like surveillance resistance. Furthermore, this dynamism reinforces the importance of continued research that contributes to and advances conversations covering the intersection of public and private sector surveillance.

D. Suggestions for Future Research

A major complication when comparing the ability of firms to resist surveillance was the difference in their business models. The diversity allowed for the exploration of how those differences influenced decision making, but comparing a social media network to a hardware company and a search engine complicates the comparisons between firms of how they use data. Google collects and utilizes search data to improve results specific to a user over time whereas Apple collects and aggregates how many users are using a function in iOS to make broad improvements to that function. By nature of the business, Apple is better equipped to resist surveillance and serve as a corporate avatar.

The Top Firms chosen for this thesis had to meet certain guidelines. The firms needed to be dominant so that they were similarly well resourced to resist surveillance, were multinational and subject to increasingly common data protection laws, and would have received enough requests to have a history in challenging them. In addition, all four Top Firms were named in Snowden's disclosures, raising the stakes for these firms to resist surveillance. Without having to consider a comparable history with U.S. government surveillance, the Top Firms could have included firms that were excluded from this thesis. Of note, there is an emerging business feature that is common among current dominant firms: digital assistants. Like search and social features, digital assistants are designed to be curated to the user necessitating a mass amount of data to fuel machine learning that improves both the user's assistant and every assistant at the same time. All of the digital assistants interact with users via a live mic that waits for a command word. Because four dominant firms are competing in a single space that contributes to network

effects and walled gardens, the firms are highly incentivized to engage users both to establish assistant loyalty and to collect as much data as possible to iterate and make the assistant better than that of the other three firms. As digital assistants complete more tasks for users, the data collected will almost certainly be attractive for U.S government surveillance. If so, measuring how firms handle privacy and business needs could be much more informative when all four firms are competing in the same highly competitive space.

As seen in the market affordance analysis, the public salience of both public and private sector surveillance becomes more pronounced as privacy scandals unfold. Privacy is continually threatened by both the U.S. government and U.S-based firms leaving the public dissatisfied with their lack of control over their own personal information. When Apple fights the FBI over encryption or Congress holds public hearings over Facebook data governance, the public is left standing on the sidelines as mere observers while their privacy rights are debated in a public forum. Future research could explore how public dissatisfaction influenced Rozenshtein's framework used to measure perceptions of societal surveillance tradeoffs and whether the resulting intragovernmental checks truly reflect changes in societal perception of both U.S. government surveillance and surveillance capitalism. Presumably there will be more scandals implicating both types of surveillance. It will be fascinating to see if continued scandals and a public desire for more oversight and accountability lead to the emergence of privacy and surveillance as deciding factors in upcoming midterm and presidential elections.

Chapter VI: Conclusion

Since the Snowden disclosures in 2013, Apple, Facebook, Google, and Microsoft have continued to resist U.S. government surveillance to restore user trust and limit protectionist policies around the world. Existing literature not only presumed that technology firms would be more effective at resisting surveillance than individual citizens, but that firms also were obligated to resist surveillance on behalf of citizens. Using Affordance Theory, this thesis measured the ability of these firms to resist surveillance by focusing on four dominant firms and evaluating the actual measures these firms used to resist surveillance post-Snowden rather than generalized concepts.

The results present a complicated picture. The Top Firms had mixed results resisting surveillance despite being well resourced and influential. Not only were there variances between firms and between affordances, but even within a single affordance for an individual firm. The ability of firms to resist surveillance was heavily influenced by the firm's business model. Existing literature assumed that if a firm prioritized business needs above individual privacy, the result would be an undesired outcome for individuals. But the drive to protect foreign markets made firms more effective and the need to preserve access to mass collected user data made firms less effective. The results revealed the complexities of surveillance resistance. Firms are certainly more equipped to resist surveillance than individual citizens, but their ability to resist surveillance is by no means guaranteed and a firm's capacity as a corporate avatar is more dynamic than previous literature would suggest.

Future research would benefit from a framework that is less structured and can be mapped over time. By observing the limitations of this paper's application of Affordance Theory, a new framework can be advanced that measures not only *if* firms are successful in resisting surveillance, but also the dynamics of *how*, *when*, and *why* they choose to resist surveillance. Once a more complex understanding of firms' surveillance resistance is established, the findings could be applied to the ideological and conceptual inquiries of researchers like Rozenstein. A deeper understanding of firm dynamics within the business environment could provide more informed insight into how firms influence the surveillance environment, particularly when considering the intragovernmental dynamics of political turnover and shifting public perceptions of both public and private sector surveillance.

Bibliography

Abbruzzese, Jason. 2014. "Apple's 2014: By the (Ridiculously Large) Numbers." *Mashable*, October 20, 2014.

<https://mashable.com/2014/10/20/apples-2014-by-the-numbers/#DomAoP7XtgqW>.

Abkowitz, Alyssa, Deepa Seetharaman, and Eva Dou. 2017. "Facebook is Trying Everything to Re-Enter China - and It's Not Working." *Wall Street Journal*, January 30, 2017.

<https://www.wsj.com/articles/mark-zuckerbergs-beijing-blues-1485791106>.

Access Now, *et al.* 2018. "Coalition Letter Opposing the CLOUD Act." *Electronic Frontier Foundation*, March 12, 2018.

<https://www.eff.org/document/coalition-letter-opposing-cloud-act>.

Adobe, *et al.* 2017. "Dear Chairman Goodlatte." *Computer & Communications Industry Associations*, May 26, 2017.

<https://www.ccianet.org/wp-content/uploads/2017/05/702-letter-201705-FINAL.pdf>.

Alba, Davey. 2017. "A Short History of the Many, Many Ways Uber Screwed Up." *WIRED*, June 21, 2017.

<https://www.wired.com/story/timeline-uber-crises/>.

Alba, Davey. 2017. "Google Fights Against Canada's Order to Change Global Search Results." *WIRED*, July 24, 2017.

<https://www.wired.com/story/google-fights-canada-order-global-search-results/>.

Angwin, Julia. 2016. "Google Has Quietly Dropped Ban on Personally Identifiable Web Tracking." *Pro Publica*, October 21, 2016.

<https://www.propublica.org/article/google-has-quietly-dropped-ban-on-personally-identifiable-web-tracking>

Apple. n.d. "Apple products are designed to do amazing things. And designed to protect your privacy." Privacy. Accessed March 26, 2018.

<https://www.apple.com/privacy/>.

Apple. n.d. "Differential Privacy." Privacy. Accessed March 25, 2018.

https://images.apple.com/privacy/docs/Differential_Privacy_Overview.pdf.

Apple. n.d. "iCloud Security Overview." Accessed March 25, 2018.

<https://support.apple.com/en-us/HT202303>.

Apple. n.d. "Newsroom." Accessed March 24, 2018.

<https://www.apple.com/newsroom/>.

Apple. n.d. "This is How We Protect Your Privacy." Privacy. Accessed November 24, 2017.

<https://www.apple.com/privacy/approach-to-privacy/>.

Apple. 2013. "Apple's Commitment to Customer Privacy." Last modified June 16, 2013.

<https://www.apple.com/apples-commitment-to-customer-privacy/>.

Apple. 2016. "Amicus Briefs in Support of Apple." Newsroom. Accessed March 2, 2018.

<https://www.apple.com/newsroom/2016/03/03Amicus-Briefs-in-Support-of-Apple/>.

- Apple. 2018. "Privacy Policy." Legal. Last modified January 19, 2018.
<https://www.apple.com/legal/privacy/en-ww/>.
- Apuzzo, Matt and Nicole Perlroth. 2014. "U.S. Relaxes Some Data Disclosure Rules." *New York Times*, January 27, 2014.
<https://www.nytimes.com/2014/01/28/business/government-to-allow-technology-companies-to-disclose-more-data-on-surveillance-requests.html>.
- Arthur, Charles. 2013. "Google Cleared of Search Results Bias after Two-Year US Investigation." *The Guardian*, January 4, 2013.
<https://www.theguardian.com/technology/2013/jan/03/google-cleared-search-bias-investigation>.
- Article 29 Data Protection Working Party. 2017. "EU - U.S. Privacy Shield - First Annual Joint Review." European Commission, November 28, 2017.
- Bainbridge, Stephen. 2015. "A Duty to Shareholder Value." *New York Times*, April 16, 2015.
<https://www.nytimes.com/roomfordebate/2015/04/16/what-are-corporations-obligations-to-shareholders/a-duty-to-shareholder-value>.
- Balakrishnan, Anita. 2016. "Shares of Apple hit 2016 high amid Samsung woes." *CNBC*, October 10, 2016.
<https://www.cnbc.com/2016/10/10/shares-of-apples-stock-tick-higher-amid-samsung-woes.html>.
- Bangeman, Eric. 2006. "Net neutrality goes up for a vote in Congress." *Ars Technica*, June 8, 2006.
<https://arstechnica.com/uncategorized/2006/06/7016-2/>.
- Barron, Laignee. 2018. "Amnesty International Is Accusing Apple of Betraying Chinese iCloud Users." *TIME*, March 22, 2018.
<http://time.com/5210315/amnesty-international-apple-chinese-icloud-users-china/>.
- BBC News. 2017. "Ireland forced to collect Apple's disputed €13bn tax bill."
<http://www.bbc.com/news/business-42237312>.
- Bedoya, Alvaro M. 2018. "Why Silicon Valley Lobbyists Love Big, Broad Privacy Bills." *New York Times*, April 11, 2018.
<https://www.nytimes.com/2018/04/11/opinion/silicon-valley-lobbyists-privacy.html>.
- Bender, David. 2015. "The Judicial Redress Act: A Path to Nowhere." *IAPP*, December 17, 2015.
<https://iapp.org/news/a/the-judicial-redress-act-a-path-to-nowhere/>.
- Bendix, Aria. 2017. "EU fines Facebook \$122 Million." *The Atlantic*, May 18, 2017.
<https://www.theatlantic.com/news/archive/2017/05/facebook-receives-122-million-fine-from-the-european-union/527325/>.
- Benner, Katie, and Paul Mozur. 2016. "Apple Sees Value in Its Stand to Protect Security." *New York Times*, February 20, 2016.
<https://www.nytimes.com/2016/02/21/technology/apple-sees-value-in-privacy-vow.html>.
- Bhuiyan, Johana. 2018. "Uber powered four billion rides in 2017. It wants to do more - and cheaper - in 2018." *Recode*, January 5, 2018.
<https://www.recode.net/2018/1/5/16854714/uber-four-billion-rides-coo-barney-harford-2018-cut-costs-customer-service>.
- Bigg, Carolyn. 2017. "China: PRC Cybersecurity Law - one week to go and there are still new developments." *Lexology*, May 24, 2017.

<https://www.lexology.com/library/detail.aspx?g=7a0e0922-7051-4345-b73c-313112e7f8a9>.

Bing Ads. 2018. "Ad Solutions for internet advertising." Accessed March 26, 2018.

<https://advertise.bingads.microsoft.com/en-us/solutions>.

Brandom, Russell. 2018. "After Facebook hearing, senators roll out new bill restraining online data use." *The Verge*, April 10, 2018.

<https://www.theverge.com/2018/4/10/17221046/facebook-data-consent-act-privacy-bill-markey-blumenthal>.

Brennan Center for Justice. n.d. "Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs." Accessed November 24, 2017.

<https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf>.

Brill, Julie. 2016. "It's Time to Update the Electronic Communications Privacy Act (ECPA)." *The Hill*, May 25, 2016.

<http://thehill.com/blogs/congress-blog/technology/281106-its-time-to-update-the-electronic-communications-privacy-act>.

Byers, Alex. 2014. "WaPo: POTUS to pivot to Congress on phone records - Buzz: Target agrees to testify on Hill - Walden: Don't Expect FCC to reclassify broadband." *Politico*, January 16, 2014.

<https://www.politico.com/tipsheets/morning-tech/2014/01/wapo-potus-to-pivot-to-congress-on-phone-records-buzz-target-agrees-to-testify-on-hill-walden-dont-expect-fcc-to-reclassify-broadband-212543>.

Calo, Ryan. 2015. "Can Americans Resist Surveillance?" Research Paper No. 2015-25, University of Washington School of Law Legal Studies.

Carmen, Ashley. 2016. "New poll suggests nearly half of Americans support Apple in its fight with the FBI." *The Verge*, February 24, 2016.

<https://www.theverge.com/2016/2/24/11105140/apple-fbi-encryption-american-poll>.

Carson, Biz. 2018. "Lyft Doubled Rides In 2017 As Its Rival Uber Stumbled." *Forbes*, January 16, 2018.

<https://www.forbes.com/sites/bizcarson/2018/01/16/lyft-doubled-rides-in-2017/#a1af3297d6be>.

Castro, Daniel, and Alan McQuinn. 2015. "Beyond the USA Freedom Act: How U.S Surveillance Still Subverts U.S Competitiveness." *The Information Technology & Innovation Foundation*, June 9, 2015.

<https://itif.org/publications/2015/06/09/beyond-usa-freedom-act-how-us-surveillance-still-subverts-us-competitiveness>.

CDT. 2017. "Section 702: What Is It & How It Works." Insights. Last modified February 15, 2017.

<https://cdt.org/insight/section-702-what-it-is-how-it-works/>.

Chacos, Brad. 2017. "Killing Cortana: How to disable Windows 10's info-hungry digital assistant." *PC World*, July 12, 2017.

<https://www.pcworld.com/article/2949759/windows/killing-cortana-how-to-disable-windows-10s-info-hungry-digital-assistant.html>.

Chalfant, Morgan. 2017. "Dreamhost to appeal ruling on DOJ request for data on anti-Trump site." *The Hill*, September 5, 2017.

<http://thehill.com/policy/cybersecurity/349259-dreamhost-intends-to-appeal-ruling-on-doj-request-for-data-on-anti-trump>.

Coles, Cameron. "Overview of Cloud Market in 2017 and Beyond." *Skyhigh*. Accessed April 25, 2018.

<https://www.skyhighnetworks.com/cloud-security-blog/microsoft-azure-closes-iaas-adoption-gap-with-amazon-aws/>.

Colt, Sam. 2014. "Tim Cook Gave His Most In-Depth Interview To Date - Here's What He Said." *Business Insider*, September 20, 2014.

<http://www.businessinsider.com/tim-cook-full-interview-with-charlie-rose-with-transcript-2014-9>.

Comey, James. 2016. "The Encryption Tightrope: Balancing Americans' Security and Privacy." Statement Before the House Committee on the Judiciary United States House of Representatives, March 1, 2016. Audio: 5:31:06.

<https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy/>.

Comey, James. 2016. "We Could Not Look the Survivors in the Eye if We Did Not Follow this Lead." *Lawfare*, February 21, 2016.

<https://www.lawfareblog.com/we-could-not-look-survivors-eye-if-we-did-not-follow-lead>.

Constine, Josh. 2017. "Facebook now has 2 billion users...and responsibility." *Tech Crunch*, June 27, 2017.

<https://techcrunch.com/2017/06/27/facebook-2-billion-users/>.

Cook, Tim. 2016. "A Message to Our Customers." Apple, February 16, 2018.

<https://www.apple.com/customer-letter/>.

Cope, Sophia. 2017. "EFF Supports Senate Email and Location Privacy Bill." *Electronic Frontier Foundation*, July 27, 2017.

<https://www.eff.org/deeplinks/2017/07/eff-applauds-senate-email-and-location-privacy-bill>.

Cover, Adrian Y. 2015. "Corporate Avatars and the Erosion of the Populist Fourth Amendment." *Iowa Law Review*, Vol. 100:1441.

Crusco, Peter A. 2017. "Indefinite Gag Orders Under the Stored Communications Act." *New York Law Journal*, February 27, 2017.

<https://www.law.com/newyorklawjournal/almID/1202779992099/?slreturn=20171024140434>.

Currier, James. 2017. "70% of Value in Tech is Driven by Network Effects." *Medium*, November 28, 2017.

<https://medium.com/@nfx/70-of-value-in-tech-is-driven-by-network-effects-8c4788528e35>.

Daskal, Jennifer. 2016. "Hearing on International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests." Statement Before the House Committee on the Judiciary United States House of Representatives, February 25, 2016.

Daskal, Jennifer. 2018. "New Bill Would Moot Microsoft Ireland Case - And Much More!" *Just Security*, February 6, 2018.

<https://www.justsecurity.org/51886/bill-moot-microsoft-ireland-case-more/>.

Deahl, Dani. 2018. "Senators propose legislation to protect the privacy of users' online data after Facebook hearing." *The Verge*, April 12, 2018.

<https://www.theverge.com/2018/4/12/17231718/facebook-data-privacy-law-klobuchar-kennedy-mark-zuckerberg>.

Determann, Lothar, Brian Hengesbaugh, and Michaela Weigl. 2016. "The EU - U.S. Privacy Shield Versus Other EU Data Transfer Compliance Options." *Bloomberg News*, September 12, 2016.

<https://www.bna.com/euus-privacy-shield-n57982076824/>.

- Digital Due Process. n.d. "Who We Are." Accessed November 15, 2017.
<https://digitaldueprocess.org/>.
- Doherty, Carroll, and Bridget Jameson. 2018. "More Support for Justice Department Than for Apple in Dispute Over Unlocking iPhone." PEW Research Center, February 22, 2018.
<http://www.people-press.org/2016/02/22/more-support-for-justice-department-than-for-apple-in-dispute-over-unlocking-iphone/>.
- Dolven, Taylor, and Alex Thompson. 2018. "Facebook may have broken state and federal law in Cambridge Analytica data share." *VICE News*, March 20, 2018.
https://news.vice.com/en_us/article/43byjb/facebook-may-have-broken-state-and-federal-law-in-cambridge-analytica-data-share.
- Dou, Eva, Jay Greene, and Yang Jie. 2017. "Microsoft Modifies Windows 10 for China's Government." *Wall Street Journal*, March 21, 2017.
<https://www.wsj.com/articles/microsoft-modifies-windows-10-for-chinas-government-1490097182>.
- Drummond, David. 2010. "A New Approach to China." Official Google Blog, January 12, 2010.
<https://googleblog.blogspot.com/2010/01/new-approach-to-china.html>.
- Drummond, David. 2010. "A New Approach to China: An Update." Official Google Blog, March 22, 2010.
<https://googleblog.blogspot.my/2010/03/new-approach-to-china-update.html>.
- Drummond, David. 2013. "Asking the U.S. government to allow Google to publish more national security request data." Official Google Blog, June 11, 2013.
<https://googleblog.blogspot.com/2013/06/asking-us-government-to-allow-google-to.html>.
- Drutman, Lee. 2015. *The Business of America is Lobbying: How Corporations Became Politicized and Politics Became More Corporate*. Oxford University Press.
- Electronic Frontier Foundation. n.d. "End 702: Upstream vs. PRISM." Accessed November 24, 2017.
<https://www.eff.org/pages/upstream-prism>.
- Eoyang, Mieke, Ben Freeman, and Benjamin Wittes. 2018. "Confidence in Government on National Security Matters: December 2017." *Lawfare*, January 9, 2018.
<https://lawfareblog.com/confidence-government-national-security-matters-december-2017>.
- Electronic Frontier Foundation. n.d. "National Security Letters FAQ." Accessed November 24, 2017.
<https://www.eff.org/issues/national-security-letters/faq>.
- EPIC. n.d. "Electronic Communications Privacy Act (ECPA)." Privacy. Accessed November 22, 2017.
<https://epic.org/privacy/ecpa/>.
- EPIC. n.d. "National Security Letters." Privacy. Accessed November 24, 2017.
<https://epic.org/privacy/nsl/>.
- European Commission. 2017. "EU - U.S. Privacy Shield: First review shows it works but implementation can be improved."
http://europa.eu/rapid/press-release_IP-17-3966_en.htm.
- Facebook Inc., Appellant v. New York County District Attorney's Office, Respondent (No.16) (2017), (Appellate Division of the Supreme Court of New York, First Department 2017).
- Facebook. n.d. "Choose Your Audience." Business. Accessed March 26, 2018.

https://www.facebook.com/business/products/ads/ad-targeting#lookalike_audiences.

Facebook. n.d. "Does Facebook sell my information." Help. Accessed March 26, 2018.
https://www.facebook.com/help/152637448140583?helpref=uf_permalink.

Facebook. n.d. "Hard Questions." The Newsroom. Accessed March 24, 2018.
<https://newsroom.fb.com/news/category/hard-questions/>.

Facebook. n.d. "Introducing Hard Questions." The Newsroom. Accessed March 24, 2018.
<https://newsroom.fb.com/news/2017/06/hard-questions/>.

Facebook. n.d. "Newsroom." Accessed March 24, 2018.
<https://newsroom.fb.com/news/>.

Facebook. 2013. "Secure Browsing by Default."
<https://www.facebook.com/notes/facebook-engineering/secure-browsing-by-default/10151590414803920/>.

Farnsworth, Meghann. 2018. "Full transcript: Apple CEO Tim Cook with Recode's Kara Swisher and MSNBC's Chris Hayes." *Recode*, April 6, 2018.
<https://www.recode.net/2018/4/6/17206532/transcript-interview-apple-tim-cook-msnbc-kara-swisher>.

Federal Trade Commission. 2011. "Facebook Settles FTC Charges That It Deceived Consumers By Failing to Keep Privacy Promises."
<https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep>.

Finkle, Jim. 2016. "Solid support for Apple in iPhone encryption fight: poll." *Reuters*, February 24, 2016.
<https://www.reuters.com/article/us-apple-encryption-poll/solid-support-for-apple-in-iphone-encryption-fight-poll-idUSKCN0VX159>.

Fleischer, Peter. 2017. "Three years of striking the right (to be forgotten) balance." *The Keyword*, May 15, 2017.
<https://www.blog.google/topics/google-europe/three-years-right-to-be-forgotten-balance/>.

FutureBrand. n.d. "How do the Global Top 100 companies rank?" Accessed November 13, 2017.
<https://fbi.futurebrand.com/rankings>.

Gallagher, Sean. 2017. "Red Flag Windows: Microsoft Modifies Windows OS for Chinese Government." *Ars Technica*, March 21, 2017.
<https://arstechnica.com/information-technology/2017/03/red-flag-windows-microsoft-modifies-windows-os-for-chinese-government/>.

Garner, Patricia. 2015. "Average revenue per user is an important growth driver." *Yahoo Finance*, February 12, 2015.
<https://finance.yahoo.com/news/average-revenue-per-user-important-210602280.html>.

Gerstein, Josh. 2017. "Judge inches toward demand for data on Trump inaugural protest website." *Politico*, September 20, 2017.
<https://www.politico.com/blogs/under-the-radar/2017/09/20/trump-inaugural-protest-website-data-judge-242946>.

Gidda, Mirren. 2017. "China's New Cybersecurity Law Could Cost Foreign Companies Their Ideas." *Newsweek*, May 31, 2017.
<http://www.newsweek.com/china-cybersecurity-hacking-intellectual-property-multinationals-618345>.

Goode, Lauren. 2016. "iMessage is the glue that keeps me stuck to the iPhone." *The Verge*, October 10, 2016.
<https://www.theverge.com/2016/10/10/13225514/apple-iphone-cant-switch-pixel-android-imessage-addiction>.

Google. n.d. "Advertising." Privacy and Terms. Accessed March 26, 2018.
<https://www.google.com/policies/technologies/ads/>.

Google. n.d. "Email encryption in transit." Accessed March 25, 2018.
<https://transparencyreport.google.com/safer-email/overview>.

Google. n.d. "How Ads Work." Privacy. Accessed March 26, 2018.
<https://privacy.google.com/how-ads-work.html>.

Google. n.d. "HTTPS encryption on the web." Accessed March 25, 2018.
<https://transparencyreport.google.com/https/overview>.

Google. n.d. "Public Policy." The Keyword. Accessed March 24, 2018.
<https://www.blog.google/topics/public-policy/>.

Google. n.d. "Security." Google Cloud Help. Accessed November 24, 2017.
<https://support.google.com/googlecloud/answer/6056693?hl=en>.

Google. 2013. "Google Cloud Storage now provides server-side encryption."
<https://cloudplatform.googleblog.com/2013/08/google-cloud-storage-now-provides.html>.

Google. 2014. "Staying at the forefront of email security and reliability: HTTPS-only and 99.978 percent availability." Google Official Blog, March 20, 2014.
<https://googleblog.blogspot.nl/2014/03/staying-at-forefront-of-email-security.html>.

Granick, Jennifer. 2016. "The Microsoft Ireland Case and the Future of Digital Privacy." *Just Security*, July 18, 2016.
<https://www.justsecurity.org/32076/microsoft-ireland-case-future-digital-privacy/>.

Grassley, Senator Chuck. 2017. "The FISA Amendments Act: Reauthorizing America's Vital National Security Authority and Protecting Privacy and Civil Liberties." Statement Before the Committee on the Judiciary, June 27, 2017. Audio: 2:54:04.
<https://www.judiciary.senate.gov/meetings/the-fisa-amendments-act-reauthorizing-americas-vital-national-security-authority-and-protecting-privacy-and-civil-liberties>.

Greenberg, Andy. 2017. "After 3 Years, Why Gmail's End-to-End Encryption is Still Vapor." *WIRED*, February 28, 2017.
<https://www.wired.com/2017/02/3-years-gmails-end-end-encryption-still-vapor/>.

Greenberg, Andy. 2016. "Apple's 'Differential Privacy' is About Collecting Your Data - But Not Your Data." *WIRED*, June 13, 2016.
<https://www.wired.com/2016/06/apples-differential-privacy-collecting-data/>.

Greenberg, Andy. 2016. "You Can Finally Encrypt Facebook Messenger, So Do It." *WIRED*, October 4, 2016.

<https://www.wired.com/2016/10/facebook-completely-encrypted-messenger-update-now/>.

Hare, Stephanie. 2016. "For your eyes only: U.S technology companies, sovereign states, and the battle over data protection." Indiana University Kelley School of Business. Elsevier 59.

Hatch, Senator Orrin. 2017. "Hatch, Coons Introduce International Communications Privacy Act (ICPA)."

<https://www.hatch.senate.gov/public/index.cfm/releases?ID=74D25161-D3F6-401E-A0AC-E16609D3FC1F>.

Hatch, Senator Orrin. 2017. "Hatch Urges Senators to Support International Communications Privacy Act."

<https://www.hatch.senate.gov/public/index.cfm/releases?ID=D82974EA-BA0C-494B-A3A1-89A7926FB802>.

Hatmaker, Taylor. 2018. "As the CLOUD Act sneaks into the omnibus, big tech butts heads with privacy advocates." *Tech Crunch*, March 22, 2018.

<https://techcrunch.com/2018/03/22/cloud-act-omnibus-bill-house/>.

Hawkins, Andrew J. 2017. "Lyft surpasses Uber in app downloads for the first time ever." *The Verge*, January 30, 2017.

<https://www.theverge.com/2017/1/30/14443560/lyft-surpass-uber-app-downloads-deleteuber>.

Higgins, Parker. 2013. "Pushing for Perfect Forward Secrecy, an Important Web Privacy Protection." *Electronic Frontier Foundation*, August 28, 2013.

<https://www.eff.org/deeplinks/2013/08/pushing-perfect-forward-secrecy-important-web-privacy-protection>.

Hodgkins III, A.R "Trey", and Jonathan S. Kallmer. n.d. "Response of the Information Technology Industry Council and the IT Alliance for Public Sector to Request for Comments on the Cost and Benefits of US International Government Procurement Obligations and 'Buy American' Policies." ITIC. Accessed September 25, 2017.

<https://www.itic.org/dotAsset/535e2fbe-d0d3-42a7-bc91-faca4725fd29.pdf>.

Hölzle, Urs. 2018. "Freedom of data movement in the cloud era." *The Keyword*, February 22, 2018.

<https://blog.google/topics/google-cloud/freedom-data-movement-cloud-era/>.

Information Commissioner's Office. n.d. "Guide to the General Data Protection Regulation (GDPR)." Accessed February 25, 2018.

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr>.

Ingram, David. 2017. "Google, Facebook show power of ad duopoly as rivals stumble." *Reuters*, July 28, 2017.

<https://www.reuters.com/article/us-alphabet-facebook-analysis/google-facebook-show-power-of-ad-duopoly-as-rivals-stumble-idUSKBN1AD1ZY>.

Isaac, Mike. 2017. "Uber Board Stands by Travis Kalanick It Reveals Plans to Repair Its Image." *New York Times*, March 21, 2017.

<https://www.nytimes.com/2017/03/21/technology/uber-board-stands-by-travis-kalanick.html>.

Isaac, Mike, Katie Benner, and Sheera Frenkel. 2017. "Uber Hid 2016 Breach, Paying Hackers to Delete Stolen Data." *New York Times*, November 21, 2017.

<https://www.nytimes.com/2017/11/21/technology/uber-hack.html>.

Jacobs, Brian. 2017. "A Cloud Over the Microsoft Warrant Case." *Forbes*, May 1, 2017.
<https://www.forbes.com/sites/insider/2017/05/01/a-cloud-over-the-microsoft-warrant-case/#7fd106c05dab>.

Jeong, Sarah. 2018. "The Supreme Court Fight over Microsoft's Foreign Servers Is over." *The Verge*, April 5, 2018.
<https://www.theverge.com/2018/4/5/17203630/us-v-microsoft-scotus-doj-ireland-ruling>.

Kalia, Amul. 2016. "With Windows 10, Microsoft Blatantly Disregards User Choice and Privacy: A Deep Dive." *Electronic Frontier Foundation*, August 17, 2016.
<https://www.eff.org/deeplinks/2016/08/windows-10-microsoft-blatantly-disregards-user-choice-and-privacy-deep-dive>.

Kam, Kan. 2018. "Buy Facebook in the Wake of Irrational Pessimism." *Forbes*, March 20, 2018.
<https://www.forbes.com/sites/kenkam/2018/03/20/buy-facebook-in-the-wake-of-irrational-pessimism/#31c44bf23b5d>.

Kang, Cecilia, Daisuke Wakabayashi, Nick Wingfield, and Mike Isaac. 2017. "Net Neutrality Protests Move Online, Yet Big Tech is Quiet." *New York Times*, December 12, 2017.
<https://www.nytimes.com/2017/12/12/technology/net-neutrality-fcc-tech.html>.

Kaufman, Brett Max. 2014. "NSA Surveillance Scandal Began One Year Ago. Here's What Tech Companies Still Need to Do." *Slate*, June 5, 2014.
http://www.slate.com/blogs/future_tense/2014/06/05/snowden_nsa_scandal_anniversary_four_things_tech_companies_still_need_to.html.

Kelly, Erin. 2018. "Zuckerberg: Federal regulation of Facebook 'inevitable.'" *USA Today*, April 11, 2018.
<https://www.usatoday.com/story/news/politics/2018/04/11/zuckerberg-federal-regulation-facebook-inevitable-faces-second-day-capitol-hill-hearings-facebook-pr/506235002/>.

Kendrick, Katharine. 2015. "Risky Business: Data Localization." *Forbes*, February 19, 2015.
<https://www.forbes.com/sites/realspin/2015/02/19/risky-business-data-localization/#3936af941077>.

Kopfstein, Janus. 2013. "Silicon Valley's Surveillance Cure-All: Transparency." *The New Yorker*, October 1, 2013.
<https://www.newyorker.com/tech/elements/silicon-valleys-surveillance-cure-all-transparency>.

Kravets, David. 2017. "Google stops challenging most US warrants for data on overseas servers." *Ars Technica*, September 9, 2017.
<https://arstechnica.com/tech-policy/2017/09/feds-google-stops-challenging-most-us-warrants-for-data-on-overseas-servers/>.

Kuchler, Hannah. 2014. "Tech companies step up encryption in wake of Snowden." *Financial Times*, November 4, 2014.
<https://www.ft.com/content/3c1553a6-6429-11e4-bac8-00144feabdco>.

Kumar, Priya. 2017. "Corporate Privacy Policy Changes during PRISM and the Rise of Surveillance Capitalism." *Media and Communication*, Vol. 5 Issue (1m): 63-75. University of Mayland.

La Monica, Paul R. 2016. "Apple's stock has worms but FBI isn't one of them." *CNN Money*, February 24, 2016.
<http://money.cnn.com/2016/02/24/investing/apple-stock-fbi-iphone/index.html>.

- Larson, Selena. 2018. "Investors sue Facebook following data harvesting scandal." *CNN Tech*, March 21, 2018.
<http://money.cnn.com/2018/03/20/technology/business/investors-sue-facebook-cambridge-analytica/index.html>.
- Leahy, Patrick. 2015. "Summary of the Electronic Communications Privacy Act Amendments Act of 2015." Accessed March 22, 2018.
<https://www.leahy.senate.gov/imo/media/doc/Section%20by%20Section%20ECPA%20Reform%20Bill%20%202015.pdf>.
- Lien, Tracey and Paresh Dave. 2016. "Apple's Tim Cook to Shareholders: Taking on the FBI is the right thing to do." *Los Angeles Times*, February 26, 2016.
<http://www.latimes.com/business/technology/la-fi-tn-apple-shareholder-meeting-fbi-20160226-story.html>.
- Liptak, Andrew. 2018. "President Donald Trump has signed the FISA reauthorization bill." *The Verge*, January 20, 2018.
<https://www.theverge.com/2018/1/20/16913534/president-donald-trump-signed-fisa-amendments-reauthorization-act-of-2017-section-702>.
- Lo, Andrew W. and Erik Brynjolfsson. 2016. "The Rise of Digital Capital." *MIT Technology Review Custom*, March 21, 2016.
<https://www.technologyreview.com/s/601081/the-rise-of-data-capital/>.
- Lobbying Disclosure. 2017. "Apple, Inc."
<http://disclosures.house.gov/ld/ldxmlrelease/2017/Q4/300934335.xml>
- Lobbying Disclosure. 2017. "Facebook, Inc."
<http://disclosures.house.gov/ld/ldxmlrelease/2017/Q4/300935366.xml>
- Lobbying Disclosure. 2017. "Google, Inc."
<http://disclosures.house.gov/ld/ldxmlrelease/2017/Q4/300935200.xml>
- Lobbying Disclosure. 2017. "Microsoft Corporation."
<http://disclosures.house.gov/ld/ldxmlrelease/2017/Q4/300935780.xml>
- Lovells, Hogan. 2015. "USA FREEDOM Act: A Step Toward Restoring Trust?" *IAPP*, June 25, 2015.
<https://iapp.org/news/a/usa-freedom-act-a-step-toward-restoring-trust/>.
- Lowensohn, Josh. 2013. "Apple's 2013 by the numbers: 150M iPhones, 71M iPads." *CNet*, October 28, 2013.
<https://www.cnet.com/news/apples-2013-by-the-numbers-150m-iphones-71m-ipads/>.
- Madden, Mary and Lee Rainie. 2015. "Americans' Attitudes About Privacy, Security, and Surveillance." PEW Research Center, May 20, 2015.
<http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/>.
- Manjoo, Farhad. 2016. "Tech's 'Frightful Five' Will Dominate Digital Life for the Foreseeable Future." *New York Times*, January 20, 2016.
<https://www.nytimes.com/2016/01/21/technology/techs-frightful-5-will-dominate-digital-life-for-foreseeable-future.html>.

Matsakis, Louise. 2018. "Congress Renews Warrantless Surveillance - And Makes It Even Worse." *WIRED*, January 11, 2018.
<https://www.wired.com/story/fisa-section-702-renewal-congress/>.

McKirdy, Euan. 2015. "China's online users more than double entire U.S. population." *CNN*, February 4, 2015.
<https://www.cnn.com/2015/02/03/world/china-internet-growth-2014/index.html>.

Menn, Joseph. 2016. "Exclusive: Yahoo secretly scanned customer emails for U.S. Intelligence sources." *Reuters*, October 4, 2016.
<https://www.reuters.com/article/us-yahoo-nsa-exclusive/exclusive-yahoo-secretly-scanned-customer-emails-for-u-s-intelligence-sources-idUSKCN1241YT>.

Meyer, David. 2017. "This Privacy Case Could Threaten Facebook's European Operations – Again." *Fortune*, October 3, 2017.
<http://fortune.com/2017/10/03/facebook-max-schrems-ireland-cjeu-privacy/>.

Mickle, Tripp and Lukas I. Alpert. 2017. "Apple Pulls New York Times App From China Store." *Wall Street Journal*, January 4, 2017.
<https://www.wsj.com/articles/apple-pulls-new-york-times-app-from-china-store-1483576379>.

Microsoft. n.d. "Data Law." Accessed March 24, 2018.
<https://blogs.microsoft.com/datalaw/>.

Microsoft. n.d. "Encryption." Trust Center. Accessed March 26, 2018.
<https://www.microsoft.com/en-us/trustcenter/security/encryption#Secure-identity>.

Microsoft. n.d. "Microsoft On the Issues." Accessed March 24, 2018.
<https://blogs.microsoft.com/on-the-issues/>.

Microsoft. n.d. "U.S. National Security Orders Report." Accessed November 24, 2017.
<https://www.microsoft.com/en-us/about/corporate-responsibility/fisa>.

Microsoft. 2013. "Statement from Microsoft about response to government demands for customer data." <https://news.microsoft.com/2013/07/11/statement-from-microsoft-about-response-to-government-demands-for-customer-data/>.

Miller, Ron. 2016. "How AWS came to be." *Tech Crunch*, July 2, 2016.
<https://techcrunch.com/2016/07/02/andy-jassys-brief-history-of-the-genesis-of-aws/>.

Miller, Ron. 2018. "Google's Diane Greene says billion-dollar cloud revenue already puts them in elite company." *Tech Crunch*, February 1, 2018.
<https://techcrunch.com/2018/02/01/googles-diane-greene-says-billion-dollar-cloud-revenue-already-puts-them-in-elite-company/>.

Minter, Adam. 2017. "Google's China Bid Won't End Well." *Bloomberg*, December 18, 2017.
<https://www.bloomberg.com/view/articles/2017-12-18/google-s-latest-china-venture-will-end-like-the-rest>.

Molla, Rani. 2018. "Mark Zuckerberg's testimony helped Facebook's stock — but the price still has a long road to recovery." *Recode*, April 13, 2018.
<https://www.recode.net/2018/4/13/17234830/facebook-mark-zuckerberg-testimony-congress-stock>.

- Moody, Glyn. 2015. "Microsoft Building Data Centers in Germany that US government can't touch." *Ars Technica*, November 12, 2015.
<https://arstechnica.com/information-technology/2015/11/microsoft-is-building-data-centres-in-germany-that-the-us-government-cant-touch/>.
- Mozur, Paul and Nick Wingfield. 2016. "Microsoft Faces New Scrutiny in China." *New York Times*, January 5, 2016.
<https://www.nytimes.com/2016/01/06/business/international/microsoft-china-antitrust-inquiry.html>.
- Mullins, Brody, Rolfe Winkler, and Brent Kendall. 2015. "Inside the U.S. Antitrust Probe of Google." *Wall Street Journal*, March 19, 2015.
<https://www.wsj.com/articles/inside-the-u-s-antitrust-probe-of-google-1426793274>.
- Murphy, Mike. 2017. "Apple's 'walled garden' approach to content has paid off massively." *Quartz*, August 3, 2017.
<https://qz.com/1045671/apples-walled-garden-approach-to-apps-and-music-has-paid-off-massively-aapl/>.
- Myers, Anna. 2017. "The Email Privacy Act: What happened and where we are now." *IAPP*, January 19, 2017.
<https://iapp.org/news/a/the-email-privacy-act-what-happened-and-where-we-are-now/>.
- Nakashima, Ellen. 2017. "Justice Department moves to end routine gag orders on tech firms." *Washington Post*, October 24, 2017.
https://www.washingtonpost.com/world/national-security/justice-department-moves-to-end-routine-gag-orders-on-tech-firms/2017/10/23/df8300bc-b848-11e7-9e58-e6288544af98_story.html?utm_term=.438838ba4b95.
- Nellis, Stephen and Cate Cadell. 2018. "Apple moves to store iCloud keys in China, raising human rights fears." *Reuters*, February 23, 2018.
<https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8o6o>.
- Newell, Jim. 2013. "Thousands gather in Washington for anti-NSA 'Stop Watching Us' rally." *The Guardian*, October 26, 2013.
<https://www.theguardian.com/world/2013/oct/26/nsa-rally-stop-watching-washington-snowden>.
- Newman, Lily Hay. 2018. "Don't Trust the VPN Facebook Wants You to Use." *WIRED*, February 15, 2018.
<https://www.wired.com/story/facebook-onavo-protect-vpn-privacy/>.
- Newman, Lily Hay. 2018. "Skype's Rolling Out End-to-end Encryption For Hundreds of Millions of People." *WIRED*, January 11, 2018.
<https://www.wired.com/story/skype-end-to-end-encryption-voice-text/>.
- Nojeim, Greg. 2014. "LEADS Act Extends Important Privacy Protections, Raises Concerns." *CDT*, September 18, 2014.
<https://cdt.org/blog/leads-act-extends-important-privacy-protections-raises-concerns/>.
- Nojeim, Greg. 2015. "MLAT Reform: A Straw Man Proposal." *CDT*, September 3, 2015.
<https://cdt.org/insight/mlat-reform-a-straw-man-proposal/>.
- O'Brien, Danny. 2017. "Who Speak for The Billions of Victims of Mass Surveillance? Tech Companies Could." *Electronic Frontier Foundation*, October 30, 2017.
<https://www.eff.org/deeplinks/2017/10/tech-companies-could-fight-non-us-surveillance>.

O'Connor, Nuala. 2018. "Reforming the U.S. Approach to Data Protection and Privacy." *Council on Foreign Affairs*, January 30, 2018.

<https://www.cfr.org/report/reforming-us-approach-data-protection>.

Ong, Thuy. 2018. "Over 90 percent of Gmail users still don't use two-factor authentication." *The Verge*, January 23, 2018.

<https://www.theverge.com/2018/1/23/16922500/gmail-users-two-factor-authentication-google>.

Ortutay, Barbara. 2018. "Facebook's Stock is Taking Another Big Plunge Today. Here's Why." *TIME*, March 26, 2018.

<http://time.com/5215500/facebook-stock-ftc-investigation/>.

Page, Larry. 2013. "What The..." Google Official Blog, June 7, 2013.

<https://googleblog.blogspot.com/2013/06/what.html>.

Paul, Ian. 2016. "You can't turn off Cortana in the Windows 10 Anniversary Update." *PC World*, July 26, 2016.

<https://www.pcworld.com/article/3100358/windows/you-cant-turn-off-cortana-in-the-windows-10-anniversary-update.html>.

Pfeifle, Sam. 2015. "'Uncertainty' is the word of the day in privacy circles." *IAPP*, October 6, 2015.

<https://iapp.org/news/a/safe-harbor-invalid-rules-ecj/>.

Popper, Ben. 2017. "The Tech Sector is Leaving the Rest of the US Economy in its dust." *The Verge*, May 16, 2017.

<https://www.theverge.com/2017/5/16/15627198/tech-sector-stock-market-record-high>.

Privacy Shield Framework. n.d. "Privacy Shield List." Accessed November 15, 2017.

<https://www.privacyshield.gov/list>.

Prokop, Andrew. 2018. "Cambridge Analytica and its many scandals, explained." *Vox*, April 4, 2018.

<https://www.vox.com/policy-and-politics/2018/3/21/17141428/cambridge-analytica-trump-russia-mueller>.

Protalinski, Emil. 2013. "Facebook passes 1.19 billion monthly active users, 874 million mobile users, and 728 million daily users." *TNW*, October 30, 2013.

<https://thenextweb.com/facebook/2013/10/30/facebook-passes-1-19-billion-monthly-active-users-874-million-mobile-users-728-million-daily-users/>.

Protalinski, Emil. 2014. "Facebook passes 1.35B monthly active users and 864M daily active users, with a third now mobile-only." *Venture Beat*, October 28, 2014.

<https://venturebeat.com/2014/10/28/facebook-passes-1-35b-monthly-active-users-and-864m-daily-active-users-with-a-third-now-mobile-only/>.

Rainie, Lee and Mary Madden. 2015. "Americans' Privacy Strategies Post-Snowden." PEW Research Center, March 16, 2015.

<http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/>.

Reeves, Martin, Simon Levin, and Daichi Ueda. 2016. "The Biology of Corporate Survival." *Harvard Business Review*, January – February 2016.

<https://hbr.org/2016/01/the-biology-of-corporate-survival>.

Reform Government Surveillance. n.d. "Global Government Surveillance Reform." Accessed March 24, 2018.

<https://www.reformgovernmentsurveillance.com/>.

Reform Government Surveillance. 2017. "Reform Government Surveillance Statement on the Introduction of the USA Liberty Act, H.R. 3989."

<http://www.reformgovernmentsurveillance.com/reform-government-surveillance-statement-on-the/>.

Reform Government Surveillance. 2017. "Statement on FISA Amendments Reauthorization Act of 2017, H.R. 4478."

<http://www.reformgovernmentsurveillance.com/statement-on-the-fisa-amendments-reauthorization/>.

Reisinger, Don. 2017. "Why Ted Cruz and Patrick Leahy Are Worried Apple is 'Enabling' Chinese Censorship." *Fortune*, October 20, 2017.

<http://fortune.com/2017/10/20/ted-cruz-apple-china-censorship/>.

Reitman, Rainey. 2017. "USA Liberty Act Won't Fix What's Most Broken with NSA Internet Surveillance." *Electronic Frontier Foundation*, October 16, 2017.

<https://www.eff.org/deeplinks/2017/10/usa-liberty-act-wont-fix-whats-most-broken-nsa-internet-surveillance>.

Reitman, Rainey. 2017. "Who Has Your Back? Government Data Requests 2017." *Electronic Frontier Foundation*, July 10, 2017.

<https://www.eff.org/who-has-your-back-2017#executive-summary>.

Richardson, Michelle. 2017. "We Know a Lot More About U.S. Spying Since Section 702's Last Reauthorization." *Just Security*, September 8, 2017.

<https://www.justsecurity.org/44793/lot-u-s-spying-section-702s-reauthorization/>.

Rosen, Alex. 2017. "Encryption: A Double Edged Sword." *American Security Project*, February 2, 2017.

<https://www.americansecurityproject.org/encryption-a-double-edged-sword/>.

Rosenzweig, Paul, Charles Stimson, and David Shedd. 2016. "Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program." *The Heritage Foundation*, May 13, 2016.

<http://www.heritage.org/defense/report/maintaining-americas-ability-collect-foreign-intelligence-the-section-702-program>.

Rozenshtein, Alan Z. 2018. "Surveillance Intermediaries." *Stanford Law Review* Vol. 70: 99.

Sacks, Samm, Paul Triolo, and Graham Webster. 2017. "Beyond the Worst Case Assumptions on China's Cybersecurity Law." *New America*, October 13, 2017.

<https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/>.

Salgado, Richard. 2013. "ECPA Part 1: Lawful Access to Stored Content." Statement Before the House Committee on the Judiciary United States House of Representatives, March 19, 2013. Audio, 1:20:43.

<https://judiciary.house.gov/hearing/ecpa-part-1-lawful-access-to-stored-content-0/>.

Salgado, Richard. 2017. "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era." Statement Before the House Committee on the Judiciary United States House of Representatives, June 15, 2017. Audio, 3:50:52.

<https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era/>.

- Salgado, Richard. 2017. "Updating Our Transparency Report and electronic privacy laws." *The Keyword*, September 28, 2017.
<https://www.blog.google/topics/public-policy/updating-our-transparency-report-and-electronic-privacy-laws/>.
- Samee Ali, Safia and Halimah Abdullah. 2016. "Did the Patriot Act Change US Attitudes on Surveillance?" *NBC News*, September 8, 2016.
<https://www.nbcnews.com/storyline/9-11-anniversary/did-patriot-act-change-us-attitudes-surveillance-n641586>.
- Sargsyan, Tatevik. 2016. "Data Localization and the Role of Infrastructure for Surveillance, Privacy, Security." *International Journal of Communication*, no. 10 (2016): 2221-2237. doi: 1932-8036/20160005.
- Scarantino, Andrea. 2003. "Affordance Explained." *Philosophy of Science* Vol. 70, No.5.
- SCOTUSblog. n.d. "United States v. Microsoft Corp." Accessed February 28, 2018.
<http://www.scotusblog.com/case-files/cases/united-states-v-microsoft-corp/>.
- Seifert, Dan. 2013. "Secret program gives NSA, FBI backdoor access to Apple, Google, Facebook, Microsoft data." *The Verge*, June 6, 2013.
<https://www.theverge.com/2013/6/6/4403868/nsa-fbi-mine-data-apple-google-facebook-microsoft-others-prism>.
- Senate Judiciary Committee. 2013. "An Open Letter to Washington."
<https://www.judiciary.senate.gov/imo/media/doc/121113RecordSub-Leahy.pdf>.
- Sewell, Bruce. 2016. "The Encryption Tightrope: Balancing Americans' Security and Privacy." Statement Before the House Committee on the Judiciary United States House of Representatives, March 1, 2016. Audio: 5:31:06. <https://judiciary.house.gov/hearing/the-encryption-tightrope-balancing-americans-security-and-privacy/>.
- Shankleman, Jessica. 2014. "Tim Cook tells climate change sceptics to ditch Apple shares." *The Guardian*, March 3, 2014.
<https://www.theguardian.com/environment/2014/mar/03/tim-cook-climate-change-sceptics-ditch-apple-shares>.
- Siddiqui, Faiz. 2017. "#Deleteuber will have lasting fallout for ride-hailing app, study says." *The Washington Post*, May 16, 2017.
https://www.washingtonpost.com/news/dr-gridlock/wp/2017/05/16/deleteuber-will-have-lasting-fallout-for-ride-hailing-app-study-says/?utm_term=.0a1018d567fb.
- Skype. n.d. "Does Skype use encryption?" Support. Accessed March 26, 2018.
<https://support.skype.com/en/faq/FA31/does-skype-use-encryption>.
- Smith, Brad. 2013. "Protecting customer data from government snooping." *Microsoft on the Issues*, December 4, 2013.
<https://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/>.
- Smith, Brad. 2016. "International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests." Statement Before the House Committee on the Judiciary United States House of Representatives, February 25, 2016. Audio: 4:08:17.
<https://judiciary.house.gov/hearing/international-conflicts-of-law-concerning-cross-border-data-flow-and-law-enforcement-requests/>.

Smith, Brad. 2017. "A legislative path to create new laws is better than arguing over old laws." *Microsoft on the Issues*, June 23, 2017.
<https://blogs.microsoft.com/on-the-issues/2017/06/23/legislative-path-create-new-laws-better-arguing-old-laws/>.

Smith, Brad. 2017. "Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights." Statement Before the House Committee on the Judiciary United States House of Representatives, May 10, 2017. Audio: 2:24:44.
<https://www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights>.

Smith, Brad. 2017. "US Supreme Court will hear petition to review Microsoft search warrant case while momentum to modernize the law continues in Congress." *Microsoft on the Issues*, October 16, 2017.
<https://blogs.microsoft.com/on-the-issues/2017/10/16/us-supreme-court-will-hear-petition-to-review-microsoft-search-warrant-case-while-momentum-to-modernize-the-law-continues-in-congress/>.

Smith, Brad and Carol Anne Brown. 2018. "Today in Technology: The Top Ten Tech Issues for 2018." *Microsoft on the Issues*, January 2, 2018.
<https://blogs.microsoft.com/on-the-issues/2018/01/02/today-technology-top-ten-tech-issues-2018/>.

Smith, H. Jeff. 2003. "The Shareholders vs. Stakeholders Debate." *MIT Sloan Management Review*, July 15, 2003.
<https://sloanreview.mit.edu/article/the-shareholders-vs-stakeholders-debate/>.

Soghoian, Christopher. 2015. "An End to Privacy Theater: Exposing and Discouraging Corporate Disclosure of User Data to the Government." TPRC 2010.

Sonderby, Chris. 2017. "Reinforcing Our Commitment to Transparency." *Newsroom*, December 18, 2017.
<https://newsroom.fb.com/news/2017/12/reinforcing-our-commitment-to-transparency/>.

Stinson, Elizabeth. 2017. "How the Internet Showed Up for Net Neutrality Today from Reddit to Google." *WIRED*, July 12, 2017.
<https://www.wired.com/story/day-of-action-internet-protests-google-facebook-reddit/>.

Strumpf, Dan. 2017. "Apple's Tim Cook: No Point Yelling at China." *Wall Street Journal*, December 7, 2017.
<https://www.wsj.com/articles/apples-tim-cook-no-point-yelling-at-china-1512563332>.

Swisher, Kara. 2015. "White House. Red Chair. Obama Meets Swisher." *Recode*, February 15, 2015.
<https://www.recode.net/2015/2/15/11559056/white-house-red-chair-obama-meets-swisher>.

The Economist. 2010. "Shareholders v Stakeholders: A new idolatry."
<http://www.economist.com/node/15954434#print>.

The Economist. 2017. "Data is giving rise to a new economy."
<http://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>.

The Economist. 2017. "The European Union levies a record fine of €2.4bn against Google."
<https://www.economist.com/news/business/21724312-google-allegedly-abused-its-market-dominance-search-european-union-levies-record-fine>.

Timberg, Craig, Romm, Tony, Dwoskin, Elizabeth. 2018. "Lawmakers agree social media needs regulation, but say prompt federal action is unlikely." *Washington Post*, April 11, 2018.

https://www.washingtonpost.com/business/technology/lawmakers-agree-social-media-needs-regulation-but-say-prompt-federal-action-is-unlikely/2018/04/11/d3ce71bo-3daf-11e8-8d53-eba0ed2371cc_story.html?noredirect=on&utm_term=.dd3a05a411d4.

Turner, Nathaniel J. 2017. "The House Takes a Big Step Toward Protecting Privacy in the Digital Age." *ACLU*, April 27, 2017.

<https://www.aclu.org/blog/privacy-technology/internet-privacy/house-takes-big-step-toward-protecting-privacy-digital-age>.

Turow, Joseph, Michael Hennessy, and Nora Draper. 2015. "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation." Annenberg School for Communication, University of Pennsylvania.

<https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and>.

U.S. Congress. n.d. "S.2986 - International Communications Privacy Act." Accessed November 15, 2017.

<https://www.congress.gov/bill/114th-congress/senate-bill/2986?q=%7B%22search%22%3A%5B%22international+communications+privacy+act%22%5D%7D&r=3>.

U.S. Department of Justice. 2014. "Dear General Counsels."

<https://www.justice.gov/iso/opa/resources/366201412716018407143.pdf>.

U.S. Department of Justice. n.d. "Electronic Communications Privacy Act of 1986 (ECPA)." Federal Statutes. Accessed November 24, 2017.

<https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285>.

U.S. Department of State. n.d. "EU - U.S. Privacy Shield Ombudsman." Accessed February 24, 2017.

<https://www.state.gov/e/privacyshield/ombud/>.

U.S. House of Representatives. n.d. "FISA Section 702." Accessed March 1, 2018.

<https://intelligence.house.gov/fisa-702/>.

Vincent, James. 2017. "99.6 percent of new smartphones run Android or iOS." *The Verge*, February 16, 2017.

<https://www.theverge.com/2017/2/16/14634656/android-ios-market-share-blackberry-2016>.

Volz, Dustin. 2017. "U.S. Signals Tougher Stance with Tech Companies on Encryption." *U.S. News and World Report*, October 10, 2017.

<https://www.usnews.com/news/technology/articles/2017-10-10/us-signals-tougher-stance-with-tech-companies-on-encryption>.

Warren, Tom. 2015. "Microsoft reveals how it will make money giving away software." *The Verge*, March 16, 2015.

<https://www.theverge.com/2015/3/16/8227847/how-microsoft-makes-money>.

Weisman, Jonathan. 2013. "Momentum Builds Against N.S.A. Surveillance." *New York Times*, July 28, 2013.

<http://www.nytimes.com/2013/07/29/us/politics/momentum-builds-ag...ef=www.nytimes.com&mtref=www.nytimes.com&mtref=www.nytimes.com>.

Welch, Chris. 2013. "Apple, Google, Facebook, Microsoft, Google, Yahoo and more deny providing direct access to PRISM surveillance program." *The Verge*, June 6, 2013.

<https://www.theverge.com/2013/6/6/4404112/nsa-prism-surveillance-apple-facebook-google-respond>.

Welch, Chris. 2018. "Tim Cook wants 'well-crafted' privacy regulations after latest Facebook scandal." *The Verge*, March 24, 2018.
<https://www.theverge.com/2018/3/24/17159610/apple-ceo-tim-cook-wants-privacy-regulation-facebook-cambridge-analytica>.

White, Jeremy B. 2017. "Trump administration orders Facebook to hand over private information on 'anti-administration activists.'" *The Independent*, September 29, 2017.
<https://www.independent.co.uk/news/trump-facebook-information-order-anti-administration-activists-data-hand-over-a7974746.html>.

Whittaker, Zack. 2016. "More Snowden fallout? China bans Apple services in latest blow to US tech industry." *ZD Net*, April 22, 2016.
<http://www.zdnet.com/article/china-finally-hitting-us-where-it-hurts-in-nsa-spying-aftermath/>.

Wilhelm, Alex. 2017. "Tech's 5 biggest players now worth \$3 trillion." *Tech Crunch*, July 19, 2017.
<https://techcrunch.com/2017/07/19/techs-5-biggest-players-now-worth-3-trillion/>.

Woods, Andrew Keane. 2015. "Procedural Options for Improving Cross-Border Requests for Data." *Lawfare*, October 13, 2015.
<https://www.lawfareblog.com/procedural-options-improving-cross-border-requests-data>.

Woods, Andrew Keane. 2017. "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era." Statement Before the House Committee on the Judiciary United States House of Representatives, June 15, 2017. Audio: 3:50:52.
<https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era/>.

Wyden, Ron. n.d. "The USA Rights Act." Accessed March 22, 2018.
<https://www.wyden.senate.gov/imo/media/doc/102017%20USA%20RIGHTS%20Act%20one-pager.pdf>.

Zuckerberg, Mark. 2013. "I want to respond personally to the outrageous press reports about PRISM." Facebook, June 7, 2013.
<https://m.facebook.com/zuck/posts/10100828955847631>.