Journal of Technology Law & Policy

Volume XX – 2019-2020

ISSN 2164-800X (online)

DOI 10.5195/tlp.2020.234

http://tlp.law.pitt.edu

# Governance of the Facebook Privacy Crisis

Lawrence J. Trautman

## Abstract

In November 2018, *The New York Times* ran a front-page story describing how Facebook concealed knowledge and disclosure of Russian-linked activity and exploitation resulting in Kremlin led disruption of the 2016 and 2018 U.S. elections, through the use of global hate campaigns and propaganda warfare. By mid-December 2018, it became clear that the Russian efforts leading up to the 2016 U.S. elections were much more extensive than previously thought. Two studies conducted for the United States Senate Select Committee on Intelligence (SSCI), by: (1) Oxford University's Computational Propaganda Project and Graphika; and (2) New Knowledge, provide considerable new information and analysis about the Russian Internet Research Agency (IRA) influence operations targeting American citizens.

By early 2019 it became apparent that a number of influential and successful high-growth social media platforms had been used by nation states for propaganda purposes. Over two years earlier, Russia was called out by the U.S. intelligence community for their meddling with the 2016 American presidential elections. The extent to which prominent social media platforms have been used, either willingly or without their knowledge, by foreign powers continues to be investigated as this Article goes to press. Reporting by *The New York Times* suggests that it was not until the Facebook board meeting held September 6, 2017 that board audit committee chairman, Erskin Bowles, became aware of Facebook's internal awareness of the extent to which Russian operatives had utilized the Facebook and Instagram platforms for influence campaigns in the United States. As this Article goes to press, the degree to which the allure of advertising revenues blinded Facebook to their complicit role in offering the highest bidder access to Facebook users is not yet fully known. This Article cannot be a complete chapter in the corporate governance challenge of managing, monitoring, and oversight of individual privacy issues and content integrity on prominent social media platforms. The full extent of Facebook's experience is just now becoming known, with new revelations yet to come. All interested parties: Facebook users; shareholders; the board of directors at Facebook; government regulatory agencies such as the Federal Trade Commission (FTC) and Securities and Exchange Commission (SEC); and Congress must now figure out what has transpired and what to do about it. These and other revelations have resulted in a crisis for Facebook. American democracy has been and continues to be under attack. This article contributes to the



literature by providing background and an account of what is known to date and posits recommendations for corrective action.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

# Governance of the Facebook Privacy Crisis

Lawrence J. Trautman*

Table of Contents



* BA, The American University; MBA, The George Washington University; J.D., Oklahoma City University School of Law. Mr. Trautman is Associate Professor of Business Law and Ethics at Prairie View A&M University, a seasoned corporate director and past president of the New York and Washington, D.C. chapters of the National Association of Corporate Directors (NACD). He may be contacted at Lawrence.J.Trautman@gmail.com.

The author wishes to extend particular thanks to the following for their assistance in the inspiration, research, and preparation of this article: Peter Ormerod; Elizabeth Pollman; Bernard Sharfman; Tim Trautman; Sandra Wachter; Tal Zarsky; Vincenzo Zeno-Zencovich; and Shoshana Zuboff. All errors and omissions are my own.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

## I. OVERVIEW

In November 2018, *The New York Times* ran a front-page story describing how Facebook concealed knowledge and disclosure of Russian-linked activity and exploitation resulting in Kremlin-led disruption of the 2016 U.S. elections, "broadcast [of] viral propaganda and inspir[ing] deadly campaigns of hate across the globe."[1] By mid-December 2018, it became clear that the Russian efforts leading up to the 2016 U.S. elections were much more extensive than previously thought. Two studies conducted for the United States Senate Select Committee on Intelligence (SSCI), by: (1) Oxford University's Computational Propaganda Project and Graphika,[2] and (2) New Knowledge,[3] provide considerable new information and analysis about the Russian Internet Research Agency (IRA) influence operations targeting American citizens.

By early 2019, it became apparent that a number of influential and successful high-growth social media platforms have been used by nation states for propaganda purposes. Over two years earlier, the U.S. intelligence community called out Russia for their meddling with the 2016 American presidential elections.[4] The extent to which prominent social media platforms have been used either willingly or without their knowledge by foreign powers continue to be investigated. Reporting by *The New York Times* suggests that it wasn't until the Facebook board meeting held September 6, 2017 that board audit committee chairman, Erskin Bowles, became aware of Facebook's internal awareness of the extent to which Russian operatives had used the Facebook and Instagram platforms to influence campaigns in the United States.[5] As this Article goes to press, the degree to which the allure of advertising revenues blinded Facebook to their complicit role in offering the highest bidder access to Facebook users is not yet fully known. This Article will not be a complete chapter in the corporate governance challenge of managing, monitoring, and oversight of individual privacy issues and content integrity of prominent social media platforms. The full extent of Facebook's experience is just now becoming known, with new revelations yet to come. All interested parties—Facebook users;

[1] Sheera Frenkel et al., *Delay, Deny, Deflect: How Facebook Leaders Leaned Out in Crisis*, N.Y. TIMES, Nov. 15, 2018, at A1.

[2] Philip N. Howard et al., *The IRA, Social Media and Political Polarization in the United States, 2012–2018* (U. of Oxford Computational Propaganda Res. Project, Working Paper No. 2018.2, 2018).

[3] Renee DiResta et al., *The Tactics & Tropes of the Internet Research Agency*, NEW KNOWLEDGE (2018), https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf.

[4] Elias Groll, *United States Accuses Russia of Using Hacking to Meddle in Election*, FOREIGN POLICY (Oct. 7, 2016), https://foreignpolicy.com/2016/10/07/united-states-accuses-russia-of-using-hacking-to-meddle-in-election/.

[5] *See* Frenkel et al., *supra* note 1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

shareholders; the board of directors at Facebook; government regulatory agencies such as the Federal Trade Commission (FTC) and Securities and Exchange Commission (SEC); and Congress—must now figure out what has transpired and what to do about it. These and other revelations have resulted in a crisis for Facebook, the leading global social media platform. American democracy has been and continues to be under attack. As revelations of growing concern about Facebook's systematic lax privacy practices cascaded during the first half of 2019, the author's challenge has been to constantly edit and discard text of less value. An attempt to provide a roadmap for those readers desiring a deeper dive into various topics is offered in footnotes. This manuscript contributes to the literature about national security, privacy, and social media by providing background and an account of what is known about Facebook's privacy crisis and posits recommendations for corrective action.

This Article proceeds as follows: First, is a brief description of Facebook's business. Second, an overview of the duties and responsibilities of corporate directors is presented. Third, is a description of Facebook's corporate governance scheme. Fourth, is a look at how Facebook describes perceived risk factors. Fifth, a chronology of what is now known about Facebook's privacy crisis is presented. Sixth, revelations about Facebook from the Mueller Report are explored. Seventh, depicts coverage of how Facebook's privacy crisis escalates during 2018 and 2019. Eighth, I discuss several recommendations for corrective action. Ninth, Mark Zuckerberg's strategy announcement of March 6, 2019 is presented, along with reaction and commentary from certain thought leaders. Tenth, a few observations about the current status of Facebook's privacy crisis governance is presented. Finally, a brief conclusion.

## II. THE BUSINESS OF FACEBOOK

> *Like their expanding user base, the data collected on Facebook users has also skyrocketed. They have moved on from schools, likes, and relationship status. Today, Facebook has access to dozens of data points, ranging from ads you've clicked on, events you've attended, and your location based on your mobile device.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> *It is no secret that Facebook makes money off this data through advertising revenue, although many seem confused by, or altogether unaware, of this fact. Facebook generated $40 billion in revenue in 2017, with about 98 percent coming from advertising across Facebook and Instagram.*
>
> *Senator Chuck Grassley, Chairman,*
> *Senate Judiciary Committee*
> *April 10, 2018*[6]

First, an overview of the business of Facebook, primarily as described in the company's disclosure documents is pertinent. The genesis of the social media platform that would become Facebook has become well known from the popular movie *The Social Network*,[7] based upon the bestselling book by Ben Mezrich.[8] The creation of Facebook dates back to Mark Zuckerberg's 2003 alcohol-enhanced Harvard dorm room all-nighter creation of Facemash.[9] This involved the hacking and collecting of student pictures of females from various Harvard University databases, followed with a vote "on which one was hotter—then [to be] watched as some complex algorithms calculated who were the hottest . . . on campus."[10] Facemash had gone viral across the Harvard campus: "In under two hours, the site had already logged twenty-two thousand votes."[11] Just a few months later, after navigating disciplinary action from Harvard for improper database hacking and use of student pictures, Mark Zuckerberg's efforts had produced *Thefacebook*.[12] By early 2004, *Thefacebook* was gaining traction with a management team consisting of Mark Zuckerberg (founder and CEO), Eduardo Saverin (CFO), Dustin Moskovitz (VP programming) and Chris Hughes (director of PR).[13] The entity now known as Facebook, Inc. (or, hereinafter "The Company"), was incorporated in Delaware in July 2004 and became publicly-traded by virtue of its initial public offering in May

---

[6] *Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Judiciary Comm. and S. Comm. on Comm., Sci., and Transp.*, 115th Cong. 2 (2018) (statement of Sen. Chuck Grassley, Chairman, S. Comm. on the Judiciary).

[7] THE SOCIAL NETWORK (Columbia Pictures 2010).

[8] BEN MEZRICH, THE ACCIDENTAL BILLIONAIRES: THE FOUNDING OF FACEBOOK (Anchor Books 2009).

[9] *Id. passim*.

[10] *Id.* at 56.

[11] *Id.*

[12] *Id.* at 95.

[13] *Id.* at 118.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

2012.[14] Having its principal executive offices located at 1601 Willow Road, Menlo Park, California, the Company reported 43,030 full-time employees as of November 30, 2019.[15]

***A. Business***

Describing its mission as "to give people the power to build community and bring the world closer together," according to Facebook, "[our] top priority is to build useful and engaging products that enable people to connect and share with friends and family through mobile devices, personal computers, and other surfaces."[16] In addition:

> We also help people discover and learn about what is going on in the world around them, enable people to share their opinions, ideas, photos and videos, and other activities with audiences ranging from their closest friends to the public at large, and stay connected everywhere by accessing our products, including:
>
> - ***Facebook.*** Facebook enables people to connect, share, discover, and communicate with each other on mobile devices and personal computers. There are a number of different ways to engage with people on Facebook, the most important of which is News Feed which displays an algorithmically-ranked series of stories and advertisements individualized for each person.
> - ***Instagram.*** Instagram is a community for sharing visual stories through photos, videos, and direct messages. Instagram is also a place for people to stay connected with the interests and communities that they care about.
> - ***Messenger.*** Messenger is a messaging application that makes it easy for people to connect with other people, groups and businesses across a variety of platforms and devices.
> - ***WhatsApp.*** WhatsApp is a fast, simple, and reliable messaging application that is used by people around the world to connect securely and privately.

[14] Facebook, Inc., Annual Report (Form 10-K), at 7 (Feb. 1, 2008) [hereinafter 2017 Form 10-K]; *see also* NIALL FERGUSON, THE SQUARE AND THE TOWER: NETWORKS AND POWER, FROM THE FREEMASONS TO FACEBOOK 352–59 (2018) (providing historical account of Facebook and networks development).

[15] *Company Info*, FACEBOOK, https://about.fb.com/company-info/ (last visited Nov. 15, 2019) (for employee count); Facebook, Inc., Annual Report (Form 10-K), at 7 (Jan. 31, 2019) [hereinafter 2018 Form 10-K] (for headquarters address).

[16] 2017 Form 10-K, *supra* note 14, at 5.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> - ***Oculus.*** Our Oculus virtual reality technology and content platform power products that allow people to enter a completely immersive and interactive environment to train, learn, play games, consume content, and connect with others.
>
> We generate substantially all of our revenue from selling advertising placements to marketers. Our ads enable marketers to reach people based on a variety of factors including age, gender, location, interests, and behaviors. Marketers purchase ads that can appear in multiple places including on Facebook, Instagram, Messenger, and third-party applications and websites. We are also investing in a number of longer-term initiatives, such as connectivity efforts, artificial intelligence research, and augmented and virtual reality, to develop technologies that we believe will help us better serve our communities and pursue our mission to give people the power to build community and bring the world closer together.[17]

### *B. Competition*

Facebook discloses, "[o]ur business is characterized by innovation, rapid change, and disruptive technologies. We compete with companies that sell advertising, as well as with companies that provide social, media, and communication products and services that are designed to engage users on mobile devices and online."[18] In addition:

> We face significant competition in every aspect of our business, including from companies that facilitate communication and the sharing of content and information, companies that enable marketers to display advertising, companies that distribute video and other forms of media content, and companies that provide development platforms for applications developers. We compete to attract, engage, and retain people who use our products, to attract and retain marketers, and to attract and retain developers to build compelling mobile and web applications that integrate with our product. . . .
>
> As we introduce or acquire new products, as our existing products evolve, or as other companies introduce new products and services, we may become subject to additional competition.[19]

[17] *Id.*

[18] *Id.*

[19] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

## III. GOVERNANCE: THE BASICS

> *In theory, the need for corporate governance rests on the idea that when separation exists between the ownership of a company and its management, self-interested executives have the opportunity to take actions that benefit themselves, with shareholders and stakeholders bearing the cost of these actions. This scenario is typically referred to as the* ***agency problem****, with the costs resulting from this problem described as* ***agency costs****. Executives make investment, financing, and operating decisions that better themselves at the expense of other parties related to the firm. To lessen agency costs, some type of control or monitoring system is put in place in the organization. That system of checks and balances is called* ***corporate governance****.*
>
> *David Larcker and Brian Tayan*
> *Stanford University*[20]

Lessons learned from Facebook's privacy and content manipulation provide a valuable teaching moment for all others engaged in using the Internet for marketing, or hosting user generated content on their sites. I have written elsewhere about every board's responsibility for governance during times of crisis.[21] A brief discussion regarding corporate governance; the duties of loyalty and care; business judgment rule; and Facebook's board composition follows.

### *A. Board Authority*

Legal authority for corporations is created by state-granted charters, their governance dictated by state law, with the responsibility for managing the affairs of the corporation delegated to corporate directors.[22] Delaware courts, for example, have stated that the business judgment rule is a "presumption that in making a business decision the directors of a corporation acted on an informed basis, in good

[20] DAVID LARCKER & BRIAN TAYAN, CORPORATE GOVERNANCE MATTERS 4 (FT Press 2011).

[21] *See generally* Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance*, 13 HASTINGS BUS. L.J. 275 (2017); Lawrence J. Trautman, *Who Sits on Texas Corporate Boards? Texas Corporate Directors: Who They Are and What They Do*, 16 HOUS. BUS. & TAX L.J. 44 (2016).

[22] DEL. CODE ANN. tit. 8, § 141(a) (1991) ("The business and affairs of a corporation organized under this chapter shall be managed by or under the direction of a board of directors, except as may be otherwise provided in this chapter or in its certificate of incorporation."). While more than half of all publicly owned United States corporations are chartered under the laws of the state of Delaware, corporate counsel and directors will want to closely examine the laws of relevant states when considering any particular matter; *see also* Gilson & Kraakman, *Delaware's Intermediate Standard for Defensive Tactics: Is There Substance to Proportionality Review?*, 44 BUS. LAW. 247, 248 (Feb. 1989) ("Delaware corporate law . . . governs the largest proportion of the largest business transactions in history"); Stephen M. Bainbridge, *Why a Board? Group Decisionmaking in Corporate Governance*, 55 VAND. L. REV. 1 (2002).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

faith and in the honest belief that the action taken was in the best interests of the company."[23] It is this business judgment rule, according to professor Stephen M. Bainbridge that "pervades every aspect of state corporate law."[24] Under Delaware law, directors owe their corporation and shareholders fiduciary duties of care and loyalty.[25] Discussing "The Role of Corporate Directors in Dealing with Corporate Crises" several former SEC commissioners and seasoned legal experts observe that when in crisis, "Whatever the cause, the Board is expected to act quickly and effectively to mitigate the damage to the company."[26] The foundation of corporate governance is built upon the duty of care, duty of loyalty, and duty of good faith.

***B. Duty of Loyalty***

The duty of loyalty stands for the proposition that directors, "must act in good faith and must not allow his [or her] personal interests to prevail over the interests of the corporation."[27] It is really as simple as no self-dealing.

---

[23] Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 29 J. MARSHALL J. COMPUTER & INFO. L. 313, 322 (2011), citing Unitrin, Inc. v. Am. Gen. Corp., 651 A.2d 1361, 1373 (Del. 1995) (quoting Aronson v. Lewis, 473 A.2d 75 (Del. 1992)). *See also* Robert J. Rhee, *The Tort Foundation of Duty of Care and Business Judgment*, 88 NOTRE DAME L. REV. 1139 (2013); Sean J. Griffith, *Good Faith Business Judgment: A Theory of Rhetoric in Corporate Law Jurisprudence*, 55 DUKE L.J. 1–73 (2005).

[24] Stephen M. Bainbridge, *The Business Judgment Rule as Abstention Doctrine*, 57 VAND. L. REV. 83 (2004) (citing Sinclair Oil Corp. v. Levien, 280 A.2d 717 (Del. 1971) (fiduciary duties of controlling shareholder); Shlensky v. Wrigley, 237 N.E.2d 776 (Ill. App. 1868) (operational decision)). *See also* Douglas M. Branson, *The Rule that Isn't a Rule - the Business Judgment Rule*, 36 VAL. U. L. REV. 631 (2002); Lyman Johnson, *Corporate Officers and the Business Judgment Rule*, 60 BUS. LAW. (2005); Robert Sprague & Aaron J. Lyttle, *Shareholder Primacy*, 16 STAN. J. L. BUS. & FIN. 1 (2011).

[25] Trautman & Altenbaumer-Price, *supra* note 23, at 313 (citing Smith v. Van Gorkom, 488 A.2d 858 (Del. Supr. 1985)); Stephen M. Bainbridge, Star Lopez & Benjamin Oklan, *The Convergence of Good Faith and Oversight*, 55 UCLA L. REV. 559 (2008); Julian Velasco, *How Many Fiduciary Duties Are There in Corporate Law?*, 83 S. CAL. L. REV. 1213 (2010); Bernard S. Black, *The Core Fiduciary Duties of Outside Directors*, ASIA BUS. L. REV. 3 (2001); *but see* William T. Allen, *Modern Corporate Governance and the Erosion of the Business Judgment Rule in Delaware Corporate Law*, CLPE Research Paper No. 06/2008 (Mar. 12, 2008); Stuart R. Cohn, *Demise of the Director's Duty of Care: Judicial Avoidance of Standards and Sanctions Through the Business Judgment Rule*, 62 TEX. L. REV. 591 (1983); Eric J. Pan, *Rethinking the Board's Duty to Monitor: A Critical Assessment of the Delaware Doctrine*, 38 FLA. ST. U. L. REV. 209 (2011); Bernard S. Black, Brian R. Cheffins & Michael Klausner, *Outside Director Liability*, 58 STAN. L. REV. 1055 (2006).

[26] Cynthia Glassman, Alan Beller, John Olson, Lawrence Trautman & Laura Unger, Panelists at the George Washington University School of Law Denit Trust Challenges in Corporate Governance Series: The Role of Corporate Directors in a Crisis (Oct. 21, 2013).

[27] *See* Byron F. Egan, Remarks at 37th Annual Conference on Security Regulation & Business Law in Dallas, Texas: How Recent Fiduciary Duty Cases Affect Advice to Directors and Officers of Delaware and Texas Corporations, at 7 (Feb. 13, 2015) (transcript available courtesy of Bryon F. Egan) (citing *Gearhart*, 741 F.2d at 719 n.4; Christopher M. Bruner, *The Fiduciary Enterprise of Corporate Law*, 74 WASH. & LEE L. REV. 790 (2017)); Deborah DeMott, *Corporate Officers as Agents*, 74 WASH. & LEE L. REV. 847 (2017); Asaf Eckstein & Gideon Parchomovsky, *Toward a Horizontal Fiduciary Duty in*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

### *C. Duty of Care*

A careful, diligent approach to the effective discharge of every director's individual duties and responsibilities is required to discharge the legal Duty of Care. As discussed by professors Lyman P.Q. Johnson and Mark Sides, it is the duty of care that:

> specifies the manner in which directors must discharge their legal responsibilities . . . includ[ing] electing, evaluating, and compensating corporate officers; reviewing and approving corporate strategy, budgets, and capital expenditures; monitoring internal financial information systems and financial reporting obligations, and complying with legal requirements; making distributions to shareholders; approving transactions not in the ordinary course of business; appointing members to committees and discharging committee assignments, including the important audit, compensation and nominating committees. . . .
>
> The duty of due care arises in both the discrete decision-making context *and in the oversight and monitoring areas [my emphasis added]*. . . . In the decision-making-setting—whether it involves directors making a routine business decision or responding to a high-stakes unsolicited bid for corporate control—the duty of care inquiry clearly focuses on a board's "decision-making process."[28] Directors in that setting are under an obligation to obtain and act with due care on all material information reasonably available.[29]

*Corporate Law*, 104 CORNELL L. REV. 101 (2019); JOHN C.P. GOLDBERG, THE FIDUCIARY DUTY OF CARE, THE OXFORD HANDBOOK OF FIDUCIARY LAW (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., Oxford Univ. Press 2018); Paul B. Miller, *The Identification of Fiduciary Relationships*, EVAN J. CRIDDLE, PAUL B. MILLER & ROBERT H. SITKOFF EDS., THE OXFORD HANDBOOK OF FIDUCIARY LAW (New York: Oxford University Press 2019); Dalia Tsuk Mitchell, *Status Bound: The Twentieth Century Evolution of Director's Liability*, 5 N.Y.U. J. L. & BUS. 63 (2009); Dalia Tsuk Mitchell, *The Import of History to Corporate Law*, 59 ST. LOUIS U. L.J. 683 (2015); Robert H. Sitkoff, *Other Fiduciary Duties: Implementing Loyalty and Care*, THE OXFORD HANDBOOK OF FIDUCIARY LAW (Evan J. Criddle, Paul B. Miller & Robert H. Sitkoff eds., Oxford University Press, forthcoming).

[28] Trautman & Altenbaumer-Price, *supra* note 23, at 313 (citing Lyman P.Q. Johnson & Mark A. Sides, *Corporate Governance and the Sarbanes-Oxley Act: The Sarbanes-Oxley Act and Fiduciary Duties*, 30 WM. MITCHELL L. REV. 1149, 1197 (2004) and Citron v. Fairchild Camera & Instrument Corp., 569 A.2d 53, 66 (Del. 1989)); Brehm v. Eisner, 746 A.2d 244, 264 (Del. 2000) ("Due care in the decision making context is process due care only.").

[29] Trautman & Altenbaumer-Price, *supra* note 23, at 231 (citing Paramount Communications, Inc. v. QVC Network, Inc., 637 A.2d 34, 48 (Del. 1994)). *See also* Donald C. Langevoort, *Internal Controls After Sarbanes-Oxley: Revisiting Corporate Law's Duty of Care as Responsibility for Systems*, 31 J. CORP. L. 949–73 (2006); Christopher M. Bruner, *Is the Corporate Director's Duty of Care a "Fiduciary" Duty? Does It Matter?*, 48 WAKE FOREST L. REV. 1027 (2013); William T. Allen, Jack B. Jacobs & Leo E. Strine, *Realigning the Standard of Review of Director Due Care with Delaware Public Policy: A Critique*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

The Delaware Supreme Court found in the landmark 1985 case of *Smith v. Van Gorkom*,[30] that the experienced and sophisticated directors[31] of Trans Union Corporation were not entitled to the protection of the business judgment rule[32] and had breached their fiduciary duty to their shareholders when considering acquisition of Trans Union, "(1) by their failure to inform themselves of all information reasonably available to them and relevant to their decision to recommend the Pritzker merger; and (2) by their failure to disclose all material information such as a reasonable shareholder would consider important in deciding whether to approve the Pritzker offer."[33] Absent accompanying disloyal acts, it was generally accepted that "courts had rarely found individual directors liable for breaching their duty of care," before this decision involving the Trans Union board.[34]

---

*of Van Gorkom and its Progeny as a Standard of Review Problem*, 96 NW. U. L. REV. 449 (2002); Lynn A. Stout & Margaret M. Blair, *Trust, Trustworthiness, and the Behavioral Foundations of Corporate Law*, 149 U. PA. L. REV. 1735 (2001); Robert J. Rhee, *The Tort Foundation of Duty of Care and Business Judgment*, 88 NOTRE DAME L. REV. 1139 (2013); Lucian A. Bebchuk, Joseph E. Bachelder, Roel C. Campos, Byron S. Georgiou, Alan G. Hevesi, William Lerach, Robert Mendelsohn, Robert A.G. Monks, Toby Myerson, John F. Olson, Leo E. Strine & John C. Wilcox, *Director Liability*, 31 DEL. J. CORP. L. 1011 (2006).

[30] Trautman & Altenbaumer-Price, *supra* note 23 (citing *Smith v. Van Gorkom*). *See also* Steven A. Ramirez, *The Chaos of Smith*, 45 WASHBURN L.J. 343 (2006); Stephen J. Lubben & Alana J. Darnell, *Delaware's Duty of Care*, 31 DEL. J. CORP. L. 589 (2006); Cheryl Lyn Wade, *What Independent Directors Should Expect from Inside Directors:* Smith v. Van Gorkom *as a Guide to Intra-Firm Governance*, 45 WASHBURN L.J. 367 (2006); Lawrence A. Hamermesh, *Twenty Years after* Smith v. Van Gorkom*: An Essay on the Limits of Civil Liability of Corporate Directors and the Role of Shareholder Inspection Rights*, 45 WASHBURN L.J. 283 (2006); Stephen M. Bainbridge, Smith v. Van Gorkom, Law-Econ Research Paper No. 08-13 (2008), UCLA Sch. of Law; Bernard S. Sharfman, *The Enduring Legacy of* Smith v. Van Gorkom, 33 DEL. J. CORP. L. 287 (2008); Bernard S. Sharfman, *Being Informed Does Matter: Fine Tuning Gross Negligence Twenty Plus Years after Van Gorkom*, 62 BUS. LAW. 135 (2006).

[31] Trautman & Altenbaumer-Price, *supra* note 23, at 313 (citing Peter V. Letsou, *Cases and Materials on Corporate Mergers and Acquisitions* n.21 at 643 (2006) (observing "Trans Union's five 'inside' directors had backgrounds in law and accounting, 116 years of collective employment by the company and 68 years of combined experience on its Board. Trans Union's five 'outside' directors included four chief executives of major corporations and an economist who was a former dean of a major school of business and chancellor of a university. The 'outside' directors had 78 years of combined experience as chief executive officers of major corporations and 50 years of cumulative experience of Trans Union. Thus, defendants argue that the Board was eminently qualified to reach an informed judgment on the proposed 'sale' of Trans Union notwithstanding their lack of any advance notice on the proposal, the shortness of their deliberation, and their determination not to consult with their investment banker or to obtain a fairness opinion.")

[32] Trautman & Altenbaumer-Price, *supra* note 23, at 313 (citing Smith v. Van Gorkom, 488 A.2d 858 (Del. Supr. 1985)).

[33] Letsou, *supra* note 30, at 644.

[34] Jacqueline M. Veneziani, Note & Comment: *Causation and Injury in Corporate Control Transactions:* Cede & Co. v. Technicolor, Inc., 69 WASH. L. REV. 1167, 1194 n.3 (1994) ("Before *Van Gorkom* was decided, one commentator had stated that '[t]he search for cases in which directors . . . have been held liable in derivative suits for negligence uncomplicated by self dealing is a search for a very small number of needles in a very large haystack.'"); *see also* Joseph W. Bishop, Jr., *Sitting Ducks and*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

### *D. Duty of Good Faith*

For a director to have the protection of the business judgment rule against a claim for breach of fiduciary duty, a director must be able to demonstrate that she acted in "good faith."[35] Many factors "define what it means for a corporate director to act in good faith . . . includ[ing] the judicial application of state corporate law, federal and state legislation, shareholder activism . . . corporate governance ratings, and the expectations of the public in response to the media's treatment of current issues in corporate governance."[36] *Stockbridge v. Gemini Air Cargo, Inc.*, holds that the board of directors of a Delaware corporation is charged with the legal responsibility to manage its business for the benefit of the corporation and its shareholders with "due care, good faith, and loyalty."[37] Delaware Chief Justice E. Norman Veasey observes:

> The evolving business and judicial expectations of director conduct over the years are part of the common law grist for the fiduciary duty mill. As Chancellor Allen stressed in Caremark, the kind of sustained inattention of directors exemplified by the failure to institute law compliance programs contemplated by the federal sentencing guidelines and expected of prudent businesses could be held to be a violation of fiduciary duty of good faith. That standard of conduct—good faith—is key to director conduct, and it must be considered when one looks at the directors' processes and motivations to be certain that they are honest and not disingenuous or reckless.[38]

---

*Decoy Ducks: New Trends in the Indemnification of Corporate Directors and Officers*, 77 YALE L.J. 1078, 1099 (1968).

[35] Byron Egan, *Director Duties: Process and Proof, TexasBarCLE Webcast: Corporate Minutes/Director Duties* n.45 (Oct. 23, 2008), www.jw.com/site/jsp/publicationinfo.jsp?id=1044; *see also* Leo E. Strine, Lawrence A. Hamermesh, R. Franklin Balotti & Jeffrey M. Gorris, *Loyalty's Core Demand: The Defining Role of Good Faith in Corporation Law*, 93 GEO. L.J. 629 (2010); Sean J. Griffith, *Good Faith Business Judgment: A Theory of Rhetoric in Corporate Law Jurisprudence*, 55 DUKE L.J. (2005); Melvin A. Eisenberg, *The Duty of Good Faith in Corporate Law*, 31 DEL. J. CORP. L. 1 (2005); A. Sale, *Good Faith's Procedure and Substance, in re Caremark International Inc., Derivative Litigation*, THE ICONIC CASES IN CORPORATE LAW (Macey ed., West/Thomson 2008); Christopher M. Bruner, *Good Faith, State of Mind, and the Outer Boundaries of Director Liability in Corporate Law*, 41 WAKE FOREST L. REV. 1131 (2006).

[36] Janet E. Kerr, *Developments in Corporate Governance: The Duty of Good Faith and Its Impact on Director Conduct*, 13 GEO. MASON L. REV. 1037, 1038 (2005–2006); *see also* Hillary A. Sale, *Delaware's Good Faith*, 89 CORNELL L. REV. 456 (2004).

[37] *Id.* at 1045 (citing Stockbridge v. Gemini Air Cargo, Inc., 611 S.E. 2d 600, 606 (2005) (quoting Malone v. Brincat, 722 A.2d 5, 10 (Del. 1998)).

[38] E. Norman Veasey, *Policy and Legal Overview of Best Corporate Governance Principles*, 56 SMU L. REV. 2135, 2141 (2003); *see also* Christine Hurt, *The Duty to Manage Risk*, Illinois Program in



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> *What we have learned over the past few months is alarming. We have seen how foreign actors are abusing social media platforms, like Facebook, to interfere in elections and taking millions of Americans' personal information without their knowledge to manipulate public opinion and target individual voters.*
>
> *Specifically, on February 16th [2018], Special Counsel Mueller issued an indictment against the Russia-based Internet Research Agency and thirteen of its employees for "interference operations targeting the United States."*
>
> *Senator Dianne Feinstein*
> *Ranking Member, Senate*
> *Judiciary Committee*
> *April 10, 2018*[39]

Presented below is a brief description of Facebook's board of directors, including age, position and certain biographical information.

### *A. Board Composition*

The Facebook board of directors as of March 31, 2018 consists of the following individuals:

| Name | Age | Positions |
|---|---|---|
| Mark Zuckerberg | 33 | Chairman and Chief Executive Officer |
| Sheryl K. Sandberg | 48 | Chief Operating Officer and Director |
| Marc L. Andreessen(1)(2) | 46 | Director |
| Erskine B. Bowles(1) | 72 | Director |
| Kenneth I. Chenault | 66 | Director |
| Susan D. Desmond-Hellmann*(1) | 60 | Director |
| Reed Hastings(2) | 57 | Director |
| Jan Koum | 42 | Director |
| Peter A. Thiel(2) | 50 | Director |

* Lead Independent Director
(1) Member of the audit committee

Law, Behavior and Social Science Paper No. LBSS14-09 (2013); Robert T. Miller, *Oversight Liability for Risk Management Failures at Financial Firms*, 84 S. CAL. L. REV. 47 (2011).

[39] *Facebook, Social Media Privacy, and the Use and Abuse of Data: Before the Joint Hearing of the S. Judiciary Comm. and S. Commerce Comm.*, 115th Cong. 2 (2018) (statement of Sen. Dianne Feinstein, Ranking Member, S. Comm. on the Judiciary).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

(2) Member of the compensation and governance committee

The Company discloses the following biographical information and provides a statement for each of its directors in its proxy solicitation materials provided for the annual meeting to be held on May 31, 2018:[40]

> *Mark Zuckerberg* is our founder and has served as our Chief Executive Officer (CEO) and as a member of our board of directors since July 2004. Mr. Zuckerberg has served as Chairman of our board of directors since January 2012. Mr. Zuckerberg attended Harvard University where he studied computer science. . . .
>
> *Sheryl K. Sandberg* has served as our Chief Operating Officer (COO) since March 2008 and as a member of our board of directors since June 2012. From November 2001 to March 2008, Ms. Sandberg served in various positions at Google, Inc., most recently as Vice President, Global Online Sales & Operations. Ms. Sandberg also is a former Chief of Staff of the U.S. Treasury Department and previously served as a consultant with McKinsey & Company, a management consulting company, and as an economist with The World Bank. In addition to serving as our COO, Ms. Sandberg has been a member of the board of directors of SurveyMonkey since July 2015. Ms. Sandberg previously served as a member of the boards of directors of Starbucks Corporation from March 2009 to March 2012 and the Walt Disney Company from March 2010 to March 2018. Ms. Sandberg holds an A.B. in economics from Harvard University and an M.B.A. from Harvard Business School. . . .
>
> *Marc L. Andreessen* has served as a member of our board of directors since June 2008. Mr. Andreessen is a co-founder and has been a General Partner of Andreessen Horowitz, a venture capital firm, since July 2009. Previously, Mr. Andreessen co-founded and served as the Chairman of the board of directors of Opsware, Inc. (formerly known as Loudcloud Inc.), a software company. He also served as Chief Technology Officer of America Online, Inc., an Internet services company. Mr. Andreessen was a co-founder of Netscape Communications Corporation, a software company, serving in various positions, including Chief Technology Officer and Executive Vice President of Products. In addition to serving on our board of directors, Mr. Andreessen currently serves as a member of the boards of directors of several private companies. Mr. Andreessen previously served as a member of the

[40] Facebook, Inc., Definitive Proxy Statement (Form 14A) (Apr. 13, 2018) at 10–12 [hereinafter Facebook 2018 Proxy Statement].



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

boards of directors of eBay Inc. from September 2008 to October 2014, Hewlett-Packard Company from September 2009 to October 2015, and Hewlett Packard Enterprise Company from November 2015 to April 2018. Mr. Andreessen holds a B.S. in computer science from the University of Illinois at Urbana-Champaign. . . .

*Erskine B. Bowles* has served as a member of our board of directors since September 2011. Mr. Bowles is President Emeritus of the University of North Carolina and served as President from January 2006 through December 2010. Mr. Bowles has also been a Senior Advisor and non-executive vice chairman of BDT Capital Partners, LLC, a private, investment firm, since January 2012. From February 2010 until December 2010, he served as Co-Chair of the National Commission on Fiscal Responsibility and Reform. Mr. Bowles was Managing Director of Carousel Capital LLC, a private investment firm, from 1999 to 2001, and was a Senior Advisor for the firm from 2001 to 2015. He was also a partner of Forstmann Little & Co., an investment firm, from 1999 to 2001. Mr. Bowles began his career in corporate finance at Morgan Stanley & Co. LLC and subsequently helped found and ultimately served as Chairman and Chief Executive Officer of Bowles Hollowell Connor & Co., an investment banking firm. He also was a founder of Kitty Hawk Capital, a venture capital firm. Mr. Bowles served as White House Chief of Staff from 1996 to 1998 and Deputy White House Chief of Staff from 1994 to 1995. In addition to serving on our board of directors, Mr. Bowles currently serves as a member of the board of directors of Norfolk Southern Corporation. Mr. Bowles also served as a member of the board of directors of General Motors Company from June 2005 to April 2009, Cousins Properties Incorporated from August 2003 to May 2012, Belk, Inc. from May 2011 to November 2015, and Morgan Stanley from December 2005 to February 2018. Mr. Bowles holds a B.S. in business from the University of North Carolina at Chapel Hill and an M.B.A. from Columbia University Graduate School of Business. . . .

*Kenneth I. Chenault* has served as a member of our board of directors since February 2018. Mr. Chenault has served as Chairman and a Managing Director of General Catalyst, a venture capital firm, since February 2018. Mr. Chenault previously served as Chief Executive Officer of American Express Company, a financial services company, from January 2001 to February 2018, and as Chairman of American Express Company from April 2001 to February 2018. Mr. Chenault joined American Express in 1981 as Director of Strategic Planning and served subsequently in a number of increasingly senior positions, including Vice Chairman and President and Chief Operating Officer, until his



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

appointment as Chief Executive Officer. Mr. Chenault also serves on the boards of directors of International Business Machines Corporation and The Procter & Gamble Company. Mr. Chenault holds a B.A. in history from Bowdoin College and a J.D. from Harvard Law School. . . .

*Susan D. Desmond-Hellmann* has served as a member of our board of directors since March 2013. Dr. Desmond-Hellmann has served as the Chief Executive Officer of the Bill & Melinda Gates Foundation since May 2014. Prior to the Bill & Melinda Gates Foundation, Dr. Desmond-Hellmann was the Chancellor at University of California, San Francisco (UCSF) from August 2009 to May 2014. From 2004 through 2009, Dr. Desmond-Hellmann served as President of Product Development at Genentech, where she was responsible for pre-clinical and clinical development, business development, and product portfolio management. She joined Genentech in 1995. Prior to joining Genentech, Dr. Desmond-Hellmann was associate director of clinical cancer research at Bristol-Myers Squibb Pharmaceutical Research Institute. In addition to serving on our board of directors, Dr. Desmond-Hellmann previously served as a member of the board of directors of The Procter & Gamble Company from December 2010 until October 2016. Dr. Desmond-Hellmann holds a B.S. in pre-med and an M.D. from the University of Nevada, Reno, and an M.P.H. from the University of California, Berkeley. . . .

*Reed Hastings* has served as a member of our board of directors since June 2011. Mr. Hastings has served as the Chief Executive Officer and Chairman of the board of directors of Netflix, Inc., a provider of an Internet subscription service for movies and television shows, since 1999. Prior to Netflix, Mr. Hastings served as Chief Executive Officer of Technology Network, a political service organization for the technology industry. Mr. Hastings served as Chief Executive Officer of Pure Atria Software, a maker of software development tools, from 1991 until it was acquired by Rational Software Corporation in 1997. Mr. Hastings previously served as a member of the board of directors of Microsoft Corporation from March 2007 to November 2012. Mr. Hastings holds a B.A. in mathematics from Bowdoin College and an M.S.C.S. in computer science from Stanford University. . . .

*Jan Koum* has served as a member of our board of directors since October 2014. Since February 2009, Mr. Koum has served and continues to serve as co-founder and Chief Executive Officer of WhatsApp Inc. (WhatsApp), a cross-platform mobile messaging



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> application company and our wholly-owned subsidiary. Mr. Koum attended San Jose State University where he studied math and computer science. Mr. Koum left San Jose State University before achieving a degree. . . .
>
> *Peter A. Thiel* has served as a member of our board of directors since April 2005. Mr. Thiel has served as President of Thiel Capital, an investment firm, since 2011 and a Partner of Founders Fund, a venture capital firm, since 2005. In 1998, Mr. Thiel co-founded PayPal, Inc., an online payment company, where he served as Chief Executive Officer, President, and Chairman of its board of directors from 2000 until its acquisition by eBay in 2002. Mr. Thiel holds a B.A. in philosophy from Stanford University and a J.D. from Stanford Law School. . . .[41]

### *B. Board Leadership Structure and Controlled-Company Status*

Facebook provides the following description of its board leadership structure in its proxy materials for to their meeting of shareholders to be held May 31, 2018:

> Mark Zuckerberg, our founder and CEO, serves as Chairman of our board of directors, presides over meetings of the board of directors, and holds such other powers and carries out such other duties as are customarily carried out by the Chairman of our board of directors. Mr. Zuckerberg brings valuable insight to our board of directors due to the perspective and experience he brings as our founder and CEO, and as our largest and controlling stockholder. Dr. Desmond-Hellmann currently serves as our Lead Independent Director and presides over portions of regularly scheduled meetings at which only our independent directors are present, serves as a liaison between the Chairman and the independent directors, and performs such additional duties as the board of directors may otherwise determine and delegate. Generally, each regular meeting of our board of directors includes a meeting of our independent directors without management present.
>
> ***Controlled Company Status***
>
> Because Mr. Zuckerberg controls a majority of our outstanding voting power, we are a "controlled company" under the corporate governance rules of The Nasdaq Stock Market LLC (Nasdaq). Therefore, we are not required to have a majority of our board of directors be independent, nor are we required to have a compensation committee or an independent nominating function. In light of our status as a controlled company, our board of

[41] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> directors has determined not to have an independent nominating function and to have the full board of directors be directly responsible for nominating members of our board.[42]

***C. Director Independence***

The Company provides the following disclosures regarding director independence in its proxy materials for their meeting of shareholders to be held May 31, 2018:

> The rules of Nasdaq generally require that a majority of the members of a listed company's board of directors be independent. In addition, the Nasdaq rules generally require that, subject to specified exceptions, each member of a listed company's audit, compensation, and governance committees be independent. Although we are a "controlled company" under the corporate governance rules of Nasdaq and, therefore, are not required to comply with certain rules requiring director independence, we have nevertheless opted, under our corporate governance guidelines, to have a majority of the members of our board of directors be independent.
>
> Audit committee members must also satisfy the independence criteria set forth in Rule 10A-3 under the Securities Exchange Act of 1934, as amended (Exchange Act). In order to be considered independent for purposes of Rule 10A-3, a member of an audit committee of a listed company may not, other than in his or her capacity as a member of the audit committee, the board of directors, or any other board committee: accept, directly or indirectly, any consulting, advisory, or other compensatory fee from the listed company or any of its subsidiaries; or be an affiliated person of the listed company or any of its subsidiaries.
>
> [The Facebook] board of directors has determined that none of our non-employee directors has a relationship that would interfere with the exercise of independent judgment in carrying out the responsibilities of a director and that each of these directors is "independent" as that term is defined under the rules of Nasdaq. Our board of directors has also determined that Messrs. Andreessen and Bowles, and Dr. Desmond-Hellmann, who comprise our audit committee, and Messrs. Andreessen, Hastings, and Thiel, who comprise our compensation & governance committee, satisfy the independence standards for those

[42] *Id.* at 13.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

committees established by applicable SEC rules and Nasdaq rules.[43]

***D. Committee Structure***

Boards of directors organize their work through committees.[44] Facebook discloses that the board "has established an audit committee and a compensation and governance committee, each of which have the composition and responsibilities described below. Members serve on these committees until their resignations or until otherwise determined by our board of directors. Each of these committees has a written charter."[45]

***E. Audit Committee***

In its proxy materials for their meeting of shareholders to be held May 31, 2018, Facebook provides the following description of its audit committee:

> Our audit committee is comprised of Messrs. Andreessen and Bowles, and Dr. Desmond-Hellmann. Mr. Bowles is the chairman of our audit committee, is our audit committee financial expert, as that term is defined under SEC rules, and possesses financial sophistication as defined under the rules of Nasdaq. The designation does not impose on Mr. Bowles any duties, obligations or liabilities that are greater than are generally imposed on members of our audit committee and our board of directors. Our board of directors has adopted a charter for our audit committee. As more fully described in its charter, our audit committee is directly responsible for, among other things:
>
> - selecting the independent registered public accounting firm to audit our financial statements;
> - ensuring the independence of the registered public accounting firm;
> - discussing the scope and results of the audit with the independent registered public accounting firm, and reviewing, with management and that firm, our interim and year-end operating results;
> - developing procedures to enable submission of anonymous concerns about accounting or auditing matters;

[43] *Id.*

[44] Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment*, 11 FLA. ST. U. BUS. REV. 75 (2012).

[45] Facebook 2018 Proxy Statement, *supra* note 40, at 14.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

- considering the adequacy of our internal accounting controls and audit procedures;
- reviewing related party transactions;
- reviewing our program for promoting and monitoring compliance with applicable legal and regulatory requirements;
- reviewing our legal, financial, and enterprise risk exposures, and the steps management has taken to monitor and control such exposures;
- pre-approving all audit and non-audit services to be performed by the independent registered public accounting firm; and
- overseeing our internal audit function.

During 2017, the audit committee met in person or by telephone or videoconference, or acted by unanimous written consent, ten times.[46]

### *F. Compensation and Governance Committee*

A comprehensive discussion of Facebook's compensation governance and compensation-setting process is beyond the scope and not this focus of this single journal article. Nevertheless, Facebook provides the following description of its compensation and governance committee in its proxy materials for their meeting of shareholders to be held May 31, 2018:

> Our compensation & governance committee is comprised of Messrs. Andreessen, Hastings, and Thiel. Mr. Hastings is the chairman of our compensation & governance committee. Each member of this committee is a non-employee director, as defined pursuant to Rule 16b-3 promulgated under the Exchange Act, and an outside director, as defined under Section 162(m) of the Internal Revenue Code of 1986, as amended. Our board of directors has adopted a charter for our compensation & governance committee. As more fully described in its charter, our compensation & governance committee is responsible for, among other things:
>
> - evaluating the performance of our executive officers;
> - evaluating, recommending, approving and reviewing executive officer compensation

[46] Facebook 2018 Proxy Statement, *supra* note 40, at 14–15; *see also* Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?*, 11 DEPAUL BUS. & COM. L.J. 205 (2013); Lawrence J. Trautman, Jason Triche & James C. Wetherbe, *Corporate Information Technology Governance Under Fire*, 8 J. STRAT. & INT'L STUD. 105 (2013).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

arrangements, plans, policies and programs maintained by us;

- administering our equity-based compensation plans and our annual bonus plan;
- considering and making recommendations regarding non-employee director compensation;
- considering and making recommendations to our board of directors regarding its remaining responsibilities relating to executive compensation;
- monitoring succession planning for certain of our key executives;
- developing and recommending corporate governance guidelines and policies;
- overseeing the evaluation process for our board of directors and committees thereof;
- reviewing and granting proposed waivers of the code of conduct for executive officers; and
- advising our board of directors on corporate governance matters and board of director performance matters, including recommendations regarding the structure and composition of our board of directors and committees thereof.[47]

## V. RISK FACTORS

> *Something is awry. It is true that many capitalists, including surveillance capitalists, vigorously employ these century-old justifications for their freedom when they reject regulatory, legislative, judicial, societal, or any other form of public interference in their methods of operation.*
>
> *Soshana Zuboff*
> *The Charles Edward Wilson*
> *Professor Emerita*
> *Harvard Business School*
> *2019*[48]

In its proxy materials for their meeting of shareholders to be held May 31, 2018, the Company provides the following introductory discussion about the board's role in risk oversight:

[47] Facebook 2018 Proxy Statement, *supra* note 40, at 15.

[48] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 497 (2019).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> Our board of directors as a whole has responsibility for overseeing our risk management and believes that a thorough and strategic approach to risk oversight is critical. The board of directors exercises this oversight responsibility directly and through its committees. The oversight responsibility of the board of directors and its committees is informed by regular reports from our management team, including senior personnel that lead a variety of functions across the business, and from our internal audit department, as well as input from external advisors, as appropriate. These reports are designed to provide timely visibility to the board of directors and its committees about the identification and assessment of key risks, our risk mitigation strategies, and ongoing developments.
>
> The full board of directors has primary responsibility for evaluating strategic and operational risk management, and for CEO succession planning. Our audit committee has the responsibility for overseeing our major financial, legal, and regulatory risk exposures, which span a variety of areas including litigation, regulatory compliance, reputational and policy matters, platform integrity efforts, financial reporting, cybersecurity, and international operations. Our audit committee also oversees the steps our management has taken to monitor and control these exposures, including policies and procedures for assessing and managing risk and related compliance efforts. Finally, our audit committee oversees our internal audit function. Our compensation & governance committee evaluates risks arising from our corporate governance and compensation policies and practices. . . .[49]

A discussion of all risk factors identified by Facebook as material or having the potential to become material is beyond the scope of this Article. Nevertheless, a number of these factors that are most significant to the Company or of particular importance to the discussion of privacy issues are presented below. Factors dealing with issues such as tax liabilities, capital structure, reliance on key employees, or changes in accounting practices are ignored for purposes of this assessment but may be found in the source documents.

[49] Facebook 2018 Proxy Statement, *supra* note 40, at 16.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

### *A. Business and Industry Related Risks*

Facebook lists a large number of risk factors that "may have a material adverse effect on our business, financial condition, and results of operations."[50] This list of risk factors and uncertainties is not exhaustive and the Company discloses that "additional risks and uncertainties that we are aware of, or that we currently believe are not material, may also become important factors that adversely affect our business."[51] Setting aside risk factors related to items such as, tax liabilities, capital structure, reliance on key employees, some of the Company's primary perceived risk factors include:

1. If we fail to retain existing users or add new users, or if our users decrease their level of engagement with our products, our revenue, financial results, and business may be significantly harmed.
2. We generate substantially all of our revenue from advertising. The loss of marketers, or reduction in spending by marketers, could seriously harm our business.
3. Our user growth, engagement, and monetization on mobile devices depend upon effective operation with mobile operating systems, networks, and standards that we do not control.
4. Our business is highly competitive. Competition presents an ongoing threat to the success of our business.
5. Action by governments to restrict access to Facebook or our other products in their countries could substantially harm our business and financial results.
6. Our new products and changes to existing products could fail to attract or retain users or generate revenue and profits.
7. We make product and investment decisions that may not prioritize short-term financial results and may not produce the long-term benefits that we expect.
8. If we are not able to maintain and enhance our brands, or if events occur that damage our reputation and brands, our ability to expand our base of users, marketers, and developers may be impaired, and our business and financial results may be harmed.

---

[50] 2017 Form 10-K, *supra* note 14, at 8. *See also* Lawrence J. Trautman & Kara Altenbaumer-Price, *D&O Insurance: A Primer*, 1 AM. U. BUS. L. REV. 337 (2012) (for discussion of insurance in mitigating corporate risk).

[51] 2017 Form 10-K, *supra* note 14, at 8.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

9. Security breaches and improper access to or disclosure of our data or user data, or other hacking and phishing attacks on our systems, could harm our reputation and adversely affect our business.
10. Unfavorable media coverage could negatively affect our business.
11. Our financial results will fluctuate from quarter to quarter and are difficult to predict.
12. We expect our rates of growth to decline in the future.
13. Our costs are continuing to grow, which could reduce our operating margin and profitability. If our investments are not successful, our business and financial performance could be harmed.
14. Given our levels of share-based compensation, our tax rate may vary significantly depending on our stock price.
15. Our business is subject to complex and evolving U.S. and foreign laws and regulations regarding privacy, data protection, content, competition, consumer protection, and other matters. Many of these laws and regulations are subject to change and uncertain interpretation, and could result in claims, changes to our business practices, monetary penalties, increased cost of operations, or declines in user growth or engagement, or otherwise harm our business.
16. We have been subject to regulatory and other government investigations, enforcement actions, and settlements, and we expect to continue to be subject to such proceedings and other inquires in the future, which could cause us to incur substantial costs or require us to change our business practices in a manner materially adverse to our business.
17. We are currently, and expect to be in the future, party to patent lawsuits and other intellectual property rights claims that are expensive and time consuming and, if resolved adversely, could have a significant impact on our business, financial condition, or results of operations.
18. We are involved in numerous class action lawsuits and other litigation matters that are expensive and time consuming, and, if resolved adversely, could harm our business, financial condition, or results of operations.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

19. We may incur liability as a result of information retrieved from or transmitted over the Internet or published using our products or as a result of claims related to our products.
20. Our CEO has control over key decision making as a result of his control of a majority of the voting power of our outstanding capital stock.
21. We plan to continue to make acquisitions, which could harm our financial condition or results of operations and may adversely affect the price of our common stock.
22. We may not be able to successfully integrate our acquisitions, and we may incur significant costs to integrate and support the companies we acquire.
23. If our goodwill or finite-lived intangible assets become impaired, we may be required to record a significant charge to earnings.
24. Our business is dependent on our ability to maintain and scale our technical infrastructure, and any significant disruption in our service could damage our reputation, result in a potential loss of users and engagement, and adversely affect our financial results.
25. We could experience unforeseen difficulties in building and operating key portions of our technical infrastructure.
26. Our products and internal systems rely on software that is highly technical, and if it contains undetected errors or vulnerabilities, our business could be adversely affected.
27. Technologies have been developed that can block the display of our ads, which could adversely affect our financial results.
28. Real or perceived inaccuracies in our user and other metrics may harm our reputation and negatively affect our business.
29. We cannot assure you that we will effectively manage our growth.
30. The loss of one or more of our key personnel, or our failure to attract and retain other highly qualified personnel in the future, could harm our business.
31. We may not be able to continue to successfully grow usage of and engagement with mobile and web applications that integrate with Facebook and our other products.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

32. We currently generate substantially all of our Payments revenue from developers that use Facebook on personal computers, and we expect that our Payments revenue will continue to decline as usage of Facebook on personal computers continues to decline.

33. Payment transactions may subject us to additional regulatory requirements and other risks that could be costly and difficult to comply with or that could harm our business.

34. We have significant international operations and plan to continue expanding our operations abroad where we have more limited operating experience, and this may subject us to increased business and economic risks that could affect our financial results.

35. We face design, manufacturing, and supply chain risks that, if not properly managed, could adversely impact our financial results.

36. We may face inventory risk with respect to our Oculus products.[52]

***B. Failure to Retain Existing Users or Add New Users***

Facebook recognizes that the failure "to retain existing users or add new users, or if our users decrease their level of engagement with our products, our revenue, financial results, and business may be significantly harmed." The Company discloses:

> The size of our user base and our users' level of engagement are critical to our success. Our financial performance has been and will continue to be significantly determined by our success in adding, retaining, and engaging active users of our products, particularly for Facebook and Instagram. We anticipate that our active user growth rate will continue to decline over time as the size of our active user base increases, and it is possible that the size of our active user base may fluctuate or decline in one or more markets, particularly in markets where we have achieved higher penetration rates. . . .
>
> If we are unable to maintain or increase our user base and user engagement, our revenue and financial results may be adversely affected. Any decrease in user retention, growth, or engagement could render our products less attractive to users, marketers, and

[52] 2017 Form 10-K, *supra* note 14, at 8–24. *See also* Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-commerce, Political and Regulatory Compliance Risks*, 10 WM. & MARY BUS. L. REV. 1 (2018) (for discussion of risk perception by Google, Facebook's major competitor in behavioral surplus).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> developers, which is likely to have a material and adverse impact on our revenue, business, financial condition, and results of operations. If our active user growth rate continues to slow, we will become increasingly dependent on our ability to maintain or increase levels of user engagement and monetization in order to drive revenue growth.[53]

### *C. Material Decline in Advertising Revenue*

The lure of advertising revenue is central to any understanding of Facebook's complicit involvement with issues of "fake news"; whether the Company knowingly or should have known of Russian or other foreign or domestic agents improperly seeking to influence the 2016 U.S. elections through illegal advertising on any of the Facebook platforms or, issues involving the compromising of individual privacy for advertising revenues. In the case of Facebook, "following the money" means following the advertising revenues. Materially all Facebook revenue:

> Substantially all of our revenue is currently generated from third parties advertising on Facebook and Instagram. For 2017, 2016, and 2015, advertising accounted for 98%, 97% and 95%, respectively, of our revenue. As is common in the industry, our marketers do not have long-term advertising commitments with us. Many of our marketers spend only a relatively small portion of their overall advertising budget with us. Marketers will not continue to do business with us, or they will reduce the budgets they are willing to commit to us, if we do not deliver ads in an effective manner, or if they do not believe that their investment in advertising with us will generate a competitive return relative to other alternatives. In addition, our advertising revenue growth has become increasingly dependent upon increased pricing of our ads. If we are unable to provide marketers with a suitable return on investment, the pricing of our ads may not increase, or may decline, in which case our revenue and financial results may be harmed.
>
> Our advertising revenue could also be adversely affected by a number of other factors, including:
>
> - decreases in user engagement, including time spent on our products;
> - our inability to continue to increase user access to and engagement with our mobile products;
> - product changes or inventory management decisions we may make that change the size, format, frequency, or relative prominence of ads

[53] 2017 Form 10-K, *supra* note 14, at 8–9.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

displayed on our products or of other unpaid content shared by marketers on our products;

- our inability to maintain or increase marketer demand, the pricing of our ads, or both;
- our inability to maintain or increase the quantity or quality of ads shown to users, including as a result of technical infrastructure constraints;
- reductions of advertising by marketers due to our efforts to implement advertising policies that protect the security and integrity of our platform;
- changes to third-party policies that limit our ability to deliver or target advertising on mobile devices;
- the availability, accuracy, and utility of analytics and measurement solutions offered by us or third parties that demonstrate the value of our ads to marketers, or our ability to further improve such tools;
- loss of advertising market share to our competitors, including if prices for purchasing ads increase or if competitors offer lower priced or more integrated products;
- adverse government actions or legal developments relating to advertising, including legislative and regulatory developments and developments in litigation;
- decisions by marketers to reduce their advertising as a result of adverse media reports or other negative publicity involving us, our advertising metrics or tools, content on our products, developers with mobile and web applications that are integrated with our products, or other companies in our industry;
- reductions of advertising by marketers due to objectionable content published on our products by third parties;
- the effectiveness of our ad targeting or degree to which users opt out of certain types of ad targeting, including as a result of product changes and controls that may be implemented in connection with the GDPR or other regulation or regulatory action;
- the degree to which users cease or reduce the number of times they engage with our ads;
- changes in the way advertising on mobile devices or on personal computers is measured or priced; and



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

- the impact of macroeconomic conditions, whether in the advertising industry in general, or among specific types of marketers or within particular geographies.

The occurrence of any of these or other factors could result in a reduction in demand for our ads, which may reduce the prices we receive for our ads, or cause marketers to stop advertising with us altogether, either of which would negatively affect our revenue and financial results.[54]

### *D. Dependence Upon Mobile Operating Systems, Networks & Standards*

According to Facebook, "Our user growth, engagement, and monetization on mobile devices depend upon effective operation with mobile operating systems, networks, and standards that we do not control."[55] In addition:

> The substantial majority of our revenue is generated from advertising on mobile devices. There is no guarantee that popular mobile devices will continue to feature Facebook or our other products, or that mobile device users will continue to use our products rather than competing products. We are dependent on the interoperability of Facebook and our other products with popular mobile operating systems, networks, and standards that we do not control, such as the Android and iOS operating systems. Any changes, bugs, or technical issues in such systems, or changes in our relationships with mobile operating system partners, handset manufacturers, or mobile carriers, or in their terms of service or policies that degrade our products' functionality, reduce or eliminate our ability to distribute our products, give preferential treatment to competitive products, limit our ability to deliver, target, or measure the effectiveness of ads, or charge fees related to the distribution of our products or our delivery of ads could adversely affect the usage of Facebook or our other products and monetization on mobile devices.[56]

### *E. Competition*

Facebook warns that "our business is highly competitive. Competition presents an ongoing threat to the success of our business."[57] As to details:

> We compete with companies that sell advertising, as well as with companies that provide social, media, and

[54] *Id.* at 9–10.

[55] *Id.* at 10.

[56] *Id.*

[57] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

communication products and services that are designed to engage users on mobile devices and online. We face significant competition in every aspect of our business, including from companies that facilitate communication and the sharing of content and information, companies that enable marketers to display advertising, companies that distribute video and other forms of media content, and companies that provide development platforms for applications developers. We compete with companies that offer products across broad platforms that replicate capabilities we provide. . . .

We believe that our ability to compete effectively depends upon many factors both within and beyond our control, including:

- the popularity, usefulness, ease of use, performance, and reliability of our products compared to our competitors' products;
- the size and composition of our user base;
- the engagement of users with our products and competing products;
- the timing and market acceptance of products, including developments and enhancements to our or our competitors' products;
- our ability to distribute our products to new and existing users;
- our ability to monetize our products;
- the frequency, size, format, quality, and relative prominence of the ads displayed by us or our competitors;
- customer service and support efforts;
- marketing and selling efforts, including our ability to measure the effectiveness of our ads and to provide marketers with a compelling return on their investments;
- our ability to establish and maintain developers' interest in building mobile and web applications that integrate with Facebook and our other products;
- our ability to establish and maintain publisher interest in integrating their content with Facebook and our other products;
- changes mandated by legislation, regulatory authorities, or litigation, some of which may have a disproportionate effect on us;



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> - acquisitions or consolidation within our industry, which may result in more formidable competitors;
> - our ability to attract, retain, and motivate talented employees, particularly software engineers, designers, and product managers;
> - our ability to cost-effectively manage and grow our operations; and
> - our reputation and brand strength relative to those of our competitors.
>
> If we are not able to compete effectively, our user base and level of user engagement may decrease, we may become less attractive to developers and marketers, and our revenue and results of operations may be materially and adversely affected.[58]

### *F. Government Restrictions*

The Company observes, "Action by governments to restrict access to Facebook of our other products in their countries could substantially harm our business and financial results."[59] For example:

> It is possible that governments of one or more countries may seek to censor content available on Facebook or our other products in their country, restrict access to our products from their country entirely, or impose other restrictions that may affect the accessibility of our products in their country for an extended period of time or indefinitely. For example, user access to Facebook and certain of our other products has been or is currently restricted in whole or in part in China, Iran, and North Korea. In addition, government authorities in other countries may seek to restrict user access to our products if they consider us to be in violation of their laws or a threat to public safety or for other reasons, and certain of our products have been restricted by governments in other countries from time to time. It is also possible that government authorities could take action to restrict our ability to sell advertising. In the event that content shown on Facebook or our other products is subject to censorship, access to our products is restricted, in whole or in part, in one or more countries.[60]

---

[58] *Id.* at 10.

[59] *Id.* at 13.

[60] 2017 Form 10-K, *supra* note 14, at 13; *see also* Lawrence J. Trautman, *American Entrepreneur in China: Potholes on the Silk Road to Prosperity*, 12 WAKE FOREST J. BUS. & INTELL. PROP. L. 427 (2012).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

### *G. New Products*

Facebook states, "Our new products and changes to existing products could fail to attract or retain users or generate revenue and products."[61] Accordingly:

> Our ability to retain, increase, and engage our user base and to increase our revenue depends heavily on our ability to continue to evolve our existing products and to create successful new products, both independently and in conjunction with developers or other third parties. We may introduce significant changes to our existing products or acquire or introduce new and unproven products, including using technologies with which we have little or no prior development or operating experience. . . . We have also invested, and expect to continue to invest, significant resources in growing our WhatsApp and Messenger products.[62]

### *H. Product and Investment Decisions and Financial Results*

With a focus toward disruptive technological products, Facebook observes, "We make product and investment decisions that may not prioritize short-term financial results and may not produce the long-term benefits that we expect."[63] According to Facebook:

> We frequently make product and investment decisions that may not prioritize short-term financial results if we believe that the decisions are consistent with our mission and benefit the aggregate user experience and will thereby improve our financial performance over the long term. For example, from time to time we may change the size, frequency, or relative prominence of ads in order to improve ad quality and overall user experience. . . . From time to time, we have also made, and expect to continue to make, other changes to our products which may adversely affect the distribution of content of publishers, marketers, and developers, and could reduce their incentive to invest in their efforts on Facebook. . . . In addition, we plan to continue focusing on growing users and engagement on Instagram, Messenger, and WhatsApp, and we may also introduce other stand-alone applications in the future. These efforts may reduce engagement with the core Facebook application, where we have the most proven means of monetization and which serves as the platform for many of our new user

[61] 2017 Form 10-K, *supra* note 14, at 13.

[62] *Id.*

[63] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> experiences. These decisions may adversely affect our business and results of operations and may not produce the long-term benefits that we expect.[64]

***I. Reputation and Brands***

Facebook warns, "If we are not able to maintain and enhance our brands, or if events occur that damage our reputation and brands, our ability to expand our base of users, marketers, and developers may be impaired, and our business and financial results may be harmed."[65] The Company continues:

> We believe that our brands have significantly contributed to the success of our business. We also believe that maintaining and enhancing our brands is critical to expanding our base of users, marketers, and developers. Many of our new users are referred by existing users. Maintaining and enhancing our brands will depend largely on our ability to continue to provide useful, reliable, trustworthy, and innovative products, which we may not do successfully. . . . We will also continue to experience media, legislative, or regulatory scrutiny of our decisions regarding user privacy, content, advertising, and other issues, which may adversely affect our reputation and brands. For example, we previously announced our discovery of certain ads and other content previously displayed on our products that may be relevant to government investigations relating to Russian interference in the 2016 U.S. presidential election. We also may fail to respond expeditiously to the sharing of objectionable content on our services or objectionable practices by advertisers, or to otherwise address user concerns, which could erode confidence in our brands. Our brands may also be negatively affected by the actions of users that are deemed to be hostile or inappropriate to other users, by the actions of users acting under false or inauthentic identities, by the use of our products or services to disseminate information that is deemed to be misleading (or intended to manipulate opinions), by perceived or actual efforts by governments to obtain access to user information for security-related purposes or to censor certain content on our platform, or by the use of our products or services for illicit, objectionable, or illegal ends. Maintaining and enhancing our brands may require us to make substantial investments and these investments may not be successful. Certain of our past actions have eroded confidence in our brands, and if we fail to

[64] *Id.* at 14.

[65] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> successfully promote and maintain our brands or if we incur excessive expenses in this effort, our business and financial results may be adversely affected.[66]

### *J. Security Breaches, Hacking, and Phishing Attacks*

Relevant to the inquiry into privacy issues and Russian meddling into the 2016 and 2018 U.S. elections, Facebook warns, "Security breaches and improper access to or disclosure of our data or users data, or other hacking and phishing attacks on our systems, could harm our reputation and adversely affect our business."[67] Accordingly:

> Our industry is prone to cyber-attacks by third parties seeking unauthorized access to our data or users' data or to disrupt our ability to provide service. Any failure to prevent or mitigate security breaches and improper access to or disclosure of our data or user data, including personal information, content or payment information from users, could result in the loss or misuse of such data, which could harm our business and reputation and diminish our competitive position. In addition, computer malware, viruses, social engineering (predominantly spear phishing attacks), and general hacking have become more prevalent in our industry, have occurred on our systems in the past, and will occur on our systems in the future. We also regularly encounter attempts to create false or undesirable user accounts, purchase ads, or take other actions on our platform for purposes such as spamming, spreading misinformation, or other objectionable ends. As a result of our prominence, the size of our user base, and the types and volume of personal data on our systems, we believe that we are a particularly attractive target for such breaches and attacks. Such attacks may cause interruptions to the services we provide, degrade the user experience, cause users to lose confidence and trust in our products, impair our internal systems, or result in financial harm to us. . . . Cyber-attacks continue to evolve in sophistication and volume, and inherently may be difficult to detect for long periods of time. Although we have developed systems and

---

[66] 2017 Form 10-K, *supra* note 14, at 1. *See also* Lawrence J. Trautman et al., Beginning to Think About Ethics and Values in an Age of Rapid Technological Change (Aug. 21, 2018) (discussing social media ethical issues).

[67] 2017 Form 10-K, *supra* note 14, at 14; *see also* Lawrence J. Trautman & Peter C. Ormerod, *WannaCry, Ransomware, and the Emerging Threat to Corporations*, 86(2) TENN. L. REV. 503 (2019); Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761 (2018); Lawrence J. Trautman, *Managing Cyberthreat*, 33(2) SANTA CLARA HIGH TECH. L.J. 230 (2017); Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?*, 18 N.C. J.L. & TECH. 232 (2016); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?*, 2015 U. ILL. J.L. TECH. & POL'Y 341 (2015); David D. Schein & Lawrence J. Trautman, *The Dark Web and Employer Liability*, 18(1) COLO. TECH. L.J. 1 (2019).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> processes that are designed to protect our data and user data, to prevent data loss, to disable undesirable accounts and activities on our platform, and to prevent or detect security breaches, we cannot assure you that such measures will provide absolute security, and we may incur significant costs in protecting against or remediating cyber-attacks.
>
> In addition, some of our developers or other partners, such as those that help us measure the effectiveness of ads, may receive or store information provided by us or by our users through mobile or web applications integrated with Facebook. . . .
>
> Affected users or government authorities could initiate legal or regulatory actions against us in connection with any security breaches or improper disclosure of data, which could cause us to incur significant expense and liability or result in orders or consent decrees forcing us to modify our business practices. Such incidents may also result in a decline in our active user base or engagement levels. Any of these events could have a material and adverse effect on our business, reputation, or financial results.[68]

### *K. Impact of Unfavorable Media Coverage*

Facebook highlights as a risk factor that "Unfavorable media coverage could negatively affect our business,"[69] as we will see demonstrated in (*Infra* §§ VI and VIII). Accordingly:

> We receive a high degree of media coverage around the world. Unfavorable publicity regarding, for example, our privacy practices, terms of service, product changes, product quality, litigation or regulatory activity, government surveillance, the actions of our advertisers, the actions of our developers whose products are integrated with our products, the use of our products or services for illicit, objectionable, or illegal ends, the actions of our users, the quality and integrity of content shared on our platform, or the actions of other companies that provide similar services to us, has in the past, and could in the future, adversely affect our reputation. Such negative publicity also could have an adverse effect on the size, engagement, and loyalty of our user base and result

[68] 2017 Form 10-K, *supra* note 14, at 14.

[69] *Id.* at 15.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> in decreased revenue, which could adversely affect our business and financial results.[70]

***L. Financial Results Fluctuate***

The Company devotes considerable language to the various reasons accounting for difficult to predict quarter-to-quarter fluctuations in financial results.[71] Space limitations require that I omit an additional comment on this topic.

***M. Decline Expected in Future Growth Rate***

Facebook discloses, "We expect our rates of growth to decline in the future."[72] Much like the natural laws involving Earth's gravity:

> We expect that our user growth and revenue growth rates will decline over time as the size of our active user base increases, and it is possible that the size of our active user base may fluctuate or decline in one or more markets, particularly as we achieve greater market penetration. We expect our revenue growth rate will generally decline over time as our revenue increases to higher levels. As our growth rates decline, investors' perceptions of our business may be adversely affected. . . .[73]

***N. Costs Continuing to Grow***

The Company reports, "Our costs are continuing to grow, which could reduce our operating margin and profitability. If our investments are not successful, our business and financial performance could be harmed."[74] Accordingly:

> Operating our business is costly, and we expect our expenses to continue to increase in the future as we broaden our user base, as users increase the amount and types of content they consume and the data they share with us, for example with respect to video, as we develop and implement new products, as we continue to expand our technical infrastructure, as we continue to invest in new and unproven technologies, and as we continue to hire additional employees to support our expanding operations. We will continue to invest in our messaging, security, video content, and global connectivity efforts, as well as other initiatives that may not have clear paths to monetization. . . . In addition, if our investments are not

[70] *Id.*

[71] *Id.*

[72] *Id.* at 17.

[73] *Id.*

[74] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> successful, our ability to grow revenue will be harmed, which could adversely affect our business and financial performance.[75]

### *O. Laws and Regulations*

According to Facebook, "Our business is subject to complex and evolving U.S. and foreign laws regarding privacy, data protection, content, competition, consumer protection, and other matters."[76] In addition, "many of these laws and regulations are subject to change and uncertain interpretation, and could result in claims, changes to our business practices, monetary penalties, increased cost of operations, or declines in user growth or engagement, or otherwise harm our business."[77] For example:

> We are subject to a variety of laws and regulations in the United States and abroad that involve matters central to our business, including privacy, data protection and personal information, rights of publicity, content, intellectual property, advertising, marketing, distribution, data security, data retention and deletion, electronic contracts and other communications, competition, protection of minors, consumer protection, telecommunications, product liability, taxation, economic or other trade prohibitions or sanctions, securities law compliance, and online payment services. The introduction of new products, expansion of our activities in certain jurisdictions, or other actions that we may take may subject us to additional laws, regulations, or other government scrutiny. In addition, foreign data protection, privacy, content, competition, and other laws and regulations can impose different obligations or be more restrictive than those in the United States.
>
> These U.S. federal and state and foreign laws and regulations, which in some cases can be enforced by private parties in addition to government entities, are constantly evolving and can be subject to significant change. As a result, the application, interpretation, and enforcement of these laws and regulations are often uncertain, particularly in the new and rapidly evolving industry in which we operate, and may be interpreted and applied inconsistently from country to country and inconsistently with our current policies and practices. For example, regulatory or legislative actions affecting the manner in which we display content to our users or obtain consent to various practices could adversely affect user growth and engagement. Such actions could affect the

[75] *Id.*

[76] 2017 Form 10-K *supra* note 14, at 6. *See also* Lawrence J. Trautman & George P. Michaely, *The SEC and the Internet: Regulating the Web of Deceit*, 68 CONSUMER FIN. L. Q. REP. 262 (2014).

[77] 2017 Form 10-K, *supra* note 14, at 6.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

manner in which we provide our services or adversely affect our financial results.

We are also subject to laws and regulations that dictate whether, how, and under what circumstances we can transfer, process and/or receive certain data that is critical to our operations, including data shared between countries or regions in which we operate and data shared among our products and services. For example, in 2016, the European Union and United States agreed to an alternative transfer framework for data transferred from the European Union to the United States, called the Privacy Shield, but this new framework is subject to an annual review that could result in changes to our obligations and also may be challenged by national regulators or private parties. In addition, the other bases upon which Facebook relies to legitimize the transfer of such data, such as standard Model Contractual Clauses (MCCs), have been subjected to regulatory and judicial scrutiny. For example, the Irish Data Protection Commissioner has challenged the legal grounds for transfers of user data to Facebook, Inc., and the Irish High Court has agreed to refer this challenge to the Court of Justice of the European Union for decision. We also face multiple inquiries, investigations, and lawsuits in Europe, India, and other jurisdictions regarding the August 2016 update to WhatsApp's terms of service and privacy policy and its sharing of certain data with other Facebook products and services, including a lawsuit currently pending before the Supreme Court of India. If one or more of the legal bases for transferring data from Europe to the United States is invalidated, if we are unable to transfer data between and among countries and regions in which we operate, or if we are prohibited from sharing data among our products and services, it could affect the manner in which we provide our services or adversely affect our financial results.

Proposed or new legislation and regulations could also significantly affect our business. There currently are a number of proposals pending before federal, state, and foreign legislative and regulatory bodies. In addition, the new European General Data Protection Regulation (GDPR) [took] effect in May 2018 and will apply to all of our products and services that provide service in Europe. The GDPR will include operational requirements for companies that receive or process personal data of residents of the European Union that are different than those currently in place in the European Union. For example, we may be required to implement measures to change our service or limit access to our service for minors under the age of 16 for certain countries in Europe that maintain the minimum age of 16 under the GDPR. We may also be required to obtain consent and/or offer



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> new controls to existing and new users in Europe before processing data for certain aspects of our service. In addition, the GDPR will include significant penalties for non-compliance. Similarly, there are a number of legislative proposals in the United States, at both the federal and state level, that could impose new obligations in areas affecting our business, such as liability for copyright infringement by third parties. In addition, some countries are considering or have passed legislation implementing data protection requirements or requiring local storage and processing of data or similar requirements that could increase the cost and complexity of delivering our services.
>
> These laws and regulations, as well as any associated inquiries or investigations or any other government actions, may be costly to comply with and may delay or impede the development of new products, result in negative publicity, increase our operating costs, require significant management time and attention, and subject us to remedies that may harm our business, including fines or demands or orders that we modify or cease existing business practices.[78]

***P. Regulatory and Other Governmental Investigations***

Facebook reports being "subject to regulatory and other government investigations, enforcement actions, and settlements, and we expect to continue to be subject to such proceedings and other inquires . . . which could cause us to incur substantial costs or require us to change our business practices in a manner materially adverse to our business."[79] For example:

> From time to time, we receive formal and informal inquiries from government authorities and regulators regarding our compliance with laws and regulations, many of which are evolving and subject to interpretation. We are and expect to continue to be the subject of investigations, inquiries, data requests, actions, and audits in the United States, Europe, and around the world,

[78] 2017 Form 10-K *supra* note 14, at 17. *See also* Darcy Allen et al., *Some Economic Consequences of the GDPR*, 39(2) ECON. BULL. (2019); Marco Almada, *Human Intervention in Automated Decision-Making: Toward the Construction of Contestable Systems* (2019); Jonathan Andrew, Location Data and Human Mobility: An Evaluation of a Dissonance that Frames Data Protection and Privacy Rights, EUI doctoral thesis (2018), Emre Bayamlıoğlu, *Transparency of Automated Decisions in the GDPR: An Attempt for Systemisation* (2018), https://ssrn.com/abstract=3097653; Shmuel I. Becher & Uri Benoliel, *Law in Books and Law in Action: The Readability of Privacy Policies and the GDPR*, CONSUMER L. & ECON., Klaus Mathis & Avishalom Tor eds., *Consumer Law and Economics* (Springer 2020), https://ssrn.com/abstract=3334095; Jean-Sylvestre Bergé et al., *The 'Datasphere', Data Flows Beyond Control, and the Challenges for Law and Governance*, 5(2) EURO. J. COMP. L. & GOVERN. (2018), https://ssrn.com/abstract=3185943.

[79] 2017 Form 10-K, *supra* note 14, at 18; *see also* Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who and How It Works*, 5 J.L. & CYBER WARFARE 147 (2016).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> particularly in the areas of privacy, data protection, law enforcement, consumer protection, and competition, as we continue to grow and expand our operations. For example, several data protection authorities in the European Union have initiated actions, investigations, or administrative orders seeking to assert jurisdiction over Facebook, Inc. and our subsidiaries and to restrict the ways in which we collect and use information, and other data protection authorities may do the same. Orders issued by, or inquiries or enforcement actions initiated by, government or regulatory authorities could cause us to incur substantial costs, expose us to unanticipated civil and criminal liability or penalties (including substantial monetary fines), or require us to change our business practices in a manner materially adverse to our business.[80]

Of particular concern at present, *The New York Times* states, "Regulators and law enforcement officials in the United States and Europe are investigating Facebook's conduct with Cambridge Analytica, a political data firm that worked with Mr. Trump's 2016 campaign, opening up the company to fines and other liability."[81] As a result of the 2016 and subsequent election advertising, "[b]oth the Trump administration and lawmakers have begun crafting proposals for a national privacy law, setting up a years-long struggle over the future of Facebook's data-hungry business model."[82] (See §§ VI and IX, *infra*).

***Q. Protection of Intellectual Property***

Facebook warns, "If we are unable to protect our intellectual property, the value of our brands and other intangible assets may be diminished, and our business may be adversely affected."[83] In addition:

> We rely and expect to continue to rely on a combination of confidentiality, assignment, and license agreements with our employees, consultants, and third parties with whom we have relationships, as well as trademark, copyright, patent, trade secret, and domain name protection laws, to protect our proprietary rights. In the United States and internationally, we have filed various applications for protection of certain aspects of our intellectual property, and we currently hold a significant number of registered trademarks and issued patents in multiple jurisdictions and have acquired patents and

[80] 2017 Form 10-K, *supra* note 14, at 18.

[81] Frenkel et al., *supra* note 1, at A1.

[82] *Id.*

[83] 2017 Form 10-K, *supra* note 14, at 19.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> patent applications from third parties. Third parties may knowingly or unknowingly infringe our proprietary rights, third parties may challenge proprietary rights held by us, and pending and future trademark and patent applications may not be approved. . . . Although we have generally taken measures to protect our proprietary rights, there can be no assurance that others will not offer products or concepts that are substantially similar to ours and compete with our business. . . .[84]

***R. Liability from Internet Transmissions or Publications***

The Company warns, "We may incur liability as a result of information retrieved from or transmitted over the Internet or published using our products or as a result of claims related to our products."[85]

> We have faced, currently face, and will continue to face claims relating to information that is published or made available on our products. In particular, the nature of our business exposes us to claims related to defamation, dissemination of misinformation or news hoaxes, discrimination, intellectual property rights, rights of publicity and privacy, personal injury torts, or laws regulating hate speech or other types of content. This risk is enhanced in certain jurisdictions outside the United States where our protection from liability for third-party actions may be unclear or where we may be less protected under local laws than we are in the United States. In addition, there have been various Congressional efforts to restrict the scope of the protections available to online platforms under Section 230 of the Communications Decency Act, and our current protections from liability for third-party content in the United States could decrease or change. We could incur significant costs investigating and defending such claims and, if we are found liable, significant damages. We could also face fines or orders restricting or blocking our services in particular geographies as a result of content hosted on our services. For example, recently enacted legislation in Germany may impose significant fines for failure to comply with certain content removal and disclosure obligations. If any of these events occur, our business and financial results could be adversely affected.[86]

[84] *Id.*

[85] 2017 Form 10-K, *supra* note 14, at 20.

[86] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

### *S. Disruption of Technical Infrastructure, Undetected Vulnerabilities*

Of particular importance to our discussion, Facebook highlights recognition that, "Our business is dependent on our ability to maintain and scale our technical infrastructure, and any significant disruption in our service could damage our reputation, result in a potential loss of users and engagement, and adversely affect our financial results."[87] Other technological risks include, "unforeseen difficulties in building and operating key portions of our technical infrastructure. . . . Our products and internal systems rely on software that is highly technical, and if it contains undetected errors or vulnerabilities, our business could be adversely affected."[88] Accordingly:

> Our reputation and ability to attract, retain, and serve our users is dependent upon the reliable performance of our products and our underlying technical infrastructure. . . . If our products are unavailable when users attempt to access them, or if they do not load as quickly as expected, users may not use our products as often in the future, or at all, and our ability to serve ads may be disrupted. As our user base and engagement continue to grow, and the amount and types of information shared on Facebook and our other products continue to grow and evolve, such as increased engagement with video, we will need an increasing amount of technical infrastructure, including network capacity and computing power, to continue to satisfy the needs of our users and advertisers. . . . A substantial portion of our network infrastructure is provided by third parties. Any disruption or failure in the services we receive from these providers could harm our ability to handle existing or increased traffic and could significantly harm our business. Any financial or other difficulties these providers face may adversely affect our business, and we exercise little control over these providers, which increases our vulnerability to problems with the services they provide.
>
> ***We could experience unforeseen difficulties in building and operating key portions of our technical infrastructure. . . .***
>
> ***Our products and internal systems rely on software that is highly technical, and if it contains undetected errors or vulnerabilities, our business could be adversely affected. . . .***

[87] *Id.* at 21.

[88] *Id.* at 22.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> ***Technologies have been developed that can block the display of our ads, which could adversely affect our financial results. . . .***[89]

### *T. Real or Perceived Inaccuracies in User and Other Metrics*

Facebook discloses that "real or perceived inaccuracies in our user and other metrics may harm our reputation and negatively affect our business."[90]

> The numbers for our key metrics, which include our DAUs, MAUs, and average revenue per user (ARPU), are calculated using internal company data based on the activity of user accounts. While these numbers are based on what we believe to be reasonable estimates of our user base for the applicable period of measurement, there are inherent challenges in measuring usage of our products across large online and mobile populations around the world. In addition, we are continually seeking to improve our estimates of our user base, and such estimates may change due to improvements or changes in our methodology.
>
> We regularly evaluate these metrics to estimate the number of "duplicate" and "false" accounts among our MAUs. A duplicate account is one that a user maintains in addition to his or her principal account. We divide "false" accounts into two categories: (1) user-misclassified accounts, where users have created personal profiles for a business, organization, or non-human entity such as a pet (such entities are permitted on Facebook using a Page rather than a personal profile under our terms of service); and (2) undesirable accounts, which represent user profiles that we determine are intended to be used for purposes that violate our terms of service, such as spamming. The estimates of duplicate and false accounts are based on an internal review of a limited sample of accounts, and we apply significant judgment in making this determination. For example, to identify duplicate accounts we use data signals such as similar IP addresses or usernames, and to identify false accounts we look for names that appear to be fake or other behavior that appears inauthentic to the reviewers. Our estimates may change as our methodologies evolve, including through the application of new data signals or technologies, which may allow us to identify previously undetected duplicate or false accounts and may improve our ability to evaluate a broader population of our users. As such, our estimation of duplicate or false accounts may not accurately represent the actual number of such accounts. In

[89] *Id.* at 21.

[90] *Id.* at 22.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> particular, duplicate accounts are very difficult to measure at our scale, and it is possible that the actual number of duplicate accounts may vary significantly from our estimates.
>
> In the fourth quarter of 2017, we estimate that duplicate accounts may have represented approximately 10% of our worldwide MAUs. We believe the percentage of duplicate accounts is meaningfully higher in developing markets such as India, Indonesia, and the Philippines, as compared to more developed markets. In the fourth quarter of 2017, we estimate that false accounts may have represented approximately 3–4% of our worldwide MAUs. Our estimation of false accounts can vary as a result of episodic spikes in the creation of such accounts, which we have seen originate more frequently in specific countries such as Indonesia, Turkey, and Vietnam. From time to time, we may make product changes or take other actions to reduce the number of duplicate or false accounts among our users, which may also reduce our DAU and MAU estimates in a particular period.[91]

***U. Payment Transactions***

Facebook warns, "payment transactions may subject us to additional regulatory requirements and other risks that could be costly and difficult to comply with or that could harm our business.[92] Technology thought leaders Ben Thompson and James Allworth contend that "payments" built around blockchain technology will likely become a major foundational building block for Facebook's future strategy.[93] The Company explains:

> Our users can purchase virtual and digital goods from developers that offer applications using our Payments infrastructure on the Facebook website. In addition, certain of our users can use our Payments infrastructure, including on Messenger, for other activities, such as sending money to other users and making donations to

[91] *Id.*

[92] 2017 Form 10-K, *supra* note 14, at 23; *see also* Lawrence J. Trautman, *Bitcoin, Virtual Currencies, and the Struggle of Law and Regulation to Keep Pace*, 102 MARQ. L. REV. 447 (2018); Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin versus Regulated Payment Systems: What Gives?*, 38 CARDOZO L. REV. 1041 (2017); Lawrence J. Trautman, *E-Commerce and Electronic Payment System Risks: Lessons from PayPal*, 17 U.C. DAVIS BUS. L.J. 261 (Spring 2016).

[93] *See* Ben Thompson & James Allworth, *Mark Zuckerberg's Projected Self*, EXPONENT, Episode 165 (Mar. 8, 2019) (discussing Facebook's future strategy of cross selling ease of use payments function), https://itunes.apple.com/us/podcast/exponent/id826420969?mt=2&i=1000431353735; Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, 88(1) UMKC L. REV. 1 (2019); Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?*, 69 CONSUMER FIN. L.Q. REP. 232 (2016); Lawrence J. Trautman, *Virtual Currencies: Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?*, 20 RICH. J.L. & TECH. 13 (2014).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> certain charitable organizations. We are subject to a variety of laws and regulations in the United States, Europe, and elsewhere, including those governing anti-money laundering and counter-terrorist financing, money transmission, gift cards and other prepaid access instruments, electronic funds transfer, charitable fundraising, and import and export restrictions. . . . In addition, we may be subject to a variety of additional risks as a result of Payments transactions, including:
>
> - increased costs and diversion of management time and effort and other resources to deal with bad transactions or customer disputes;
> - potential fraudulent or otherwise illegal activity by users, developers, employees, or third parties;
> - restrictions on the investment of consumer funds used to transact Payments; and
> - additional disclosure and reporting requirements.[94]

***V. International Operations***

The Company notes, "we have significant international operations and plan to continue expanding our operations abroad where we have more limited operating experience, and this may subject us to increased business and economic risks that could affect our financial results."[95] In addition:

> We have significant international operations and plan to continue the international expansion of our business operations and the translation of our products. We currently make Facebook available in more than 100 different languages, and we have offices or data centers in more than 30 different countries. We may enter new international markets where we have limited or no experience in marketing, selling, and deploying our products. Our products are generally available globally through the web and on mobile, but some or all of our products or functionality may not be available in certain markets due to legal and regulatory complexities. For example, Facebook and certain of our other products are not generally available in China . . . we are subject to a variety of risks inherent in doing business internationally, including:
>
> - Political, social, or economic instability;

[94] 2017 Form 10-K, *supra* note 14, at 23.

[95] 2017 Form 10-K, *supra* note 14, at 23. *See also* Lawrence J. Trautman, *Rapid Technological Change and U.S. Entrepreneurial Risk in International Markets: Focus on Bribery and Corruption* (2017).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

- risks related to legal, regulatory, and other government scrutiny applicable to U.S. companies with sales and operations in foreign jurisdictions, including with respect to privacy, tax, law enforcement, content, trade compliance, intellectual property, and terrestrial infrastructure matters;
- potential damage to our brand and reputation due to compliance with local laws, including potential censorship or requirements to provide user information to local authorities;
- fluctuations in currency exchange rates and compliance with currency controls;
- foreign exchange controls and tax and other regulations and orders that might prevent us from repatriating cash earned in countries outside the United States or otherwise limit our ability to move cash freely, and impede our ability to invest such cash efficiently;
- higher levels of credit risk and payment fraud;
- enhanced difficulties of integrating any foreign acquisitions;
- burdens of complying with a variety of foreign laws;
- reduced protection for intellectual property rights in some countries;
- difficulties in staffing, managing, and overseeing global operations and the increased travel, infrastructure, and legal compliance costs associated with multiple international locations;
- compliance with the U.S. Foreign Corrupt Practices Act, the U.K. Bribery Act, and similar laws in other jurisdictions; and
- compliance with statutory equity requirements and management of tax consequences.

If we are unable to expand internationally and manage the complexity of our global operations successfully, our financial results could be adversely affected.[96]

[96] 2017 Form 10-K *supra* note 14, at 24. *See also* Lawrence J. Trautman & Kara Altenbaumer-Price, *The Foreign Corrupt Practices Act: Minefield for Directors*, 6 VA. L. & BUS. REV. 145 (2011); Lawrence J. Trautman & Kara Altenbaumer-Price, *Foreign Corrupt Practices Act: An Update on Enforcement and SEC and DOJ Guidance*, 41 SEC. REG. L.J. 241 (2013); Lawrence J. Trautman & Joanna



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

## VI. THE FACEBOOK PRIVACY CRISIS

> *The Facebook matter involving Aleksander Kogan and Cambridge Analytica shed a bright light on the data practices of some of our largest technology companies. Although advertisers and political campaigns have collected and used data for years, the public seemed generally unaware. This story has forced both the public and lawmakers to confront serious issues that need to be addressed, including what role Congress should play in promoting transparency for consumers regarding data collection and use, while ensuring a well-functioning marketplace for our data-dependent technologies to drive further innovation.*
>
> *Senator Chuck Grassley,*
> *Chairman, Senate Judiciary*
> *Committee*
> *May 16, 2018*[97]

Recently, many legal scholars have been focused on issues related to the impact by social media on individual privacy rights.[98] Any discussion of the Facebook privacy crisis must start with an attempt to understand the revolutionary change in the societal and economic ecosystem that is now less than two decades old.

### *A. Surveillance Capitalism*

Harvard Business School Emerita Professor Soshana Zuboff has provided perhaps the most comprehensive analysis yet about how our world has been disrupted by the dark side of a technological future.[99] In her influential book, *The*

Kimbell, *Bribery and Corruption: The COSO Framework, FCPA, and U.K. Bribery Act*, 30 FLA. J. INT'L L. 191 (2018); Lawrence J. Trautman & Kara Altenbaumer-Price, *Lawyers, Guns and Money—The Bribery Problem and U.K. Bribery Act*, 47 INT'L LAW. 481 (2013).

[97] *Cambridge Analytica and the Future of Data Privacy: Hearing Before the S. Comm. on the Judiciary*, 115th Cong. 2 (2018) (statement of Sen. Grassley, Chairman, Senate Comm. on the Judiciary), https://www.judiciary.senate.gov/meetings/cambridge-analytica-and-the-future-of-data-privacy.

[98] *See* Patricia Abril, Avner Levin & Alissa Del Riego, *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L.J. 63 (2012); Alessandro Acquisti, Curtis R. Taylor & Liad Wagman, *The Economics of Privacy*, 52 J. ECON. LIT. (2016); Derek E. Bambauer, *Exposed*, 98 MINN. L. REV. 2025 (2014); Anita Bernstein, *Real Remedies for Virtual Injuries*, 90 N.C. L. REV. 1457 (2012); Jordan M. Blanke, *The Legislative Response to Employers' Requests for Password Disclosure*, 14 SUFFOLK U. J. HIGH TECH. L. (2014); Hannah Bloch-Wehba, *Global Platform Governance: Private Power in the Shadow of the State*, 72 SMU L. REV. 27 (2019); Christopher Borchert, Fernando M. Pinguelo & David Thaw, *Reasonable Expectations of Privacy Settings: Social Media and the Stored Communications Act*, 13 DUKE L. & TECH. REV. 36 (2015); Danah Boyd & Alice E. Marwick, *Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies*, Symposium, *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society* (2011), https://ssrn.com/abstract=1925128; Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).

[99] See ZUBOFF, *supra* note 48.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

*Age of Surveillance Capitalism*, published in 2019, Professor Zuboff writes, "At its core, surveillance capitalism is parasitic and self-referential. It revives Karl Marx's old image of capitalism as a vampire that feeds on labor, but with an unexpected turn. Instead of labor, surveillance capitalism feeds on every aspect of every human's experience."[100] In sum:

> Surveillance capitalism operates through unprecedented asymmetries in knowledge and the power that accrues to knowledge. Surveillance capitalists know everything *about us*, whereas their operations are designed to be unknowable *to us*. They accumulate vast domains of new knowledge *from us*, but not *for us*. They predict our futures for the sake of others' gain, not ours. As long as surveillance capitalism and its behavioral futures markets are allowed to thrive, ownership of the new means of behavioral modification eclipse ownership of the means of production as the fountainhead of capitalist wealth and power in the twenty-first century.[101]

Building upon the teachings of Meyer, Planck, Skinner, Friedrich Hayek and Adam Smith, Professor Zuboff discusses the linking by Smith and Hayek of freedom and ignorance:

> In Hayek's framing, the mystery of the market is that a great many people can behave effectively while remaining ignorant of the whole. Individuals not only *can* choose freely, but they *must* freely choose their own pursuits because there is no alternative, no source of total knowledge or conscious control to guide them. "Human design" is impossible, Hayek says, because the relevant information flows are "beyond the span of the control of any one mind." The market dynamic makes it possible for people to operate in ignorance without "anyone having to tell them what to do."
>
> Hayek chose the market over democracy, arguing that the market system enabled not only the division of labor but also "the coordinated utilization of resources based on *equally divided knowledge*." This system, he argued, is the only one compatible with freedom.[102]

Professor Zuboff writes, "[w]hen it comes to surveillance capitalist operations, the 'market' is no longer invisible, certainly not in the way that Smith or Hayek imagined. The competitive struggle among surveillance capitalists produces the

[100] *Id.* at 9.

[101] *Id.* at 11.

[102] *Id.* at 497.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

compulsion toward totality."[103] Therefore, in a dramatic rebuke of the foundational concept of the "market" being intrinsically unknowable—Professor Zuboff observes, "[t]otal information tends toward certainty and the promise of guaranteed outcomes. These operations mean that the supply and demand of behavioral futures markets are rendered in infinite detail. Surveillance capitalism thus replaces mystery with certainty as it substitutes rendition, behavioral modification, and prediction for the old 'unsurveyable pattern.'"[104] Professors Yochai Benkler, Robert Faris, and Hal Roberts observe that after 2016:

> Something fundamental was happening to threaten democracy, and our collective eye fell on the novel and rapidly changing—technology. Technological processes beyond the control of any person or country—the convergence of social media, algorithmic news curation, bots, artificial intelligence, and big data analysis—were creating echo chambers that reinforce our biases, were removing indicia of trustworthiness, and were generally overwhelming our capacity to make sense of the world, and with it our capacity to govern ourselves as reasonable democracies.[105]

To help us better understand this pervasive economic engine that is just a few decades old, Professor Zuboff writes that "Google is to surveillance capitalism what the Ford Motor Company and General Motors were to mass-production-based managerial capitalism. New economic logics and their commercial models are discovered by people in a time and place and then perfected through trial and error."[106] In recent years, "Google became the pioneer, discoverer, elaborator, experimenter, lead practitioner, role model, and diffusion hub of *surveillance capitalism*."[107] UC Berkeley professor and longtime Google chief economist Hal Varian is credited with providing the logic of surveillance capitalism in four primary uses: "(1) data extraction and analysis; (2) new contractual forms due to better monitoring; (3) personalization and customization; and (4) continuous experiments."[108] Professor Zuboff writes, "[i]t's not just that the cards have been

---

[103] *Id.*

[104] *Id.*

[105] YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 4 (2018).

[106] ZUBOFF, *supra* note 48.

[107] *Id.*

[108] ZUBOFF, *supra* note 48 (citing Hal R. Varian, *Computer Mediated Transactions*, 100 AM. ECON. REV. 1 (2010)); Hal R. Varian, *Beyond Big Data*, 49 BUS. ECON. 27 (2014). *See also* Gregory Day & Abbey Stemler, *Supracompetitive Privacy*, 107 IOWA L. REV. 61 (2019) (discussion regarding capturing and extracting value from data).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

reshuffled; the rules of the game have been transformed into something that is both unprecedented and unimaginable outside the digital milieu and the vast resources of wealth and scientific prowess that the new applied utopianists bring to the table."[109] As just one of the many remaining insights provided by professor Zuboff:

> Surveillance capitalisms command and control of the division of learning in society are the signature feature that breaks with the old justifications of the invisible hand and its entitlements. The combination of knowledge and freedom works to accelerate the asymmetry of power between surveillance capitalists and the societies in which they operate. This cycle will be broken only when we acknowledge as citizens, as societies, and indeed as a civilization that *surveillance capitalists know too much to qualify for freedom*.[110]

### *B. Fake News*

By now, much has been written about "fake news."[111] Professor Shoshana Zuboff traces this rather recent development to "Facebook's and Google's overreaching ambitions to supplant professional journalism on the Internet.[112] Both corporations inserted themselves between publishers and their populations, subjecting journalistic 'content' to the same categories of equivalence that dominate

---

[109] ZUBOFF, *supra* note 48, at 499.

[110] *Id.*

[111] *See* Christoph Aymanns, Jakob Foerster & Co-Pierre Georg, *Fake News in Social Networks* 1–24 (U. St. Gallen, School of Fin., Paper No. 2018/4, 2017); Jack M. Balkin, *Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation*, 51 U.C. DAVIS L. REV. 1149 (2018); Marc Jonathan Blitz, *Lies, Line Drawing and (Deep) Fake News*, 71 OKLA. L. REV. 59 (2018); Robert Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CAL. L. REV. 1753 (2018); Danielle Keats Citron, *Extremist Speech, Compelled Conformity, and Censorship Creep*, 93 NOTRE DAME L. REV. 1035 (2018); Michael C. Dorf & Sidney Tarrow, *Stings and Scams: 'Fake News,' the First Amendment, and the New Activist Journalism* 1–31 (Cornell Legal Stud., Research Paper No. 17-02, 2017); James Grimmelmann, *The Platform is the Message*, 2 GEO. L. TECH. REV. 217 (2018); Richard L. Hasen, *Cheap Speech and What It Has Done (to American Democracy)*, 16 FIRST AMEND. L. REV. 200 (2018); Richard L. Hasen, *The 2016 U.S. Voting Wars: From Bad to Worse*, 26 WM. & MARY BILL RTS. J. 629 (2018); Chris Jay Hoofnagle & Eduard Meleshinsky, *Native Advertising and Endorsement: Schema, Source-Based Misleadingness, and Omission of Material Facts*, 2015121503 TECH. SCI. (2015), https://techscience.org/a/2015121503; Dan M. Kahan, *Misconceptions, Misinformation, and the Logic of Identity-Protective Cognition* 1–9 (Yale L. Sch., Pub. L. Research Paper No. 605, 2017); Jacob Nelson & Harsh Taneja, *The Small, Disloyal Fake News Audience: The Role of Audience Availability in Fake News Consumption*, 20 NEW MEDIA & SOCIETY 3720 (2018); Mark Verstraete, Derek E. Bambauer & Jane R. Yakowitz Bambauer, *Identifying and Countering Fake News* 1–33 (Ariz. Legal Stud., Discussion Paper No. 17-15, 2017); Ari Ezra Waldman, *The Marketplace of Fake News*, 20 U. PA. J. CONST. L. 101 (2018); Abby K. Wood & Ann M. Ravel, *Fool Me Once: Regulating 'Fake News' and Other Online Advertising*, 91 S. CAL. L. REV. 1227 (2018).

[112] Keach Hagey, Lukas I. Alpert & Yaryna Serkez, *Local News Fades Out: A Divide Between Newspaper Haves and Have-Nots*, WALL ST. J., May 4, 2019, at B1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

surveillance capitalism's other landscapes."[113] Professor Zuboff states that the job of the journalist, "is to produce news and analysis that separate truth from falsehood . . . Facebook's decision to standardize the presentation of its News Feed content so that 'all news stories looked roughly the same as each other . . . [assisted] organized political disinformation campaigns . . . during the 2016 U.S. presidential election.'"[114]

### *C. Facebook Privacy Crisis*

During recent years, disagreements about privacy issues at Facebook appear to have resulted in several high-profile departures, including: Elliot Schrange, who previously served as vice president for global communications, marketing, and public policy; and security chief Alex Stamos.[115] Facebook top management, in particular Mark Zuckerberg and Sheryl Sandberg, have "cast their company as a force for social good. Facebook's lofty aims were emblazoned even on security filings: 'Our mission is to make the world more open and connected.'"[116] As a business model, "Facebook had positioned itself as a platform, not a publisher. Taking responsibility for what users posted, or acting to censor it, was expensive and complicated. Many Facebook executives worried that any such effort would backfire."[117]

### *D. Congressional Hearings*

Earlier drafts of this manuscript stressed many concerns voiced by members of Congress during hearings held in 2018. Nevertheless, many of these concerns were eclipsed by developments during early 2019, and a considerable amount of language was removed from earlier drafts of this manuscript to make room for discussion of more recent developments as new revelations were uncovered. In their annual report for the period ending December 31, 2018, Facebook starts to talk about their "privacy crisis" by disclosing:

> Beginning on March 20, 2018, multiple putative class actions and derivative actions were filed in state and federal courts in the United States and elsewhere against us and certain of our directors and officers alleging violations of securities laws, breach of fiduciary duties, and other causes of action in connection with our platform and user data practices as well as the misuse of certain

[113] ZUBOFF, *supra* note 48, at 506.

[114] *Id.* at 507; *see also* Erin Carroll, *Making News: Balancing Newsworthiness and Privacy in the Age of Algorithms*, 106 GEO. L.J. 69 (2017).

[115] *See* Frenkel et al., *supra* note 1.

[116] *Id.*

[117] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

data by a developer that shared such data with third parties in violation of our terms and policies, and seeking unspecified damages and injunctive relief. Beginning on July 27, 2018, two putative class actions were filed in federal court in the United States against us and certain of our directors and officers alleging violations of securities laws in connection with the disclosure of our earnings results for the second quarter of 2018, and seeking unspecified damages. These two actions subsequently were transferred and consolidated in the U.S. District Court for the Northern District of California with the putative securities class action described above relating to our platform and user data practices. We believe these lawsuits are without merit, and we are vigorously defending them. In addition, our platform and user data practices, as well as the events surrounding the misuse of certain data by a developer, became the subject of U.S. Federal Trade Commission, Securities and Exchange Commission, state attorneys general, and other government inquiries in the United States, Europe, and other jurisdictions. Any such inquiries could subject us to substantial fines and costs, require us to change our business practices, divert resources and the attention of management from our business, or adversely affect our business.

Beginning on September 28, 2018, multiple putative class actions were filed in state and federal courts in the United States and elsewhere against us alleging violations of consumer protection laws and other causes of action in connection with a third-party cyber-attack that exploited a vulnerability in Facebook's code to steal user access tokens and access certain profile information from user accounts on Facebook, and seeking unspecified damages and injunctive relief. We believe these lawsuits are without merit, and we are vigorously defending them. In addition, the events surrounding this cyber-attack became the subject of Irish Data Protection Commission, U.S. Federal Trade Commission and other government inquiries in the United States, Europe, and other jurisdictions. Any such inquiries could subject us to substantial fines and costs, require us to change our business practices, divert resources and the attention of management from our business, or adversely affect our business.

In addition, from time to time, we are subject to litigation and other proceedings involving law enforcement and other regulatory agencies, including in particular in Brazil and Europe, in order to ascertain the precise scope of our legal obligations to comply with the requests of those agencies, including our obligation to disclose user information in particular circumstances. A



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> number of such instances have resulted in the assessment of fines and penalties against us.[118]

***1. Congressional Hearings of April 10 and 11, 2018***

By early 2018 Facebook was in a full privacy crisis as demonstrated by the aggressive Congressional examination of Mr. Zuckerberg, "repeatedly cutting off the Facebook CEO so he couldn't 'filibuster,' as Representative Martha Blackburn put it. Representatives from both parties came back time and again to what Facebook *knows*, what Facebook *tells users* about what it knows, and what Facebook *lets advertisers do* with what it knows."[119] Mr. Zuckerberg stated, "For most of our existence, we focused on all the good that connecting people can bring. . . . After Hurricane Harvey, people raised more than $20 million for relief. And more than 70 million small businesses now use Facebook to grow and create jobs."[120] And then, Mr. Zuckerberg states:

> But it's clear now that we didn't do enough to prevent these tools from being used for harm as well. That goes for fake news, foreign interference in elections, and hate speech, as well as developers and data privacy. We didn't take a broad enough view of our responsibility, and that was a big mistake. It was my mistake, and I am sorry. I started Facebook, I run it, and I am responsible for what happens here.[121]

Following these highly publicized Congressional Hearings, on June 8, 2018[122] and June 29, 2018 Facebook provided responses to questions from the legislators, stating "we received over 2,000 questions from the Senate and House Committees before which we testified on April 10 and 11, 2018."[123]

---

[118] 2018 Form 10-K, *supra* note 15, at 30.

[119] *See* Alexis C. Madrigal, *The Most Important Exchange of the Zuckerberg Hearing*, THE ATLANTIC (Apr. 11, 2018), https://www.theatlantic.com/technology/archive/2018/04/the-most-important-exchange-of-the-zuckerberg-hearing/557795/.

[120] *Facebook, Social Media Privacy, and the Use and Abuse of Data: Hearing Before the S. Comm. on the Judiciary and S. Comm. on Commerce, Science and Transportation*, 115th Cong. 2 (2018) (statement of Mark Zuckerberg, Chairman and CEO, Facebook), https://www.judiciary.senate.gov/meetings/facebook-social-media-privacy-and-the-use-and-abuse-of-data.

[121] *Id.*

[122] Letter from Facebook, Inc. to Senator Charles Grassley, Chairman, and Senator Dianne Feinstein, Ranking Member, Senate Judiciary Comm. (June 28, 2018), https://www.judiciary.senate.gov/imo/media/doc/Zuckerberg%20Responses%20to%20Judiciary%20Committee%20QFRs.pdf.

[123] Letter from Facebook, Inc. to Rep. Chairman Gregory Walden and Ranking Member Rep. Frank Pallone, H. Comm. on Energy & Commerce (June 29, 2018), https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf (containing 752 pages of answers to congressional questions).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

### *2. Senate Judiciary Hearings on Cambridge Analytica of May 16, 2018*

As Professor Sarah Haan describes, "With the benefit of hindsight, a federal indictment, and a growing body of research, we now know that political discourse on social media in 2015 and 2016 was influenced by fake accounts run by foreign state actors."[124]

In his opening remarks, Senate Judiciary Committee Chairman Chuck Grassley observed, "The Facebook story first broke in December 2015, when *The Guardian* identified that Dr. Kogan had transferred Facebook data to Cambridge Analytica in violation of Facebook's data policy."[125] By now, over three years after its first awareness of Facebook's role in Russian election meddling, many scholars have written about this Cambridge Analytica story that continues to unfold.[126] Space limitations prohibit more coverage of this topic here.

### *3. Senate Select Committee on Intelligence Hearings of September 5, 2018*

Journalist Katy Steinmetz writes, "Facebook COO Sheryl Sandberg faced grilling from lawmakers on issues ranging from user privacy and hate speech to the integrity of their business models and criminals who use platforms to paddle drugs."[127] In her prepared opening testimony, Ms. Sandberg states:

> As this committee's bipartisan report states, in January 2017, the CIA, NSA, and FBI "revealed key elements of a comprehensive and multifaceted Russian campaign against the United States." The Committee's subsequent investigation "has exposed a far more extensive Russian effort to manipulate social media outlets to sow discord and to interfere in the 2016 election and American society," as well as additional examples of

---

[124] Sarah C. Haan, Bad Actors (unpublished manuscript) (on file with author).

[125] *See* Statement of Sen. Chuck Grassley, *supra* note 97.

[126] *See, e.g.*, ANATOLIY GRUZD, JENNA JACOBSON, PHILIP MAI & ELIZABETH DUBOIS, SOCIAL MEDIA PRIVACY IN CANADA (2018), https://ssrn.com/abstract=3195503; DAPHNE KELLER, TOWARD A CLEARER CONVERSATION ABOUT PLATFORM LIABILITY, Knight First Amendment Institute's "Emerging Threats" essay series (2018), https://ssrn.com/abstract=3186867; SHAUN B. SPENCER, THE PROBLEM OF ONLINE MANIPULATION (2019), https://ssrn.com/abstract=3341653; YAN SHVARTZSHNAIDER, NOAH APTHORPE, NICK FEAMSTER & HELEN F. NISSENBAUM, ANALYZING PRIVACY POLICIES USING CONTEXTUAL INTEGRITY ANNOTATIONS (2018), https://ssrn.com/abstract=3244876; HAMID AKIN UNVER, DIGITAL OPEN SOURCE INTELLIGENCE AND INTERNATIONAL SECURITY: A PRIMER, EDAM RES. RPTS, CYBER GOVN. & DIGITAL DEMOCRACY (2018), https://ssrn.com/abstract=3331638.

[127] Katy Steinmetz, *Lawmakers Hint at Regulating Social Media During Hearing With Facebook and Twitter Execs*, TIME (Sept. 5, 2018), http://time.com/5387560/senate-intelligence-hearing-facebook-twitter/; *see also* Natasha Lomas, *Highlights from the Senate Intelligence Hearing with Facebook and Twitter*, TECHCRUNCH (Sept. 5, 2018), https://techcrunch.com/2018/09/05/highlights-from-the-senate-intelligence-hearing-with-facebook-and-twitter/.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> Russia's attempts to "interfere in U.S. elections and those of our allies."
>
> We were too slow to spot this and too slow to act. That's on us. This interference was completely unacceptable. It violated the values of our company and of the country we love. . . .
>
> We're investing heavily in people and technology to keep our community safe and keep our service secure. This includes using artificial intelligence to help find bad content and locate bad actors. We're shutting down fake accounts and reducing the spread of false news. We've put in place new ad transparency policies, ad content restrictions, and documentation requirements for political ad buyers. We're getting better at anticipating risks and taking a broader view of our responsibilities. And we're working closely with law enforcement and our industry peers to share information and make progress together.[128]

### *E. New York Times Disclosures of November 2018*

On November 15, 2018, *The New York Times* ran a front-page story describing how Facebook covered up knowledge and disclosure of Russian-linked activity and exploitation resulting in Kremlin led disruption of the 2016 U.S. elections, "broadcast [of] viral propaganda and inspir[ing] deadly campaigns of hate across the globe."[129] Other topics receiving particular attention in this *New York Times* article include: the President Trump Muslim ban; hate speech; opposition research; and focused attack on enemies and competitors. These and other revelations have resulted in a crisis for the leading global social media platform. According to *The New York Times*, "Mr. Zuckerberg and Ms. Sandberg stumbled. Bent on growth, the pair ignored warning signs and then sought to conceal them from public view. At critical moments over the last three years, they were distracted by personal projects, and passed off security and policy decisions to subordinates. . . ."[130]

*The New York Times* article states,

> when Facebook users learned last spring [2018] that the company had compromised their privacy in its rush to expand, allowing access to the information of tens of millions of people to a political data firm linked to

[128] *Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 2 (2018) (statement of Sheryl Sandberg, Chief Operating Officer, Facebook, Inc.), https://www.intelligence.senate.gov/hearings/open-hearing-foreign-influence-operations%E2%80%99-use-social-media-platforms-company-witnesses.

[129] Frenkel et al., *supra* note 1.

[130] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> President Trump, Facebook sought to deflect blame and mask the extent of the problem.[131]

During March 2018 *The Guardian* and *New York Times* reported that consulting firm Cambridge Analytica successfully harvested personal data from a Facebook quiz app to identify potential Donald Trump voters.[132] At that time, CEO Mark Zuckerberg stated, "I started this place, I run it . . . I'm responsible for what happens here. . . . Facebook has 15,000 people working on security and reviewing content, and will have 20,000 by the end of the year [2018]."[133]

*The New York Times* observes, "as the company's stock price plummeted and its disclosures set off a consumer backlash—Facebook went on the attack."[134] Accordingly:

> While Mr. Zuckerberg has conducted a public apology tour in the last year, Ms. Sandberg has overseen an aggressive lobbying campaign to combat Facebook's critics, shift public anger toward rival companies and ward off damaging regulation. Facebook employed a Republican opposition-research firm to discredit activist protesters, in part by linking them to the liberal financier George Soros. It also tapped its business relationships, persuading a Jewish civil rights group to cast some criticism of the company as anti-Semitic.[135]

### *F. 2016 Russian Election Meddling*

Professors Yochai Benkler, Robert Faris, and Hal Roberts have written, "[o]n January 6, 2017, the Office of the Director of National Intelligence released a report that blamed Russia of running a disinformation campaign aimed to influence the U.S. election with the aim of helping Donald Trump get elected."[136] We now know that, about a year earlier, engineers at Facebook discovered Russian-linked activity during

---

[131] *Id.*

[132] *See* Michelle Castillo, *Facebook's Mark Zuckerberg: "I'm Responsible for What Happened" With data Privacy Issues*, CNBC.COM (Apr. 4, 2018), https://www.cnbc.com/2018/04/04/mark-zuckerberg-facebook-user-privacy-issues-my-mistake.html.

[133] *Id.*

[134] Frenkel et al., *supra* note 1.

[135] *Id.*

[136] YOCHAI BENKLER ET AL., NETWORK PROPAGANDA: MANIPULATION, DISINFORMATION, AND RADICALIZATION IN AMERICAN POLITICS 3 (2018) (citing to "Assessing Russian Activities and Intentions in Recent US Elections," Intelligence Community Assessment (Jan. 6, 2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.); *see also* Michael Morley, The Channels of Foreign Interference in American Elections (unpublished manuscript) (on file with author).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

spring of 2016 that was designed to disrupt the U.S. presidential election.[137] *The New York Times* reports, "a company expert on Russian cyberwarfare spotted something worrisome. He reached out to his boss, Mr. [Alex] Stamos. Mr. Stamos's team discovered that Russian hackers appeared to be probing Facebook accounts for people connected to the presidential campaigns, said two employees."[138] *The New York Times* further reports, "Months later, as Mr. Trump battled Hillary Clinton in the general election, the team also found Facebook accounts linked to Russian hackers who were messaging journalists to share information from the stolen emails."[139]

Mr. Stamos, a computer science engineer by academic training, has conducted research, published on the subject of cybersecurity,[140] and occupies by virtue of his tenure at Yahoo the distinction of likely having the most personal hands-on crisis experience with cyberbreaches of major social media enterprises.[141] Mr. Stamos reportedly informed Facebook's general counsel about the Russian hacker discovery, and according to *The New York Times*, "at the time, Facebook had no policy on disinformation or any resources dedicated to searching for it. Mr. Stamos, acting on his own, then directed a team to scrutinize the extent of Russian activity on Facebook."[142] Then, according to *The New York Times*, "In December 2016, after Mr. Zuckerberg publicly scoffed at the idea that fake news on Facebook had helped elect Mr. Trump, Mr. Stamos—alarmed that the company's chief executive seemed unaware of his team's findings—met with Mr. Zuckerberg, Ms. Sandberg and other top Facebook leaders."[143] *The New York Times* reports:

> Ms. Sandberg was angry. Looking into the Russian activity without approval, she said, had left the company exposed legally. Other executives asked Mr. Stamos why they had not been told sooner.
>
> Still, Ms. Sandberg and Mr. Zuckerberg decided to expand on Mr. Stamos's work, creating a group called Project P, for "propaganda," to study false news on the site, according to people involved in the discussions. By January 2017, the group knew that Mr. Stamos's original

[137] Frenkel et al., *supra* note 1.

[138] *Id.*

[139] *Id.*

[140] *See* CENTER FOR NAT'L SEC. & COOPERATION, Stanford U., *Alex Stamos, Adjunct Professor, William J. Perry Fellow, Visiting Scholar Hoover Institution*, https://cisac.fsi.stanford.edu/people/alex-stamos-0.

[141] *See* Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach*, 66 AM. U. L. REV. 1231 (2017).

[142] Frenkel et al., *supra* note 1.

[143] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> team had only scratched the surface of Russian activity on Facebook, and pressed to issue a public paper about their findings.
>
> But Mr. Kaplan and other Facebook executives objected. Washington was already reeling from an official finding by American intelligence agencies that Vladimir V. Putin, the Russian president, had personally ordered an influence campaign aimed at helping elect Mr. Trump.
>
> If Facebook implicated Russia further, Mr. Kaplan said, Republicans would accuse the company of siding with Democrats. And if Facebook pulled down the Russians' fake pages, regular Facebook users might also react with outrage at having been deceived: His own mother-in-law, Mr. Kaplan said, had followed a Facebook page created by Russian trolls. . . .
>
> Throughout the spring and summer of 2017, Facebook officials repeatedly played down Senate investigator's concerns about the company, while publicly claiming there had been no Russian effort of any significance on Facebook.
>
> But inside the company, employees were tracing more ads, pages and groups back to Russia. That June [2017], a reporter for *The New York Times* provided Facebook a list of accounts with suspected ties to Russia, asking about their provenance. By August 2017, Facebook executives concluded that the situation had become what one called a "five-alarm-fire," said a person familiar with the discussions.[144]

Facebook's quarterly meeting of its board of directors on September 6, 2017 proves to be a pivotal moment in the company's disclosure saga. In discharging their duty of care, Facebook directors are required to monitor and be informed.[145]

*The New York Times* reports that Mr. Zuckerberg and Ms. Sandberg, "asked Mr. Stamos and Mr. Stretch [general counsel] to brief the board's audit committee, whose chairman is Erskine Bowles, the patrician investor and White House veteran."[146] According to *The New York Times* account:

> Mr. Stretch and Mr. Stamos went into more detail with the audit committee than planned, warning that Facebook was likely to find even more evidence of Russian interference.

[144] Frenkel et al., *supra* note 1, at A14.

[145] *See* Melvin A. Eisenberg, *The Duty of Care of Corporate Directors and Officers*, 51 U. PITT. L. REV. 945 (1989).

[146] Frenkel et al., *supra* note 1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> The disclosures set off Mr. Bowles, who after years in Washington could anticipate how lawmakers might react. He grilled the two men, occasionally cursing, on how Facebook had allowed itself to become a tool for Russian interference. He demanded to know why it had taken so long to uncover the activity, and why Facebook directors were only now being told.
>
> When the full board gathered later that day, Mr. Bowles pelted questions at Facebook's founder and second-in-command. Ms. Sandberg, visibly unsettled, apologized. Mr. Zuckerberg, stone-faced, whirred through technical fixes, said three people who attended or were briefed on the proceedings.
>
> Later that day the company's abbreviated blog post went up . . . disclosing only that Russian agents had spent roughly $100,000—a relatively tiny sum—on approximately 3,000 ads.
>
> Just one day after the company's carefully sculpted admission, *The Times* published an investigation of further Russian activity on Facebook, showing how Russian intelligence had used fake accounts to promote stolen Democratic emails.[147]

*The New York Times* devotes a considerable amount of ink to a description of how these revelations by Facebook were met with an "infuriated" reception by both Democrats and Republicans in Congress—and "after stalling for weeks, Facebook eventually agreed to hand over the Russian posts to Congress. Twice in October 2017, Facebook was forced to revise its public statements, finally acknowledging that close to 126 million people had seen the Russian posts."[148] Also during October 2017, Senators Klobuchar and Warner "introduced legislation to compel Facebook and other Internet firms to disclose who bought political ads on their sites—a significant expansion of federal regulation over tech companies."[149]

### *G. Global Hate Speech*

*The New York Times* reports, "as Facebook grew, so did the hate speech, bullying and other toxic content on the platform. When researchers and activists in Myanmar, India, Germany and elsewhere warned that Facebook had become an

[147] *Id.*

[148] *Id.*

[149] Frenkel et al., *supra* note 1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

instrument of government propaganda and ethnic cleansing, the company largely ignored them."[150]

Just one of the latest examples of Facebook finding itself in the uncomfortable position of playing a role in a terrorist hate crime takes place on March 15, 2019, as 49 are murdered by a self-proclaimed white supremist gunman in New Zealand.[151] As reported by *The New York Times*, it was "a massacre apparently motivated by white extremist hatred, streamed live on Facebook and calculated to go viral."[152] *The Wall Street Journal* reports, "a Facebook, Inc. spokes-woman said the company removed the video after New Zealand police flagged it, and deleted the Facebook and Instagram accounts belonging to the alleged shooter, Brenton Tarrant, who has been charged with murder."[153] Journalist Yoree Koh reports about the shooting spree that "only 10 people were tuned into [the shooter's] live broadcast of the rampage on Facebook Live, according to archived versions of his page. But the video, which shows dozens of people inside the Al Noor mosque in Christchurch being gunned down, has likely been viewed millions of times in various formats across the Internet."[154] *The Wall Street Journal* states:

> Facebook says it has blocked 1.2 million attempts to repost the footage on its site, while taking down 300,000 more that made it past its filter that screens for such violent content. . . . The Internet allows people with deranged views to find one another and feel like they belong to a movement. Disturbing material that used to exist underground is now a click away.[155]

Social media platforms, including Facebook, "could face new legal issues because of the video, and not only in New Zealand. Prime Minister Jacinda Ardern of New Zealand has vowed to investigate the role that social media played in the attack and to take action, possibly alongside other countries, against the sites that broadcast it."[156] *The Wall Street Journal*'s Dan Gallagher observes, "[w]hile it is

---

[150] *Id.*

[151] *See* Kevin Roose, *A Shooting Disturbingly Rooted in the Internet*, N.Y. TIMES, Mar. 16, 2019, at A1; Damien Cave, *In Mosque Attacks, Quick Action and Courage*, N.Y. TIMES, Mar. 18, 2019, at A1.

[152] Richard Pérez-Peña, *Extremist Hate Fuels New Zealand Massacre*, N.Y. TIMES, Mar. 16, 2019, at A1.

[153] Jon Emont, Georgia Wells & Mike Cherney, *Massacre Roils New Zealand*, WALL ST. J., Mar. 16–17, 2019, at A1.

[154] Yoree Koh, *Why Video of Shooting Endures*, WALL ST. J., Mar. 18, 2019, at A11.

[155] Opinion, *The Internet and Evil*, WALL ST. J., Mar. 21, 2019, at A18.

[156] *See* Charlotte Graham-McLay, *Where Sharing Violent Videos Is Against Law*, N.Y. TIMES, Mar. 22, 2019, at A1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

unclear whether real-time video content is a main draw for Facebook's 2.3 billion users, it has been a central area of investment for the company. The value proposition now seems questionable."[157] For example, just days after the New Zealand event, "AirAsia CEO Tony Fernandes tweeted on Sunday that he closed his Facebook account, which had over half a million followers, as a result of Friday's live video of the Christchurch massacre."[158]

***1. President Trump's Muslim Ban***

Donald Trump's 2016 presidential election campaign was littered with racial slurs.[159] For example, then candidate Trump famously stated, "When Mexico sends its people, they're not sending their best. . . . They're sending people that have lots of problems, and they're bringing those problems with us. They're bringing drugs. They're bringing crime. They're rapists. And some, I assume, are good people."[160] As I have written elsewhere:

> *The Los Angeles Times* has stated, "if we harbor latent racism or if we fear attacks by Muslim extremists, then [Trump] elevates a rumor into a public debate: Was Barack Obama born in Kenya, and is he therefore not really president?" . . . *The Huffington Post* observes that, "Trump's retaliation against the parents of a Muslim U.S. Army officer who died while serving in the Iraq War was a low point in a campaign full of hateful rhetoric." In addition, *The Huffington Post* considers that "the most memorable moment" of the 2016 Democratic National Convention was when "Khizr Khan, the father of the late Army Captain Humayun Khan, spoke out against Trump's bigoted rhetoric and disregard for civil liberties."[161]

***2. How to Treat a President's Hate Speech?***

With respect to Facebook, *The New York Times* reports that candidate Trump, "described Muslim immigrants and refugees as a danger to America, and in

---

[157] Dan Gallagher, *Facebook's Live Video Is A Liability*, WALL ST. J., Mar. 20, 2019, at B12.

[158] *Id.*

[159] *See* Lawrence J. Trautman, *Grab 'Em By the Emoluments: The Crumbling Ethical Foundation of Donald Trump's Presidency*, 17 CONN. PUB. INT. L.J. 1, 31 (2018) [hereinafter Trautman, *Emoluments*] (depicting Mexican and Muslim slurs); Lawrence J. Trautman, *The Twenty-Fifth Amendment: Incapacity and Ability to Discharge the Powers and Duties of Office?*, 67(3) CLEV. ST. L. REV. 373 (2019); Lawrence J. Trautman, *Presidential Impeachment: A Contemporary Analysis*, 44(3) U. DAYTON L. REV. 529 (2019).

[160] Michelle Ye Hee Lee, *Donald Trump's False Comments Connecting Mexican Immigrants and Crime*, WASH. POST (July 8, 2015), https://www.washingtonpost.com/news/fact-checker/wp/2015/07/08/donald-trumps-false-comments-connecting-mexican-immigrants-and-crime/?utm_term=.f87f56b27329.

[161] Trautman, *Emoluments*, *supra* note 159, at 31.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

December 2015 posted a statement on Facebook calling for 'a total and complete shutdown' on Muslims entering the United States."[162] As just one example of Facebook's ability to spread racist speech, "Mr. Trump's call to arms—widely condemned by Democrats and some prominent Republicans—was shared more than 15,000 times on Facebook."[163] According to *The New York Times*:

> Mr. Zuckerberg, who had helped found a nonprofit dedicated to immigration reform, was appalled, said employees who spoke to him or were familiar with the conversation. He asked Ms. Sandberg and other executives if Mr. Trump had violated Facebook's terms of service. . . .
>
> Some at Facebook viewed Mr. Trump's attack on Muslims as an opportunity to finally take a stand against the hate speech coursing through its platform. But Ms. Sandberg, who was edging back to work after the death of her husband several months earlier, delegated the matter to Mr. Schrange and Monika Bickert, a former prosecutor whom Ms. Sandberg had recruited as the company's head of global policy management. . . .
>
> In video conference calls between the Silicon Valley headquarters and Washington, the three officials construed their task narrowly. They parsed the company's terms of service to see if the post, or Mr. Trump's account, violated Facebook's rules.
>
> Mr. Kaplan argued that Mr. Trump was an important public figure and that shutting down his account or removing the statement could be as obstructing free speech, said three employees who knew of the discussions. He also said it could also stoke a conservative backlash.
>
> Mr. Schrage concluded that Mr. Trump's language had not violated Facebook's rules and that the candidate's views had public value. "We were trying to make a decision based on all the legal and technical evidence before us," he said in an interview.
>
> In the end, Mr. Trump's statement and account remained on the site.[164]

[162] Frenkel et al., *supra* note 1.

[163] *Id.*

[164] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

### *H. The CNN Interviews*

The subject of considerable CNN coverage during 2018, including an interview airing on November 21, Mr. Zuckerberg is reported as having "resisted growing calls for changes to Facebook's C-suite, reiterated Facebook's potential as a force for good, and pushed back at some of the unrelenting critical coverage of his company after a year of negative headlines about fake news, election meddling and privacy concerns."[165] When asked, "Did you and other leaders try to minimize Russia's role in spreading propaganda on the platform," Mr. Zuckerberg replied:

> In 2016, there's no doubt that we missed something really important, right? The Russian effort to try to have these coordinated information operations on Facebook and also the Internet and more broadly was not something that we were expecting. Elections are always a very high security event. And we were expecting certain kinds of cyber-attacks.
>
> And we found them, right? The Russians were trying to hack into specific accounts. And we told the people and we told the FBI and all that. But we weren't on top of these coordinating information operations.
>
> So we've spent a lot of the last couple of years now basically building up our systems and strengthening them to be able to address this.
>
> But we've been very focused on this and have invested a lot in it. And anyone who wants to say that upon learning about this we haven't been very focused on trying to both address it and also that we have—I think anyone who says that we haven't made a lot of progress, I just think that that's not right.[166]

[165] Seth Fiegerman, *As Problems Pile Up, Mark Zuckerberg Stands His Ground in Exclusive CNN Business Interview*, CNN BUSINESS (Nov. 21, 2018), https://www.cnn.com/2018/11/20/tech/mark-zuckerberg-interview/index.html.

[166] CNN Newsroom, Transcripts, *Mark Zuckerberg Speaks Out* (Nov. 21, 2018), http://transcripts.cnn.com/TRANSCRIPTS/1811/21/cnr.07.html.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

## VII. THE MUELLER REPORT

> *Russia poses a very serious counterintelligence threat, certainly in the cyber arena, certainly what we call the malign foreign influence territory. Certainly in the presence of foreign intelligence officers in this country. . . .*
>
> *Christopher Wray*
> *FBI Director*
> *April 26, 2019*[167]

In a heavily redacted chapter titled "Russian 'Active Measures' Social Media Campaign," the Mueller Report states, "The first form of Russian election influence came principally from the Internet Research Agency (IRA), a Russian organization . . . conduct[ing] social media operations targeted at large U.S. audiences with the goal of sowing discord in the U.S. political system."[168] Having a goal of influencing global affairs, these activities were known as "active measures."[169] According to the Mueller Report:

> The IRA and its employees began operations targeting the United States as early as 2014. Using fictitious U.S. personas, IRA employees operated social media accounts and group pages designed to attract U.S. audiences. These groups and accounts, which addressed divisive U.S. political and social issues, falsely claimed to be controlled by U.S. activists. Over time, these social media accounts became a means to reach large U.S. audiences. . . .
>
> IRA employees posted derogatory information about a number of candidates in the 2016 U.S. Presidential election. By early to mid-2016, IRA operations included supporting the Trump Campaign and disparaging candidate Hillary Clinton. The IRA made various expenditures to carry out those activities, including buying political advertisements on social media in the name of U.S. persons and entities. . . .
>
> By the end of the 2016 election, the IRA had the ability to reach millions of U.S. persons through their social media accounts. Multiple IRA-controlled

[167] *FBI Director Wray on Global Threats and National Security, Remarks Before Council on Foreign Relations*, C-SPAN (Apr. 26, 2019), https://www.c-span.org/video/?460010-1/fbi-director-christopher-wray-speaks-council-foreign-relations&start=914 [hereinafter *FBI Director Wray on Global Threats*].

[168] THE WASHINGTON POST, SCRIBNER, THE MUELLER REPORT (2019).

[169] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> Facebook groups and Instagram accounts had hundreds of thousands of U.S. participants . . . . In November 2017, a Facebook representative testified that Facebook had identified 470 IRA-controlled Facebook accounts that collectively made 80,000 posts between January 2015 and August 2017. Facebook estimated the IRA reached as many as 126 million persons through its Facebook accounts.[170]

While a more comprehensive and exhaustive discussion of Russian efforts to meddle in the 2016 and 2018 U.S. election process far exceeds the scope and available word count for this single law review article, according to the Mueller Report, "Many IRA operations used Facebook accounts created and operated by its specialists."[171] In addition, "To reach larger U.S. audiences, the IRA purchased advertisements from Facebook that promoted the IRA groups on the newsfeeds of U.S. audience members. According to Facebook, The IRA purchased over 3,500 advertisements, and the expenditures totaled approximately $100,000."[172] The Mueller Report observes:

> Collectively, the IRA's social media accounts reached tens of millions of U.S. persons. Individual IRA social media accounts attracted hundreds of thousands of followers. For example, at the time they were deactivated by Facebook in mid-2017, the IRA's "United Muslims of America" Facebook group had over 300,000 followers, the "Don't Shoot Us" Facebook group had over 250,000 followers, the "Being Patriotic" Facebook group had over 200,000 followers, and the "Secured Borders" Facebook group had over 130,000 followers. According to Facebook, in total the IRA-controlled accounts made over 80,000 posts before their deactivation in August 2017, and these posts reached at least 29 million U.S. persons and "may have reached an estimated 126 million people."[173]

In his April 26, 2019 remarks before the Council on Foreign Relations, FBI Director Christopher Wray describes ongoing Russian Active Measures efforts as "the use of social media, fake news, propaganda, false personas, etc., to spin us up, pit us against each other, sow divisiveness and discord, undermine Americans' faith in democracy . . . is not just an election cycle threat [but] a 365 days-a-year threat

---

[170] *Id.*

[171] *Id.* at 24.

[172] *Id.* at 25.

[173] *Id.* at 26.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

[and] has absolutely continued."[174] The most likely future, Director Wray observes, "We recognize that our adversaries are going to keep adapting and upping their game, so we are viewing 2018 as just a dress rehearsal for 2020 [elections]."[175] During his July 24, 2019 testimony before Congress, former special counsel Robert Mueller states, "over the course of my career, I've seen a number of challenges to our democracy. The Russian government's effort to interfere in our election is among the most serious."[176]

## VIII. FACEBOOK PRIVACY PROBLEMS ESCALATE

> *The historical link between privacy and the forces of wealth creation helps explain why privacy is under siege today. It reminds us, first, that mass privacy is not a basic feature of human existence but a byproduct of a specific economic arrangement—and therefore a contingent and impermanent state of affairs. And it reminds us, second, that in a capitalist country, our baseline of privacy depends on where the money is. And today that has changed.*
>
> *Tim Wu*
> *Julius Silver Professor of Law,*
> *Science and Technology*
> *Columbia Law School*[177]

Facebook privacy issues continue to multiply and constitute a major governance issue. As privacy concerns and social media involvement of foreign powers in U.S. elections becomes more widely publicized during 2018 and 2019, a public relations and communications crisis grows at Facebook.[178] For example, in discussing Facebook's second quarter 2018 earnings announcement, *The Wall Street Journal*'s "Heard on the Street" columnist Dan Gallagher writes, "Facebook said that future growth would slow further, in part because it is giving users more power to keep their data private. That affects its advertising business. The stock plunged after hours following the report."[179] Mr. Gallagher explains, "users and advertisers had continued flocking to it despite a growing number of scandals related to Facebook's

[174] *FBI Director Wray on Global Threats*, *supra* note 167, at 16:28.

[175] *Id.*

[176] Sadie Gurman & Aruna Viswanatha, *Mueller Sticks to His Report, Rejects "Witch Hunt" Rebuke*, WALL ST. J., July 25, 2019, at A1.

[177] Tim Wu, *Opinion, The Way Capitalism Betrayed the Right to Be Left Alone*, N.Y. TIMES, Apr. 14, 2019, at SR3.

[178] Byron Tau, *Big Tech Companies to Testify on Russia*, WALL ST. J., July 26, 2018, at A6.

[179] Dan Gallagher, *Facebook Loses Some of Its Best Customers*, WALL ST. J., July 26, 2018, at B1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

past handling of user data as well as controversies over the powerful role it now plays in news distribution and public discourse."[180] During August 2018, Facebook announced that it dismantled bogus Russian and Iranian pages.[181] Also, about this time, Apple informed Facebook that the Facebook data-security App available at the Apple app store "violated new rules . . . designed to limit data collection by app developers."[182] News accounts surfaced that Facebook had for years sought "users' sensitive financial information."[183] In late September 2018, Facebook had to disclose "hackers gained access to nearly 50 million accounts in what amounts to the largest-ever security breach . . . at a time when it is working to regain the trust of its more than 2 billion users."[184] During November 2018, it was reported that "Facebook failed to prevent its platform from being used to 'foment division and incite offline violence in [Myanmar],'"[185] and that Robert Mercer of Cambridge Analytica "had improperly obtained and exploited Facebook data from as many as 87 million users around the globe."[186] On November 17, 2018 *The New York Times* ran an editorial titled "Facebook Cannot Be Trusted."[187] Another report states, "Mark Zuckerberg gathered about 50 of his top lieutenants . . . and told them that Facebook Inc. was at war and he planned to lead the company accordingly."[188] Other headlines read, "Growth At Any Cost: Top Facebook Executive Defended Data Collection In 2016 Memo—And Warned That Facebook Could Get People Killed";[189] "How Trickery

---

[180] *Id.*

[181] Deepa Seetharaman & Dustin Volz, *Facebook Pulls Fake Iran, Russian Pages*, WALL ST. J., Aug. 22, 2018, at A3; *see also* Farhad Manjoo, *Hack, Hack, Hacking at America's Roots*, N.Y. TIMES, Aug. 23, 2018, at B1.

[182] Deepa Seetharaman, *Facebook Cuts Security App from Apple Store*, WALL ST. J., Aug. 23, 2018, at B4.

[183] AnnaMaria Andriotis & Emily Glazer, *Facebook Sought Users' Financial Data for Years*, WALL ST. J., Sept. 19, 2018, at B1.

[184] Deepa Seetharaman & Robert McMillan, *Facebook Hackers Access Nearly 50 Million Accounts*, WALL ST. J., Sept. 29–30, 2018, at A1.

[185] Alexandra Stevenson, *Facebook Admits Role Platform Had in Fueling Violence in Myanmar*, N.Y. TIMES, Nov. 7, 2018, at B2.

[186] Adam Satariano & Nicholas Confessore, *Watchdog Finds Cambridge Analytica Misused Data*, N.Y. TIMES, Nov. 7, 2018, at B2.

[187] *Facebook Cannot Be Trusted*, Opinion, N.Y. TIMES, Nov. 17, 2018, at A26; *see also* Nicholas Confessore & Matthew Rosenberg, *Top Democrats Voice Distrust of Tech Giants*, N.Y. TIMES, Nov. 18, 2018, at A1.

[188] Deepa Seetharaman, *Zuckerberg's New Leadership Style Sparks Turmoil at Top*, N.Y. TIMES, Nov. 19, 2018, at A1.

[189] Ryan Mac, Charlie Warzel & Alex Kantrowitz, *Growth At Any Cost: Top Facebook Executive Defended Data Collection In 2016 Memo—And Warned That Facebook Could Get People Killed*,



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

Became Part of Playbook For Big Tech."[190] Next came new assertions that Facebook "violated the European Union's new data-privacy law with the way it tracks users' locations."[191] Other negative headlines include: "Facebook Considered Selling Data Access";[192] "Facebook Emails Shed Light on Tactics";[193] "Facebook's Emails Tell A Cutthroat Tale: No Gentle Giant, But a Juggernaut Playing Hardball";[194] "Facebook's Emails Tell A Cutthroat Tale: Leveraging User Data To Show Favoritism Among Its Partners";[195] "Facebook Censors at Random";[196] "Facebook's in the News, And No, It's Not Good";[197] "Facebook Criticized For Betraying Users' Data";[198] "Washington, D.C., Sues Facebook Over Privacy";[199] "Russian Trolls Hit U.S. Businesses";[200] "Why Privacy At Facebook Is Eyed Anew By the F.T.C.";[201] and "How Facebook Controls What World Can Say."[202]

---

BUZZFEED NEWS (Mar. 29, 2018), https://www.buzzfeednews.com/article/ryanmac/growth-at-any-cost-top-facebook-executive-defended-data.

[190] Jack Nicas, *How Trickery Became Part of Playbook for Big Tech*, N.Y. TIMES, Nov. 22, 2018, at B1; *see also* Deepa Seetharaman, *Soros Aide Urges Facebook Review*, WALL ST. J., Nov. 23, 2018, at B4.

[191] Daniel Michaels & Stu Woo, *Europe Fires on Google, Facebook*, WALL ST. J., Nov. 28, 2018, at B4; *see also* Adam Satariano, *Zuckerberg Snubs a Multinational Inquiry into Facebook's Practices*, N.Y. TIMES, Nov. 28, 2018, at B3.

[192] Deepa Seetharaman & Kirsten Grind, *Facebook Considered Selling Data Access*, WALL ST. J., Nov. 29, 2018, at B1.

[193] Deepa Seetharaman & Stu Woo, *Facebook Emails Shed Light on Tactics*, WALL ST. J., Dec. 6, 2018, at B1.

[194] Kevin Roose, *Facebook's Emails Tell A Cutthroat Tale: No Gentle Giant, but a Juggernaut Playing Hardball*, N.Y. TIMES, Dec. 6, 2018, at B1.

[195] Adam Satariano & Mike Isaac, *Facebook's Emails Tell A Cutthroat Tale: Leveraging User Data to Show Favoritism Among Its Partners*, N.Y. TIMES, Dec. 6, 2018, at B1.

[196] Daniel Gallant, *Opinion, Facebook Censors at Random*, WALL ST. J., Dec. 10, 2018, at A17.

[197] Brian X. Chen, *Facebook's in the News, And No, It's Not Good*, N.Y. TIMES, Dec. 10, 2018, at B7.

[198] Michael LaForgia, Nicholas Confessore & Gabriel J.X. Dance, *Facebook Criticized for Betraying Users' Data*, N.Y. TIMES, Dec. 20, 2018, at B1.

[199] Sheera Frenkel & Matthew Rosenberg, *Washington, D.C., Sues Facebook Over Privacy*, N.Y. TIMES, Dec. 20, 2018, at B3.

[200] Shelby Holliday & Rob Berry, *Russian Trolls Hit U.S. Businesses*, WALL ST. J., Dec. 22–23, 2018, at A4.

[201] Natasha Singer, *Why Privacy at Facebook Is Eyed Anew by the F.T.C.*, N.Y. TIMES, Dec. 24, 2018, at B1.

[202] Max Fisher, *How Facebook Controls What World Can Say*, N.Y. TIMES, Dec. 28, 2018, at A1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

With the start of 2019, Facebook continued to suffer from negative news headlines, such as: "Suicide Watch On Facebook Raises Issues";[203] "2nd Effort at Social Media Fakery Is Uncovered in Alabama Race";[204] "See You in Court, Facebook";[205] "Facebook Deletes Pages of Russian Propaganda";[206] "F.T.C. Is Said To Consider Hefty Fines For Facebook";[207] "Questions Persist About a Viral Video Perfect Storm";[208] "Calculating How Much of Facebook Is Phony";[209] "Germany Moves to Rein In Facebook Data Gathering";[210] "When Facebook Spread Lies, a German Cop Spread Truth";[211] "Facebook labelled 'digital gangsters' by report on fake news";[212] "New York Governor Orders Probe Into Facebook Access to Data From Other Apps";[213] "You Give Apps Sensitive Personal Information. Then They Tell Facebook";[214] "Apps Send User Secrets to Facebook";[215] "Probe Seeks Facebook Data Documents";[216] "Criminal Investigation Digs Into Facebook's Data-

[203] Natasha Singer, *Suicide Watch on Facebook Raises Issues*, N.Y. TIMES, Jan. 1, 2019, at A1.

[204] Scott Shane & Alan Blinder, *2nd Effort at Social Media Fakery Is Uncovered in Alabama Race*, N.Y. TIMES, Jan. 7, 2019, at A1.

[205] Neema Singh Guliani, *See You in Court, Facebook*, Opinion, N.Y. TIMES, Jan. 7, 2019, at A23.

[206] Adam Satariano, *Facebook Deletes Pages of Russian Propaganda*, N.Y. TIMES, Jan. 18, 2019, at B4.

[207] Cecilia Kang, *F.T.C. Is Said to Consider Hefty Fines for Facebook*, N.Y. TIMES, Jan. 19, 2019, at B1.

[208] Sheera Frenkel, *Questions Persist About a Viral Video Perfect Storm*, This Week in Tech, N.Y. TIMES, Jan. 28, 2019, at B3.

[209] Jack Nicas, *Calculating How Much of Facebook Is Phony*, N.Y. TIMES, Jan. 31, 2019, at B1.

[210] Natasha Singer, *Germany Moves to Rein in Facebook Data Gathering*, N.Y. TIMES, Feb. 8, 2019, at B1.

[211] Max Fisher & Amanda Taub, *When Facebook Spread Lies, a German Cop Spread Truth*, N.Y. TIMES, Feb. 13, 2019, at A7.

[212] David Pegg, *Facebook Labelled 'Digital Gangsters' by Report on Fake News*, GUARDIAN (Feb. 17, 2019), https://www.theguardian.com/technology/2019/feb/18/facebook-fake-news-investigation-report-regulation-privacy-law-dcms.

[213] Jonathan Stempel & Katie Paul, *New York Governor Orders Probe into Facebook Access to Data from Other Apps*, REUTERS (Feb. 22, 2019), https://www.reuters.com/article/us-facebook-new-york/new-york-governor-orders-probe-into-facebook-access-to-data-from-other-apps-idUSKCN1QB2AJ.

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

[215] Sam Schechner & Mark Secada, *Apps Send User Secrets to Facebook*, WALL ST. J., Feb. 23–24, 2019, at A1.

[216] Sam Schechner, *Probe Seeks Facebook Data Documents*, WALL ST. J., Mar. 1, 2019, at B4.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

Sharing Deals";[217] "Facebook Stored Users' Passwords Improperly";[218] "Fake News Roils WhatsApp in India";[219] "Facebook's Zuckerberg Is Making Enemies, Not Friends";[220] "Facebook's Scandal of Fake celebrity News";[221] "Regulators Everywhere Are Circling Facebook: Fines, constraints and penalties for Zuckerberg are on the table";[222] "Call for Easter Attack Stayed on Facebook";[223] and many, many more.

The Federal Trade Commission (FTC) lists 450 pages of correspondence between Facebook and the FTC for the period March 10, 2011 through March 20, 2018.[224] As this article nears completion during late 2019, *The New York Times* reports that, "After Facebook was hit. . . with a fine of around $5 billion for privacy violations, critics immediately said it escaped largely unscathed: The settlement neither bruised its bottom line nor severely restricted its ability to collect people's data."[225] Facebook reported that "it was setting aside $3 billion to pay for any potential settlement with the FTC";[226] now, "regulators and lawmakers in Washington, Europe and in countries including Canada have already begun multiple investigations and proposing new restrictions against Facebook that will probably embroil it in policy debates and legal wrangling for years to come."[227] This follows

---

[217] Michael LaForgia, Matthew Rosenberg & Gabriel J.X. Dance, *Criminal Investigation Digs into Facebook's Data-Sharing Deals*, N.Y. TIMES, Mar. 14, 2019, at A1.

[218] Jeff Horwitz & Robert McMillan, *Facebook Stored Users' Passwords Improperly*, WALL ST. J., Mar. 22, 2019, at A1.

[219] Newley Purnell, *Fake News Roils WhatsApp in India*, WALL ST. J., Apr. 1, 2019, at A1.

[220] Laura Forman, *Facebook's Zuckerberg Is Making Enemies, Not Friends*, WALL ST. J., Apr. 2, 2019, at B12.

[221] Mehmet Oz & Kai Falkenberg, Opinion, *Facebook's Scandal of Fake Celebrity News*, WALL ST. J., Apr. 15, 2019, at A15.

[222] Cecilia Kang & Adam Satariano, *Regulators Everywhere Are Circling Facebook: Fines, Constraints and Penalties for Zuckerberg are on the Table*, N.Y. TIMES, Apr. 26, 2019, at B1.

[223] Newley Purnell, *Call for Easter Attack Stayed on Facebook*, WALL ST. J., May 1, 2019, at A7.

[224] FED. TRADE COMM'N, COMMUNICATIONS BETWEEN FTC AND FACEBOOK, March 10, 2011 through March 20, 2018 (2018), https://www.ftc.gov/about-ftc/foia/frequently-requested-records/facebook.

[225] Adam Satariano, *Facebook Misses Out on a Bullet, But Not Pain*, N.Y. TIMES (July 15, 2019), https://www.nytimes.com/2019/07/13/technology/facebook-privacy-investigations.html; *see also* Celilia Kang, *Facebook Fine Could Total Billions If F.T.C. Talks Lead to a Deal*, N.Y. TIMES (Feb. 14, 2019), https://www.nytimes.com/2019/02/14/technology/facebook-ftc-settlement.html.

[226] Brent Kendall & John D. McKinnon, *FTC Ruling on Facebook Probe Looms Over Big Tech*, WALL ST. J., Apr. 26, 2019, at A2; *see also* Mike Isaac & Cecilia Kang, *Hefty Penalty for Facebook Over Privacy*, N.Y. TIMES, Apr. 25, 2019, at A1.

[227] Adam Satariano, *Facebook Misses Out on a Bullet, But Not Pain*, N.Y. TIMES (July 15, 2019), https://www.nytimes.com/2019/07/13/technology/facebook-privacy-investigations.html.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

a 2011 agreement where Facebook "agreed to settle charges that it had deceived consumers on privacy."[228]

By late March 2019, Facebook is accused of violating the Fair Housing Act.[229] Additional unauthorized Facebook user records continue to surface.[230] *The Wall Street Journal* reports "the U.K. government plans to create a regulatory body to force the removal of harmful content from the Internet, one of the most far-reaching proposals from a host of countries trying to put a tighter leash on global technology companies."[231] New global regulations now seem a certainty.[232] During mid-year 2019, additional negative headlines abound: criticizing Facebook's "unintended consequences";[233] continued front page coverage about the F.T.C.'s likely landmark penalty;[234] co-founder Chris Hughes advocates a Facebook break-up;[235] "Tech Backlash Puts Silicon Valley on Edge";[236] "To Curb Online Bullying, Instagram Has to Spot It";[237] "For Sale on Facebook: 'Loot to Order' Antiquities From War

[228] Natasha Singer, *Why the F.T.C. Is Taking a New Look at Facebook Privacy*, N.Y. TIMES (Dec. 22, 2018), https://www.nytimes.com/2018/12/22/technology/facebook-consent-decree-details.html.

[229] Katie Benner, Glenn Thrush & Mike Isaac, *U.S. Claims Ad Practices at Facebook Discriminate*, N.Y. TIMES, Mar. 29, 2019, at B1; Josh D. McKinnon & Jeff Horwitz, *Facebook Accused of Aiding Bias in Housing*, WALL ST. J., Mar. 29, 2019, at A1.

[230] *See* Sarah Frier, Matt Day & Josh Eidelson, *Millions of Facebook Records Found on Amazon Cloud Servers*, BLOOMBERG (Apr. 3, 2019, 1:23 PM), https://www.bloomberg.com/news/articles/2019-04-03/millions-of-facebook-records-found-on-amazon-cloud-servers.

[231] *See* Sam Schechner & Parmy Olson, *U.K. Tightens Hold on Social Media*, WALL ST. J., Apr. 8, 2019, at B4.

[232] *See* Jamie Condliffe, *Who Will Write the Rules for Big Tech?*, N.Y. TIMES, Apr. 8, 2019, at B5; *see also* Sam Schechner, *Facebook Bends to EU Demands*, WALL ST. J., Apr. 19, 2019, at B3; *see also* Maya Uppaluru, *The U.S. Needs a New Paradigm for Data Governance*, HARV. BUS. REV. (Apr. 16, 2018), https://hbr.org/2018/04/the-u-s-needs-a-new-paradigm-for-data-governance.

[233] Bret Stephens, Opinion, *Facebook's Unintended Consequences*, N.Y. TIMES, May 4, 2019, at A19.

[234] Cecilia Kang, *A Severe Penalty Awaits Facebook, But How Severe?*, N.Y. TIMES, May 5, 2019, at A1.

[235] Chris Hughes, Opinion, *It's Time to Break Up Facebook*, N.Y. TIMES (May 9, 2019), https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html.

[236] Robert McMillan & Jeff Horowitz, *Tech Backlash Puts Silicon Valley on Edge*, WALL ST. J., May 10, 2019, at B4.

[237] Kevin Roose, *To Curb Online Bullying, Instagram Has to Spot It*, N.Y. TIMES, May 10, 2019, at B1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

Zones";[238] "How Hackers Broke Whatsapp With Just a Phone Call";[239] "Facebook Privacy Settlement Delayed";[240] "Pelosi Says Facebook Enabled Russian Interference in Election";[241] "Tech Titans Face Tough Scrutiny From All Sides: Apple, Google, Facebook and Amazon May Face Inquiries";[242] "Tech Titans Build Lobbyist Army, Trying to Repel Threats to Power";[243] "Facebook Bolsters Antitrust Defenses";[244] "Overthrow the Prince of Facebook";[245] "When Free Is Too High A Price: Most Ills from Facebook and Google Trace Back to Their No-cost Models";[246] "Emails Stoke Worry at Facebook Amid Probe";[247] "Report Points Finger at Russia Over E.U. Vote Disinformation";[248] "Facebook Turns to Ads for Image Repair";[249] "Refugees Discover There's No Escape From Facebook";[250] "Suddenly, an Interest in Tech Antitrust";[251] "Reprimands Of Big Tech Cross Aisle";[252] "Justice Dept. Is

[238] Karen Zraick, *For Sale on Facebook: 'Loot to Order' Antiquities from War Zones*, N.Y. TIMES, May 10, 2019, at A10.

[239] Lily Hay Newman, *How Hackers Broke WhatsApp With Just a Phone Call*, WIRED (May 14, 2019), https://www.wired.com/story/whatsapp-hack-phone-call-voip-buffer-overflow/.

[240] John D. McKinnon, *Facebook Privacy Settlement Delayed*, WALL ST. J., May 25, 2019, at A2.

[241] Cecilia Kang, *Pelosi Says Facebook Enabled Russian Interference in Election*, N.Y. TIMES, May 30, 2019, at B4.

[242] Cecilia Kang, David Streitfeld & Annie Karni, *Tech Titans Face Tough Scrutiny from All Sides: Apple, Google, Facebook and Amazon May Face Inquiries*, N.Y. TIMES, June 4, 2019, at A1.

[243] Cecilia Kang & Kenneth P. Vogel, *Tech Titans Build Lobbyist Army, Trying to Repel Threats to Power*, N.Y. TIMES, June 6, 2019, at A1.

[244] *See* Deepa Seetharaman & Jeff Horowitz, *Facebook Bolsters Antitrust Defenses*, WALL ST. J., June 7, 2019, at B1.

[245] Peggy Noonan, Opinion, *Overthrow the Prince of Facebook*, WALL ST. J., June 8–9, 2019, at A15.

[246] Christopher Mimms, *When Free Is Too High A Price: Most Ills from Facebook and Google Trace Back to Their No-cost Models*, WALL ST. J., June 8–9, 2019, at B1.

[247] John D. McKinnon, Emily Glazer, Deepa Seetharaman & Jeff Horwitz, *Emails Stoke Worry at Facebook Amid Probe*, WALL ST. J., June 13, 2019, at A1.

[248] Adam Satariano, *Report Points Finger at Russia Over E.U. Vote Disinformation*, N.Y. TIMES, June 15, 2019, at A1.

[249] Alexandra Bruell, *Facebook Turns to Ads for Image Repair*, WALL ST. J., June 15, 2019, at B3.

[250] Vindu Goel & Shaikh Azizur Rahman, *Refugees Discover There's No Escape from Facebook*, N.Y. TIMES, June 15, 2019, at B1.

[251] Jim Kerstetter & Pui-Wing Tam, *Suddenly, an Interest in Tech Antitrust*, N.Y. TIMES, June 17, 2019, at B3.

[252] Steve Lohr, Mike Isaac & Nathaniel Popper, *Reprimands of Big Tech Cross Aisle*, N.Y. TIMES, July 17, 2019, at B1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

Set to Put Internet Giants Under Antitrust Scrutiny";[253] "Zuckerberg Is Required to Certify Compliance";[254] "Privacy Flaw Found in Facebook App";[255] "Facebook Settles in 2 Inquiries. Now For Round 3: After Fines Over Data, a New Antitrust Investigation";[256] "Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data";[257] "Facebook Brand Value Falls Again";[258] "Zuckerberg Says Facebook Won't Police Political Speech";[259] and "Dissent Erupts at Facebook."[260]

### *A. Litigation Starts*

The Delaware Court of Chancery Vice Chancellor, Joseph R. Slights III, observes that numerous lawsuits have been filed against Facebook, "some as direct consumer class actions, some as government enforcement actions and some as derivative actions against Facebook fiduciaries—alleging that Facebook's implementation of a business model that exposed private user data to unauthorized third-party access has caused harm to consumers and harm to the Company."[261] For

---

[253] Daisuke Wakabayashi, Katie Benner & Steve Lohr, *Justice Dept. Is Set to Put Internet Giants Under Antitrust Scrutiny*, N.Y. TIMES, July 24, 2019, at A1.

[254] Ryan Tracy & John D. McKinnon, *Facebook Settlement Requires Mark Zuckerberg to Certify Privacy Protections*, WALL ST. J. (July 23, 2019, 8:32 PM), https://www.wsj.com/articles/facebook-settlement-requires-mark-zuckerberg-to-certify-compliance-11563923987.

[255] Sarah E. Needleman, *Flaw in Facebook's Messenger Kids Exposed Children to Unauthorized Chats*, WALL ST. J. (July 24, 2019, 11:14 AM), https://www.wsj.com/articles/flaw-in-facebooks-messenger-kids-exposed-children-to-unauthorized-chats-11563894874.

[256] Mike Isaac & Natasha Singer, *Facebook, Penalized in 2 Inquiries, Faces a 3rd*, N.Y. TIMES, July 25, 2019, at A1.

[257] Press Release, Sec. & Exch. Comm'n, Facebook to Pay $100 Million for Misleading Investors About the Risks It Faced From Misuse of User Data (July 24, 2019) (on file with author), https://www.sec.gov/news/press-release/2019-140.

[258] Nat Ives, *Amazon Surges and Facebook Falls Again in Report on Brand Value*, WALL ST. J. (Oct. 16, 2019, 7:00 PM), https://www.wsj.com/articles/amazon-surges-and-facebook-falls-again-in-report-on-brand-value-11571266801.

[259] Cecilia Kang & Mike Isaac, *Zuckerberg Says Facebook Won't Police Political Speech*, N.Y. TIMES, Oct. 18, 2019, at B1.

[260] Mike Isaac, *Dissent Erupts at Facebook*, N.Y. TIMES, Oct. 29, 2019, at B1.

[261] *See In re* Facebook, Inc. Sec. 220 Litig., CV 2018-0661-JRS, 2019 WL 2320842, at *8 (Del. Ch. May 30, 2019), *as revised* (May 31, 2019), *judgment entered sub nom*. *In re* Facebook, Inc., (Del. Ch. 2019) [hereinafter Opinion by Vice Chancellor Slights] (citing *e.g.*, Sbriglio v. Zuckerberg, C.A. No. 2018-0307-JRS (derivative action in Delaware); Leagre v. Zuckerberg, C.A. No. 2018-0675-JRS; *In re* Facebook, Inc., Consumer Privacy User Profile Litig., C.A. No. 3:18-md02843 (a multidistrict privacy litigation in the U.S. District Court in the Northern District of California); Yuan v. Facebook, Inc. et al., C.A. No. 3:18-cv-01725 (a federal securities action pending in the U.S. District Court in the Northern District of California); District of Columbia v. Facebook, Inc., C.A. No. 2018-CA-008715 (a consumer class action brought by the United States Government pending in the District of Columbia); State of Illinois *ex rel.* Foxx v. Facebook Inc. et al., Case No. 2018-CH-03868 (Cook Cty. Cir. Ct.) (a consumer action brought by the Cook County State's Attorney in Illinois).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

the benefit of privacy scholars and policymakers, Vice Chancellor Slight's § 220 analysis, where he concludes that "Plaintiffs Have Demonstrated Proper Purposes for Inspection," is included here as follows:

> The preponderance of the evidence presented at trial provides a credible basis to infer the Board and Facebook senior executives failed to oversee Facebook's compliance with the Consent Decree and its broader efforts to protect the private data of its users. I summarize that evidence below.
>
> *First*, Plaintiffs presented the Parliamentary Report where, after summarizing emails, meeting minutes, witness interviews and other evidence, the Parliamentary Committee concluded the "Cambridge Analytica Scandal was facilitated by Facebook's policies and the incident displays the fundamental weakness of Facebook in managing its responsibilities to the people whose data is used for its own Commercial purposes." According to the Parliamentary Report,
>
> "[i]f [Facebook] had fully complied with the [Consent Decree], [the Cambridge Analytica scandal] . . . would not have happened." The Parliamentary Report went on to summarize evidence that Facebook had implemented a business plan to override its users' privacy settings in order to transfer data to some app developers' and "to charge high prices . . . for the exchange of that data." And, importantly, the Parliamentary Report concluded that the Board was aware of data privacy breaches but attempted "to deflect attention" from these breaches to avoid scrutiny.
>
> *Second*, the Consent Decree demonstrates that an enforceable regulatory order mandated that the Company's management and its Board implement and monitor Facebook's compliance with specifically identified and detailed data privacy procedures. Lest there be any doubt about whether the Board was aware of the specific requirements of the Consent Decree, the document itself makes clear that it is to be "deliver[ed] . . . to . . . all current and future principals, officers, directors, and managers[.]" While there is certainly room to defend the claim, there is some evidence the Board knew of the Company's obligations to implement data security measures, knew the Company had not implemented or maintained those measures as required by the Consent Decree and, nevertheless, condoned the Company's monetization of its users' private data in violation of the Consent Decree. The Consent Decree was an affirmative obligation imposed on the Company much like positive law. The legal academy has observed that Delaware courts are more inclined to find Caremark oversight liability at the board level when



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> the company operates in the midst of obligations imposed upon it by positive law yet fails to implement compliance systems, or fails to monitor existing compliance systems, such that a violation of law and resulting liability occurs. Professor Elizabeth Pollman aptly describes this as a circumstance where the board acts with "disobedience." Our law does not countenance board level disobedience. Stated differently, Delaware law does not charter law breakers. Delaware law allows corporations to pursue diverse means to make a profit, subject to a critical statutory floor, which is the requirement that Delaware corporations only pursue "lawful business" by "lawful acts." As a result, a fiduciary of a Delaware corporation cannot be loyal to a Delaware corporation by knowingly causing it to seek profit by violating the law . . . . Telling your parents that all the kids are getting caught shoplifting, cheating, or imbibing illegal substances is not, fortunately, a good excuse. For fiduciaries of Delaware corporations, there is no room to flout the law governing the corporation's affairs. If the fiduciaries of a Delaware corporation do not like the applicable law, they can lobby to get it changed. But until it is changed, they must act in good faith to ensure that the corporation tries to comply with its legal duties. Plaintiffs have presented a credible basis to infer that the Board acted with disobedience by allowing Facebook to violate the Consent Decree. They are entitled to inspect books and records to investigate that potential wrongdoing.
>
> *Third*, Plaintiffs point to information released to the public sphere since they initiated their Demand indicating that a key component of Facebook's business plan was to monetize access to user data through agreements with partners based on "reciprocity," even after entering into the Consent Decree. Facebook's long-term business model was to "go with full reciprocity and access to app friends," permitting business partners to obtain full information from users, including users' Facebook friends. There is some evidence Facebook whitelisted these business partners, giving them unauthorized access to the Facebook platform and Facebook's user data for a substantial fee. All the while, its users were left in the dark.
>
> *Fourth*, Plaintiffs presented a credible basis to infer the Board knew the Company was allowing unauthorized third-party access to user data. The New York Times reported Erskine Bowles, chairman of the Audit Committee, received a report from Stamos, then Chief Information Security Officer, and Colin Stretch, Facebook's General Counsel, about Russian interference with the Facebook platform and potential data privacy violations. On the same day, Bowles questioned Zuckerberg and Sandberg at a full Board meeting



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

regarding the extent to which they, and other Facebook senior management, had been transparent with the Board regarding data privacy issues. At that meeting, Stamos expressed concerns that the Company had not monitored the protection of user data carefully, prompting Sandberg, as noted above, to accuse Stamos of "throw[ing] us under the bus!" According to The New York Times, the Company's failure adequately to address data privacy ultimately led Whatsapp co-founder, Jan Koum, to resign from the Board.

*Fifth*, Plaintiffs have provided evidence that multiple regulatory authorities have opened investigations into Facebook's data privacy lapses. Perhaps most troubling, following the Cambridge Analytica breach, the FTC opened an investigation to determine the extent to which Facebook violated the Consent Decree. News outlets have recently reported the investigation could result in a multibillion dollar fine against Facebook—the largest fine ever imposed by the FTC.

After the Cambridge Analytica scandal, the ICO fined Facebook the maximum fine permitted under British law, £500,000, for permitting third party developers to access user information without sufficient consent. In addition, the Parliamentary Report revealed the ICO concluded that Facebook's "business practices and the way applications interact with data on the platform have contravened data protections law."

*Finally*, Facebook is subject to numerous lawsuits based on the same underlying misconduct. These complaints further support Plaintiffs' credible basis to infer wrongdoing.

In light of the low Section 220 evidentiary threshold, I am satisfied Plaintiffs have proven "legitimate issues of wrongdoing." [internal citations omitted][262]

[262] *See* Opinion by Vice Chancellor Slights, *supra* note 261, at 39 (citing James D. Cox & Randall S. Thomas, *Corporate Darwinism: Disciplining Managers in a World With Weak Shareholder Litigation*, 95 N.C. L. REV. 19, 55–56 (2016)); Donald C. Langevoort, *Caremark and Compliance: A Twenty-Year Lookback*, 90 TEMP. L. REV. 727, 735 (2018); Elizabeth Pollman, *Corporate Disobedience*, 68 DUKE L.J. 709, 756 (2019).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

### *B. Proposed Cryptocurrency Libra*

On June 18, 2019 Facebook announced a new digital currency named Libra, along with a digital wallet called Calibra.[263] *The Guardian* reports that Libra is described "as a means to connect people who do not have access to traditional banking platforms. With close to 2.4 billion people using Facebook each month, Libra could be a financial game changer, but will face close scrutiny as Facebook continues to reel from a series of privacy scandals."[264] Soon after Facebook's announcement, Jerome H. Powell, chair of the Federal Reserve said the U.S. central bank had "serious concerns" about Libra.[265] Other negative headlines read "Facebook Confronts Broad Resistance to Crypto Plans,"[266] "The Trouble Starts If Facebook's New Currency Succeeds;"[267] and "Facebook, Grilled By Lawmakers, Defends Cryptocurrency."[268] During hearings held before the House Committee on Financial Services on July 17, 2019, on "Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System," Georgetown University Law Professor Chris Brummer testified that:

> - The Libra White Paper fails, most fundamentally, to inform potential holders in unambiguous terms that they can lose money, and that runs on the coin are possible.
> - The White Paper fails to clearly disclose that Libra holders will be exposed to counterparty risk in the form of mismanagement of reserve investments.
> - The White Paper fails to disclose governance risks, including the negative impact Libra Association decisions, and conflicts of interest, could have on the nature and value of Libra coins.

---

[263] Press Release, Facebook, Inc., Coming in 2020: Calibra (June 18, 2019) (on file with author), https://newsroom.fb.com/news/2019/06/coming-in-2020-calibra/.

[264] Kari Paul, *Libra: Facebook Launches Cryptocurrency in Bid to Shake Up Global Finance*, THE GUARDIAN, (June 18, 2019, 5:00 AM), https://www.theguardian.com/technology/2019/jun/18/libra-facebook-cryptocurrency-new-digital-money-transactions.

[265] Alan Rappeport & Nathaniel Popper, *Trump Administration Warns of Threats with Cryptocurrencies*, N.Y. TIMES, July 16, 2019, at B3.

[266] Dave Michaels, Kate Davidson & Sam Schechner, *Facebook Confronts Bipartisan Resistance to Cryptocurrency Plans*, WALL ST. J. (July 16, 2019, 10:14 AM), https://www.wsj.com/articles/facebook-says-libra-cryptocurrency-to-be-regulated-by-swiss-financial-authorities-11563208951.

[267] Eric Posner, *The Trouble Starts If Facebook's New Currency Succeeds*, THE ATLANTIC (June 25, 2019), https://www.theatlantic.com/ideas/archive/2019/06/dont-trust-libra-facebooks-new-cryptocurrency/592450/.

[268] Nathaniel Popper & Mike Isaac, *Facebook, Grilled by Lawmakers, Defends Cryptocurrency*, N.Y. TIMES, July 18, 2019, at B3.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

- The White Paper fails to disclose how the decentralized application interfaces it is envisioning could compromise the "secure, scalable, and reliable blockchain" Facebook is promising, as well as AML compliance and cybersecurity.
- Depending on how the White Paper is interpreted, Libra potentially comprises a source of systemic risk.[269]

Columbia Law Professor Katharina Pistor warns, "existing legal and regulatory frameworks . . . were not designed to govern digital currencies . . . [and] Many of the activities associated with managing Libra and its reserve will be beyond the reach of regulators in the United States, or any other country for that matter."[270] Former Chairman of the U.S. Commodity Futures Trading Commission, Under Secretary of the Treasury for Domestic Finance, and assistant Secretary of the Treasury, Gary Gensler states, "Facebook's Libra proposal comes in the midst of important public policy debates on how best to protect consumers and their data privacy in the face of rapidly advancing technologies and data analytics."[271]

## IX. RECOMMENDATIONS FOR CORRECTIVE ACTION

> *Although there is nothing unusual about the prospect of capitalist enterprises seeking every kind of knowledge advantage in a competitive marketplace, the surveillance capitalist capabilities that translate ignorance into knowledge are unprecedented. . . surveillance capital derives from the dispossession of human experience, operationalized in its unilateral and pervasive programs of rendition: our lives are scraped and sold to fund their*

[269] *Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System: Hearing Before the H. Comm. on Fin. Servs.*, 116th Cong. (2019) (statement of Chris Brummer, Professor of Law, Georgetown University), https://docs.house.gov/meetings/BA/BA00/20190717/109821/HHRG-116-BA00-Wstate-BrummerC-20190717.pdf.

[270] *Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System Before the H. Comm. on Fin. Servs.*, 116th Cong. (2019) (statement of Katharina Pistor, Law Professor, Columbia Law School), https://docs.house.gov/meetings/BA/BA00/20190717/109821/HHRG-116-BA00-Wstate-PistorK-20190717-U1.pdf.

[271] *Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System Before the H. Comm. on Fin. Servs.*, 116th Cong. (2019) (statement of Gary Gensler, Professor of Practice, MIT Sloan School of Management); *see also* AnnaMaria Andriotis, Peter Rudegeair & Liz Hoffman, *Inside Facebook's Botched Bid to Launch a New Currency*, WALL ST. J., Oct. 17, 2019, at A1; Cecilia Kang & Nathaniel Popper, *Facebook Sticks to a Full-Court Press on Libra*, N.Y. TIMES, Oct. 22, 2019, at B1; Peter Rudegair & Ryan Tracy, *Facebook Chief Stands Firm on Plans for Libra*, WALL ST. J., Oct. 24, 2019, at B1.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> *freedom and our subjugation, their knowledge and our ignorance about what they know.*
>
> *Soshana Zuboff*
> *The Charles Edward Wilson*
> *Professor Emerita*
> *Harvard Business School*
> *2019*[272]

### *A. NIST Privacy Framework*

As this manuscript nears completion, the voluntary NIST Privacy Framework is still in discussion draft stage.[273] The *Core* of the *Framework* is designed to promote "communicating prioritized privacy protection activities and outcomes across the organization," and "consists of five concurrent and continuous functions—Identify, Protect, Control, Inform, and Respond."[274] Upon completion, it seems likely that the "Privacy Framework" may have a major influence on future privacy legislation.[275]

### *B. Proposed Internet Bill of Rights*

Kara Swisher, journalist for *The New York Times* writes, "it has become ever clearer with every misstep—including but not limited to Russian Interference on social media platforms, the amplification of hate speech and fake news, and the misuse of personal information—that tech's freedom has come at a steep price to the American people."[276] Sir Tim Berners-Lee, credited as "the inventor of the world wide web and founder of the Web Foundation" states:

> If the Internet is to live up to its potential as a force for good in the world, we need safeguards that ensure fairness, openness and human dignity. This bill of rights provides a set of principles that are about giving users more control of their online lives while creating a healthier Internet economy. This is a bipartisan issue with broad public support, giving leaders an opportunity to work together to make the Internet work for everyone.[277]

---

[272] *See* ZUBOFF, *supra* note 48, at 498.

[273] NAT'L INST. OF STDS. & TECH., DISCUSSION DRAFT, NIST PRIVACY FRAMEWORK: AN ENTERPRISE RISK MANAGEMENT TOOL (Apr. 30, 2019) [hereinafter NIST Privacy Framework], https://www.nist.gov/system/files/documents/2019/04/30/nist-privacy-framework-discussion-draft.pdf.

[274] *Id.* at 4.

[275] *See* NIST Privacy Framework, *supra* note 273.

[276] Kara Swisher, Opinion, *Introducing the Internet Bill of Rights*, N.Y. TIMES (Oct. 4, 2018), https://www.nytimes.com/2018/10/04/opinion/ro-khanna-internet-bill-of-rights.html.

[277] Press Release, Office of Representative Ro Khanna, Rep. Khanna Releases "Internet Bill of Rights" Principles, Endorsed by Sir Tim Berners-Lee (Oct. 4, 2018), https://khanna.house.gov/media/press-releases/release-rep-khanna-releases-internet-bill-rights-principles-endorsed-sir-tim.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

Representing the 17th District of California, which covers communities in Silicon Valley, U.S. Congressman Ro Khanna introduced the following set of principles for an Internet Bill of Rights:

> You should have the right:
>
> (1) To have access to and knowledge of all collection and uses of personal data by companies;
>
> (2) To opt-in consent to the collection of personal data by any party and to the sharing of personal data with a third party;
>
> (3) Where context appropriate and with a fair process, to obtain, correct, or delete personal data controlled by any company and to have those requests honored by third parties;
>
> (4) To have personal data secured and to be notified in a timely manner when a security breach or unauthorized access of personal data is discovered;
>
> (5) To move all personal data from one network to the next;
>
> (6) To access and use the [I]nternet without [I]nternet service providers blocking, throttling, engaging in paid prioritization, or otherwise unfairly favoring content, applications, services, or devices.
>
> (7) To [I]nternet service without the collection of data that is unnecessary for providing the requested service absent opt-in consent;
>
> (8) To have access to multiple viable, affordable [I]nternet platforms, services, and providers with clear and transparent pricing;
>
> (9) Not to be unfairly discriminated against or exploited based on your personal data; and
>
> (10) To have an entity that collects your personal data have reasonable business practices and accountability to protect your privacy.[278]

### *C. Senator Elizabeth Warren*

On March 8, 2019 Senator Elizabeth Warren stated in an online post, "Today's big tech companies have too much power—too much power over our economy, our society and our democracy. . . . They've bulldozed competition, used our private

[278] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

information for profit and tilted the playing field against everyone else."[279] In brief, the Warren proposal consists of two primary parts:

> First, it called for regulating dominant tech platforms like Google and Facebook as utilities and prohibiting them from both operating the platforms and owning and operating related businesses that run on those platforms. Her rules would apply to companies with $25 billion or more of global annual revenue. Ms. Warren would require smaller companies with revenue between $90 million and $25 billion to operate in a "fair, reasonable, and nondiscriminatory" manner, but wouldn't demand that they structurally separate different parts of their businesses. Secondly, the senator said she would appoint regulators who would unwind "illegal and anticompetitive tech mergers" that the government has previously blessed. Deals Ms. Warren targeted included Amazon's acquisition of Whole Foods, Facebook's purchase of WhatsApp and Instagram, and several Google acquisitions. . . .[280]

Senator Warren's presidential campaign has also placed billboards visible to the commuter trains traveling from San Francisco to the heart of Silicon Valley reading, "Break Up Big Tech."[281] She is just one voice in a growing chorus of political leaders reacting to privacy demands from constituents framed as an antitrust remedy.[282]

### *D. State Law Scheme for Individual Privacy*

Professor Peter C. Ormerod observes that "[i]n recent years, the federal courts, led by the Supreme Court, have made it increasingly difficult to vindicate information security rights and harms under the doctrine of constitutional standing."[283] In *Spokeo v. Robins*, the Supreme Court held in 2016 that a statutorily-

---

[279] Brent Kendall & Jacob Schlesinger, *Elizabeth Warren Calls for Breakup of Amazon, Google, Facebook*, WALL. ST. J. (Mar. 8, 2019), https://www.wsj.com/articles/elizabeth-warren-calls-for-breakup-of-amazon-google-facebook-11552065735?mod=searchresults&page=1&pos=19.

[280] *Id.*

[281] Nellie Bowles, *Elizabeth Warren Sticks Her Message in Big Tech's Face*, N.Y. TIMES (June 3, 2019), https://www.nytimes.com/2019/06/03/technology/elizabeth-warren-big-tech-break-up.html.

[282] *See* Kristina Peterson, *Lawmakers to Watch on Big Tech: Antitrust Stances of Key Figures Vary from Breakup Demands to More Measured Steps*, WALL ST. J., June 5, 2019, at A8; *see also* Jacob M. Schlesinger, Brent Kendall & John D. McKinnon, *Hunting for Giants: For Decades, the Washington Consensus Was to Let Markets Decide How Big Companies Could Get. No Longer. "Antitrust Law Now Stands at its Most Fluid and Negotiable Moment in a Generation,"* WALL ST. J., June 8–9, 2019, at B1.

[283] Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1896 (2019).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

recognized right lacked sufficient "concreteness" to constitute a "case or controversy" that may be adjudicated by federal courts under Article III.[284] Professor Ormerod writes, "*Spokeo* and its progeny in the lower courts are an enormous problem for information security regulatory reform because users whose information has been compromised are generally foreclosed from suing in federal court."[285]

Professor Ormerod proposes that states adopt legislation:

> Impos[ing] a fiduciary duty on entities that collect or retain personally-identifiable information . . . arguing that states should enact legislation that would codify a tort for the breach of an information fiduciary's duty. This avenue is both good policy and sound strategy because it minimizes First Amendment arguments against vindicating informational harms. . . .
>
> [D]efendants should be strictly liable for information misuse. . . .
>
> [T]he statute should prescribe a schedule of damages that begins with nominal damages and attorneys' fees for strict liability and ratchets up damages with a defendant's culpability. . . .
>
> [T]his mechanism will, for the first time, impose some substantial costs for excessive information retention . . . structuring the remedy this way will benefit the cybersecurity insurance market, thereby helping disperse information misuse costs in a more distributed and equitable way. . . .[286]

As an example of Facebook privacy challenges, Professor Ormerod points to the following examples of information misuse: "the Cambridge Analytica scandal, where a Facebook app developer breached Facebook's terms of service when he—under the auspices of academic research—collected user's data and provided that trove of information to a for-profit political consulting firm."[287] Then, in another scenario, a Facebook employee was reportedly terminated for using "his position to stalk women."[288] Next, Facebook appears to have used collected data to provide

---

[284] Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893, 1896 (2019) (citing Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016)).

[285] Ormerod, *supra* note 284, at 1894.

[286] *Id.* at 1896–97.

[287] *Id.* at 1898 (citing Matthew Rosenberg, Nicholas Confessore & Carole Cadwalladr, *How Trump Consultants Exploited the Facebook Data of Millions*, N.Y. TIMES (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html).

[288] *Id.* (citing Joseph Cox, *Facebook is Investigating a Claim That an Employee Used His Position to Stalk Women*, MOTHERBOARD (Apr. 30, 2018), https://mother-board.vice.com/en_us/article/kzxdny/



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

"advertisers with users' cell phone numbers, even when the company only acquired those numbers for multifactor authentication purposes."[289]

## X. MARCH 2019 MARK ZUCKERBERG STRATEGY ANNOUNCEMENT

> *To date, numerous governments have launched formal investigations into the company [Facebook] including the United Kingdom, Australia, Canada, Nigeria, Kenya, and India. There's much we do not know about Cambridge Analytica, but there are significant facts already in the public record. We know that Cambridge Analytica was established by Robert and Rebecca Mercer in 2013 at the urging of former White House chief strategist Steve Bannon as an American subsidiary of a London-based firm, SCL Group.*
>
> *It has reported that the intent of creating an American shell was to give the appearance of compliance with the United States election law that prohibits foreigners from working on United States elections. According to CEO Alexander Nix, Cambridge Analytica worked for candidates in 44 United States elections in 2014.*
>
> *Senator Dianne Feinstein*
> *Ranking Member, Senate*
> *Judiciary Committee*
> *May 16, 2018*[290]

On March 6, 2019, Facebook CEO Mark Zuckerberg posted the following blog. Because of its historical significance, it is reproduced below in full:

> *My focus for the last couple of years has been understanding and addressing the biggest challenges facing Facebook. This means taking positions on important issues concerning the future of the Internet. In this note, I'll outline our vision and principles around building a privacy-focused messaging and social networking platform. There's a lot to do here, and we're committed to working openly and consulting with experts across society as we develop this.*
>
> . . .

facebook-investigating-employee-stalking-women-online; Sam Levin, *Facebook Fires Engineer Accused of Stalking, Possibly by Abusing Data Access*, THE GUARDIAN (May 2, 2018), https://www.theguardian.com/technology/2018/may/02/facebook-engineer-fired-alleged-stalker-tinder).

[289] *Id.* at 1898 (citing Kashmir Hill, *Facebook is Giving Advertisers Access to Your Shadow Contact Information*, GIZMODO (Sept. 26, 2018), https://gizmodo.com/facebook-is-giving-advertisers-access-to-your-shadow-co-1828476051).

[290] *Cambridge Analytica and the Future of Data Privacy: Before the S. Judiciary Comm.*, 115th Cong. 2 (2018) (statement of Sen. Dianne Feinstein, Ranking Member, S. Comm. on the Judiciary).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

Over the last 15 years, Facebook and Instagram have helped people connect with friends, communities, and interests in the digital equivalent of a town square. But people increasingly also want to connect privately in the digital equivalent of the living room. As I think about the future of the Internet, I believe a privacy-focused communications platform will become even more important than today's open platforms. Privacy gives people the freedom to be themselves and connect more naturally, which is why we build social networks.

Today we already see that private messaging, ephemeral stories, and small groups are by far the fastest growing areas of online communication. There are a number of reasons for this. Many people prefer the intimacy of communicating one-on-one or with just a few friends. People are more cautious of having a permanent record of what they've shared. And we all expect to be able to do things like payments privately and securely.

Public social networks will continue to be very important in people's lives—for connecting with everyone you know, discovering new people, ideas and content, and giving people a voice more broadly. People find these valuable every day, and there are still a lot of useful services to build on top of them. But now, with all the ways people also want to interact privately, there's also an opportunity to build a simpler platform that's focused on privacy first.

I understand that many people don't think Facebook can or would even want to build this kind of privacy-focused platform—because frankly we don't currently have a strong reputation for building privacy protective services, and we've historically focused on tools for more open sharing. But we've repeatedly shown that we can evolve to build the services that people really want, including in private messaging and stories.

I believe the future of communication will increasingly shift to private, encrypted services where people can be confident what they say to each other stays secure and their messages and content won't stick around forever. This is the future I hope we will help bring about.

We plan to build this the way we've developed WhatsApp: focus on the most fundamental and private use case—messaging—make it as secure as possible, and then build more ways for people to interact on top of that, including calls, video chats, groups, stories, businesses, payments, commerce, and ultimately a platform for many other kinds of private services.

This privacy-focused platform will be built around several principles:



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

**Private interactions.** People should have simple, intimate places where they have clear control over who can communicate with them and confidence that no one else can access what they share.

**Encryption.** People's private communications should be secure. End-to-end encryption prevents anyone—including us—from seeing what people share on our services.

**Reducing Permanence.** People should be comfortable being themselves, and should not have to worry about what they share coming back to hurt them later. So we won't keep messages or stories around for longer than necessary to deliver the service or longer than people want them.

**Safety.** People should expect that we will do everything we can to keep them safe on our services within the limits of what's possible in an encrypted service.

**Interoperability.** People should be able to use any of our apps to reach their friends, and they should be able to communicate across networks easily and securely.

**Secure data storage.** People should expect that we won't store sensitive data in countries with weak records on human rights like privacy and freedom of expression in order to protect data from being improperly accessed.

Over the next few years, we plan to rebuild more of our services around these ideas. The decisions we'll face along the way will mean taking positions on important issues concerning the future of the Internet. We understand there are a lot of tradeoffs to get right, and we're committed to consulting with experts and discussing the best way forward. This will take some time, but we're not going to develop this major change in our direction behind closed doors. We're going to do this as openly and collaboratively as we can because many of these issues affect different parts of society.

**Private Interactions as a Foundation**

For a service to feel private, there must never be any doubt about who you are communicating with. We've worked hard to build privacy into all our products, including those for public sharing. But one great property of messaging services is that even as your contacts list grows, your individual threads and groups remain private. As your friends evolve over time, messaging services evolve gracefully and remain intimate.

This is different from broader social networks, where people can accumulate friends or followers until the services feel more public. This is well-suited to many



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

important uses—telling all your friends about something, using your voice on important topics, finding communities of people with similar interests, following creators and media, buying and selling things, organizing fundraisers, growing businesses, or many other things that benefit from having everyone you know in one place. Still, when you see all these experiences together, it feels more like a town square than a more intimate space like a living room.

There is an opportunity to build a platform that focuses on all of the ways people want to interact privately. This sense of privacy and intimacy is not just about technical features—it is designed deeply into the feel of the service overall. In WhatsApp, for example, our team is obsessed with creating an intimate environment in every aspect of the product. Even where we've built features that allow for broader sharing, it's still a less public experience. When the team built groups, they put in a size limit to make sure every interaction felt private. When we shipped stories on WhatsApp, we limited public content because we worried it might erode the feeling of privacy to see lots of public content—even if it didn't actually change who you're sharing with.

In a few years, I expect future versions of Messenger and WhatsApp to become the main ways people communicate on the Facebook network. We're focused on making both of these apps faster, simpler, more private and more secure, including with end-to-end encryption. We then plan to add more ways to interact privately with your friends, groups, and businesses. If this evolution is successful, interacting with your friends and family across the Facebook network will become a fundamentally more private experience.

**Encryption and Safety**

People expect their private communications to be secure and to only be seen by the people they've sent them to—not hackers, criminals, over-reaching governments, or even the people operating the services they're using.

There is a growing awareness that the more entities that have access to your data, the more vulnerabilities there are for someone to misuse it or for a cyber attack to expose it. There is also a growing concern among some that technology may be centralizing power in the hands of governments and companies like ours. And some people worry that our services could access their messages and use them for advertising or in other ways they don't expect.

End-to-end encryption is an important tool in developing a privacy-focused social network. Encryption



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

is decentralizing—it limits services like ours from seeing the content flowing through them and makes it much harder for anyone else to access your information. This is why encryption is an increasingly important part of our online lives, from banking to healthcare services. It's also why we built end-to-end encryption into WhatsApp after we acquired it.

In the last year, I've spoken with dissidents who've told me encryption is the reason they are free, or even alive. Governments often make unlawful demands for data, and while we push back and fight these requests in court, there's always a risk we'll lose a case—and if the information isn't encrypted we'd either have to turn over the data or risk our employees being arrested if we failed to comply. This may seem extreme, but we've had a case where one of our employees was actually jailed for not providing access to someone's private information even though we couldn't access it since it was encrypted.

At the same time, there are real safety concerns to address before we can implement end-to-end encryption across all of our messaging services. Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things. When billions of people use a service to connect, some of them are going to misuse it for truly terrible things like child exploitation, terrorism, and extortion. We have a responsibility to work with law enforcement and to help prevent these wherever we can. We are working to improve our ability to identify and stop bad actors across our apps by detecting patterns of activity or through other means, even when we can't see the content of the messages, and we will continue to invest in this work. But we face an inherent tradeoff because we will never find all of the potential harm we do today when our security systems can see the messages themselves.

Finding the right ways to protect both privacy and safety is something societies have historically grappled with. There are still many open questions here and we'll consult with safety experts, law enforcement and governments on the best ways to implement safety measures. We'll also need to work together with other platforms to make sure that as an industry we get this right. The more we can create a common approach, the better.

On balance, I believe working towards implementing end-to-end encryption for all private communications is the right thing to do. Messages and calls are some of the most sensitive private conversations people have, and in a world of increasing cyber security threats and heavy-handed government intervention in many countries, people want us to take the extra step to



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

secure their most private data. That seems right to me, as long as we take the time to build the appropriate safety systems that stop bad actors as much as we possibly can within the limits of an encrypted service. We've started working on these safety systems building on the work we've done in WhatsApp, and we'll discuss them with experts through 2019 and beyond before fully implementing end-to-end encryption. As we learn more from those experts, we'll finalize how to roll out these systems.

**Reducing Permanence**

We increasingly believe it's important to keep information around for shorter periods of time. People want to know that what they share won't come back to hurt them later, and reducing the length of time their information is stored and accessible will help.

One challenge in building social tools is the "permanence problem." As we build up large collections of messages and photos over time, they can become a liability as well as an asset. For example, many people who have been on Facebook for a long time have photos from when they were younger that could be embarrassing. But people also really love keeping a record of their lives. And if all posts on Facebook and Instagram disappeared, people would lose access to a lot of valuable knowledge and experiences others have shared.

I believe there's an opportunity to set a new standard for private communication platforms—where content automatically expires or is archived over time. Stories already expire after 24 hours unless you archive them, and that gives people the comfort to share more naturally. This philosophy could be extended to all private content.

For example, messages could be deleted after a month or a year by default. This would reduce the risk of your messages resurfacing and embarrassing you later. Of course you'd have the ability to change the timeframe or turn off auto-deletion for your threads if you wanted. And we could also provide an option for you to set individual messages to expire after a few seconds or minutes if you wanted.

It also makes sense to limit the amount of time we store messaging metadata. We use this data to run our spam and safety systems, but we don't always need to keep it around for a long time. An important part of the solution is to collect less personal data in the first place, which is the way WhatsApp was built from the outset.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

**Interoperability**

People want to be able to choose which service they use to communicate with people. However, today if you want to message people on Facebook you have to use Messenger, on Instagram you have to use Direct, and on WhatsApp you have to use WhatsApp. We want to give people a choice so they can reach their friends across these networks from whichever app they prefer.

We plan to start by making it possible for you to send messages to your contacts using any of our services, and then to extend that interoperability to SMS too. Of course, this would be opt-in and you will be able to keep your accounts separate if you'd like.

There are privacy and security advantages to interoperability. For example, many people use Messenger on Android to send and receive SMS texts. Those texts can't be end-to-end encrypted because the SMS protocol is not encrypted. With the ability to message across our services, however, you'd be able to send an encrypted message to someone's phone number in WhatsApp from Messenger.

This could also improve convenience in many experiences where people use Facebook or Instagram as their social network and WhatsApp as their preferred messaging service. For example, lots of people selling items on Marketplace list their phone number so people can message them about buying it. That's not ideal, because you're giving strangers your phone number. With interoperability, you'd be able to use WhatsApp to receive messages sent to your Facebook account without sharing your phone number—and the buyer wouldn't have to worry about whether you prefer to be messaged on one network or the other.

You can imagine many simple experiences like this—a person discovers a business on Instagram and easily transitions to their preferred messaging app for secure payments and customer support; another person wants to catch up with a friend and can send them a message that goes to their preferred app without having to think about where that person prefers to be reached; or you simply post a story from your day across both Facebook and Instagram and can get all the replies from your friends in one place.

You can already send and receive SMS texts through Messenger on Android today, and we'd like to extend this further in the future, perhaps including the new telecom RCS standard. However, there are several issues we'll need to work through before this will be possible. First, Apple doesn't allow apps to interoperate



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

with SMS on their devices, so we'd only be able to do this on Android. Second, we'd need to make sure interoperability doesn't compromise the expectation of encryption that people already have using WhatsApp. Finally, it would create safety and spam vulnerabilities in an encrypted system to let people send messages from unknown apps where our safety and security systems couldn't see the patterns of activity.

These are significant challenges and there are many questions here that require further consultation and discussion. But if we can implement this, we can give people more choice to use their preferred service to securely reach the people they want.

**Secure Data Storage**

People want to know their data is stored securely in places they trust. Looking at the future of the Internet and privacy, I believe one of the most important decisions we'll make is where we'll build data centers and store people's sensitive data.

There's an important difference between providing a service in a country and storing people's data there. As we build our infrastructure around the world, we've chosen not to build data centers in countries that have a track record of violating human rights like privacy or freedom of expression. If we build data centers and store sensitive data in these countries, rather than just caching non-sensitive data, it could make it easier for those governments to take people's information.

Upholding this principle may mean that our services will get blocked in some countries, or that we won't be able to enter others anytime soon. That's a tradeoff we're willing to make. We do not believe storing people's data in some countries is a secure enough foundation to build such important Internet infrastructure on.

Of course, the best way to protect the most sensitive data is not to store it at all, which is why WhatsApp doesn't store any encryption keys and we plan to do the same with our other services going forward.

But storing data in more countries also establishes a precedent that emboldens other governments to seek greater access to their citizen's data and therefore weakens privacy and security protections for people around the world. I think it's important for the future of the Internet and privacy that our industry continues to hold firm against storing people's data in places where it won't be secure.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> **Next Steps**
>
> Over the next year and beyond, there are a lot more details and tradeoffs to work through related to each of these principles. A lot of this work is in the early stages, and we are committed to consulting with experts, advocates, industry partners, and governments—including law enforcement and regulators—around the world to get these decisions right.
>
> At the same time, working through these principles is only the first step in building out a privacy-focused social platform. Beyond that, significant thought needs to go into all of the services we build on top of that foundation—from how people do payments and financial transactions, to the role of businesses and advertising, to how we can offer a platform for other private services.
>
> But these initial questions are critical to get right. If we do this well, we can create platforms for private sharing that could be even more important to people than the platforms we've already built to help people share and connect more openly.
>
> Doing this means taking positions on some of the most important issues facing the future of the Internet. As a society, we have an opportunity to set out where we stand, to decide how we value private communications, and who gets to decide how long and where data should be stored.
>
> I believe we should be working towards a world where people can speak privately and live freely knowing that their information will only be seen by who they want to see it and won't all stick around forever. If we can help move the world in this direction, I will be proud of the difference we've made.[291]

### *A. Reaction from Thought Leaders*

Mark Zuckerberg's blog comments of March 6, 2019 were met with considerable reaction from the technology community. *The New York Times* coverage noted that Facebook "plans to start shifting people toward private conversations and away from public broadcasting. Mr. Zuckerberg, who runs Facebook, Instagram, WhatsApp and Messenger . . . expressed his intention to

[291] Mark Zuckerberg, *A Privacy-Focused Vision for Social Networking*, FACEBOOK (Mar. 6, 2019), https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

change the essential nature of social media."[292] Journalist Mike Isaac reports, "Instead of encouraging public posts . . . [Zuckerberg] would focus on private and encrypted communications, in which users message mostly smaller groups of people they know. Unlike publicly shared posts that are kept as users' permanent records, the communications could also be deleted after a certain period of time."[293] *The Wall Street Journal* reported that Facebook "will develop products within those messaging services—such as payments and e-commerce—that eventually could allow it to diversify from the ad-supported business model that led to a number of privacy missteps."[294] Jeff Horowitz reports on an interview where Mark Zuckerberg described, "the shift as a response to user demand, saying people increasingly prefer to communicate in small groups or one-to-one in the style of its WhatsApp messaging platform, rather than blasting their thoughts to a public audience, as most users do on its Instagram and the company's flagship Facebook platform."[295] Just days after the Zuckerberg blog, Chris Cox, one of the company's first fifteen engineers and Facebook's Chief Product Officer resigned—and Chris Daniels, WhatsApp Vice President has also departed.[296] And now, a sampling of reaction within days of the Zuckerberg blog post from several technology industry thought leaders:

Christopher Mims

*The Wall Street Journal*'s technology writer Christopher Mims writes: "Mark Zuckerberg has outlined a new vision for Facebook Inc. that he says is focused on privacy. It is a major shift in direction, but it doesn't mean what you think it means."[297] Mr. Mims continues:

> What the Facebook chief executive's manifesto really promises is a more tightly integrated version of Facebook's various apps and services, cloaked in the raiments of privacy but, in fact, continuing to operate in contradiction to it. Facebook would still gather data from its existing sources—the core social network, its Instagram app, a web-wide tracking system and countless apps that sometimes send the company deeply personal

[292] Mike Isaac, *Users' Privacy Is New Focus, Facebook Says: Change by Zuckerberg Follows Scandals*, N.Y. TIMES, Mar. 7, 2019, at A1.

[293] *Id.*

[294] Jeff Horowitz, *Facebook Pivots to Private Sharing*, WALL ST. J., Mar. 7, 2019, at A1.

[295] *Id.*

[296] Mike Isaac, *2 Facebook Leaders Quit, Adding to Churn at Top*, N.Y. TIMES, Mar. 15, 2019, at B1; Jeff Horwitz & Georgia Wells, *Facebook Executives Exit After Shift in Strategy*, WALL ST. J., Mar. 15, 2019, at A1.

[297] Christopher Mims, *Privacy Doesn't Mean Privacy from Facebook*, WALL ST. J., Mar. 9–10, 2019, at B4.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

information—but also increasingly from messaging apps. These would double as interfaces with businesses and, eventually, usurp the functions of our credit cards and digital wallets. (He mentioned "payments" in his note four times.)

Mr. Zuckerberg understood long before most of us did that the public sharing that made his business so successful was a fad. The price he paid for WhatsApp—$22 billion—seemed like a multiple-zero typo, but now it is considered a prescient investment.

Recent data from Edison Research suggest Facebook's primary social network has lost an estimated 15 million users since 2017 in the U.S. alone. Most of those are in the coveted 12-to-34-year-old demographic. Yet Facebook's most recent quarterly report shows a company at the apex of its power, earning record profits and growing its overall user base as people shift to Instagram and WhatsApp. It's clear Facebook must follow its users to the services they are turning to as alternatives to its flagship, and there can be no doubt that internal numbers, some of which Mr. Zuckerberg referenced, show people devoting more time to messaging, small groups and ephemeral posts like Instagram stories.

WhatsApp was Facebook's quick access into a world that has two dominant players occupying very different spheres: Tencent's WeChat and Apple's iMessage. WeChat has become a de facto operating system for life in China. While it doesn't have the encryption features that Mr. Zuckerberg described, it has all of the revenue-generating services that he covets. . . .

Belatedly, Mr. Zuckerberg seems to have realized that the reputational damage of the Cambridge Analytica data breach a half-dozen scandals since could affect his company's bottom line. . . . It's clear his company intends to continue to advertise to us, even on its encrypted platforms. . . .

That Facebook wants to make it possible for dissidents to use its services to communicate securely is admirable, but must be weighed against the fact that this will put even more of the communications on Facebook beyond the reach of the company's own content filters. Pivoting to privacy is a neat judo move for Facebook, as the company's former chief security officer Alex Stamos observed on Twitter. It allows the company to absolve itself of responsibility for the content that passes through



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> its systems, while also allowing it to claim a victory for individual freedom.[298]

Kara Swisher

In an op-ed for *The New York Times*, Kara Swisher observes that Mark Zuckerberg's decision process is data driven.[299] Ms. Swisher writes:

> That data shows that the future is not looking good for the bloated, oversharing, fake-news spewing, Russian-infected big blue app. Social media is in big trouble with the young and it is long past time for it to shift to a privacy-oriented stance that was never part of its DNA, except perhaps as a throwaway line in a news release.
>
> Now Mr. Zuckerberg has written a blog post—with not one single trace of irony and with nary a mention of the many privacy abuses he has presided over—announcing that the company would be betting big on the private messaging and protected communications for its billions of users.
>
> You know, like snapchat.
>
> Over the years, Facebook has swiped many nifty ideas from Snapchat, the ephemeral messaging platform—which Mr. Zuckerberg tried to buy many years ago when it was still a start-up. That has been especially true at the Facebook-owned Instagram, which did a wholesale shoplifting of Snapchat's Stories by creating . . . wait for it. . . Instagram Stories!
>
> In a podcast interview with me, the Instagram co-founder and former chief executive Kevin Systrom did not even bother to hide the act. He said that he admired the creativity of Evan Spiegel, the Snapchat founder, and that there was nothing wrong with taking a good idea and making it better. . . .
>
> But this time Mr. Zuckerberg is pilfering so much more, sketching out a future business that looks a lot like China's We-Chat mixed in. And, mostly, not at all like Facebook. . . .
>
> One person I spoke with likened Mr. Zuckerberg to a captain who has decided not to go down with his ship.

---

[298] *Id.*

[299] Kara Swisher, Opinion, *Facebook Steals a Good Idea*, N.Y. TIMES, Mar. 10, 2019, at SR11.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> He's just going to jump to another ship rather than fix the first one. And keep on going.[300]

Ben Thompson

Ben Thompson is one of the most prolific and visionary observers of the technology scene, through his blog *Stratechery*,[301] The *Daily Update*,[302] and various subject-specific podcasts.[303] Categorizing Facebook as one of the two Super Aggregators (Google is the other one), making "money through ads, and advertisers come to Facebook and Google because they want to reach consumers. From an advertiser perspective, users—or to be more precise, access to users' attention—is a product they are absolutely paying for."[304] Mr. Thompson has observed:

> First and foremost, regulators need to understand that the power of Aggregators comes from controlling demand, not supply. Specifically, consumers voluntarily use Google and Facebook, and "suppliers" like content providers, advertisers, and users themselves, have no choice but to go where consumers are. To that end:
>
> Facebook's ultimate threat can never come from publishers or advertisers, but rather demand—that is, users. The real danger, though, is not from users also using competing social networks (although Facebook has always been paranoid about exactly that); that is not enough to break the virtuous cycle. Rather, the only thing that could undo Facebook's power is users actively rejecting the app. And, I suspect, the only way users would do that en masse would be if it became accepted fact that Facebook is actively bad for you—the online equivalent of smoking.
>
> For Facebook, the Cambridge Analytica scandal was akin to the Surgeon General's report on smoking: the threat was not that regulators would act, but that users would, and nothing could be more fatal. That is because the regulatory corollary of Aggregation Theory is that the ultimate form of regulation is user generated.

---

[300] *Id.*

[301] Ben Thompson, *Facebook's Privacy Cake*, STRATECHERY (Mar. 7, 2019), https://stratechery.com/2019/facebooks-privacy-cake/.

[302] *The Daily Update*, STRATCHERY, https://stratechery.com/membership/.

[303] *Id.*

[304] Ben Thompson, *Data Factories*, STRATECHERY (Oct. 2, 2018), https://stratechery.com/2018/data-factories/?utm_source=Memberful&utm_campaign=6be8b28dc0-weekly_article_12_19_2018&utm_medium=email&utm_term=0_d4c7fece27-6be8b28dc0-110912269.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> If regulators, EU or otherwise, truly want to constrain Facebook and Google—or, for that matter, all of the other ad networks and companies that in reality are far more of a threat to user privacy—then the ultimate force is user demand, and the lever is demanding transparency on exactly what these companies are doing.[305]

Readers and regulators should benefit from a reading of Mr. Thompson's full analysis of Mr. Zuckerberg's vision statement, on the website *Stratechery*. Here is a brief summary:

> Look again at what Zuckerberg outlined:
>
> - Private interactions
> - Encryption
> - Reducing Permanence
> - Safety
> - Interoperability
> - Secure data storage
>
> The first three are all about owning the 1×1 private ephemeral space; critically, none of them have anything to do with Facebook's core feed-based products. Facebook is going to continue to exist as it has to date, as will Instagram, including all of the data collection and ad targeting that currently exist. The "Privacy-Focused Vision for Social Networking" is *in addition to* Facebook's current products, not *in place of*. This is the mistake made by those that took Zuckerberg too seriously . . . why wouldn't Facebook want to move in this direction? There are multiple benefits:
>
> - First, this is a valuable space to own for all of the reasons that Snapchat succeeded in the first place. People want a place to communicate freely without fear of snooping or a historical record.
>
> - Second, to the extent the rise of 1×1 networking is inexorable, it is better for Facebook that it happen on their properties. Not only does Facebook preserve the ability to advertise on privacy-focused platforms—the company can leverage data from Facebook to advertise in its messaging products (although I am skeptical that messaging products are well-suited to advertising)—it also prevents would-be competitors from capturing leverageable attention.

[305] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

- Third, as we have seen over the last 24 hours, there are tremendous PR benefits from a privacy-focused service. Facebook has changed nothing about its core service or data collection policies, yet the assumption is that the company is pivoting and the only debate is whether to believe them or not.

Perhaps most compelling, though, is the degree to which this move locks in Facebook's competitive position. . . . Moreover, given Facebook's focus on end-to-end encryption, the company has made it that much harder to even get off the ground: not even Snapchat is fully end-to-end encrypted (pictures are, but not text messages).

There is an even more important benefit to Facebook voluntarily forgoing the data within messages and limiting the time it keeps surrounding metadata (make no mistake, end-to-end encryption is a real thing—Facebook will *not* be able to see encrypted messages). . . .

Why can Facebook deliver most of the value? Because they are still Facebook! They still have the core Facebook app, Instagram, "Like"-buttons scattered across the web—none of that is going away with this announcement. They can very much afford a privacy-centric messaging offering in a way that any would-be challenger could not. Privacy, it turns out, is a competitive advantage for Facebook, not the cudgel the company's critics hoped it might be.

Safety, Interoperability, and Strategy Credits

The last three items in Zuckerberg's list are interesting in their own right; to take them one-by-one:

Safety: This is about the very real trade-offs that come with end-to-end encryption. One obvious issue is law-enforcement: . . . when it comes to phone security; end-to-end encryption is both more challenging and yet simpler, simply because it is, properly implemented, truly unbreakable.

Another issue is misinformation: for all of the issues surrounding misinformation on Facebook, at least misinformation is traceable; that is not the case if messages are encrypted, which has already been an issue with WhatsApp in India. One could certainly make the cynical argument that, in the process of cloaking itself in privacy, Facebook is washing its hands of misinformation.

To be sure, Facebook is confident it can leverage its ability to analyze metadata to stop bad actors; that the exact same sort of audience analysis is perfectly portable



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

to advertising is a rather happy benefit as far as Facebook is concerned.

Interoperability: This is perhaps the feature that is easiest to be cynical about; while it can certainly be frustrating to have to balance multiple messaging apps, for much of the world consolidating Facebook-owned messaging will not fully address the problem, thanks to alternatives like Messages, LINE, Kakao, etc. Moreover, even in areas where Facebook owns both the Phone (via WhatsApp) and the phonebook (via Facebook and Instagram), exactly how much consumer demand is there for integration?

There is, to be sure, a business argument: Facebook has already unified much of the ad infrastructure underlying its services, and unifying messaging is, to the extent Facebook wants to build a business platform on messaging, a natural next step. There is also a regulatory argument: while it is difficult to make the argument that Facebook has broken antitrust laws, the remedy, should that be accomplished, is obvious—split off Instagram and WhatsApp. That will be harder to do if they are fully integrated with Facebook, not simply on the advertising side but also the user side.

Secure Data Storage: This is an interesting addition to this piece, as it has little to do with messaging in the communications sense, but a lot to do with messaging in the political sense. . . .

Privacy Moats

Ultimately there are three broad takeaways from Zuckerberg's article:

- Stop expecting companies to act against their interests. Facebook isn't killing their core business any[ ]more than Apple, to take a pertinent example, is willing to go to the mat to protect user data in China.

- Facebook doing something that benefits itself is not inherently bad for end users. It is perfectly reasonable that the company can be instituting genuinely user-friendly changes like end-to-end encryption even as it furthers its own self-interests.

- Relatedly, and most importantly, there needs to be much more appreciation for the anti-competitive trade-offs inherent in an absolutist approach to privacy. Facebook is doing what its fiercest critics supposedly want, and enhancing its competitive position as a result.

This was a point I made last year. . . .

If an emphasis on privacy and the non-leakage of data is a priority, it follows that the platforms that already



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> exist will be increasingly entrenched. And, if those platforms will be increasingly entrenched, then the more valuable might regulation be that ensures an equal playing field on top of those platforms. The reality is that an emphasis on privacy will only increase the walls on those gardens; it may be fruitful to rule out the possibility of unfair expansion.
>
> This is a debate that is woefully lacking. The reality is that the only user-friendly way to enforce privacy—which is another way of saying the only scalable way in a demand-driven world—is to severely limit inter-operability and over-burden would-be challengers. Regulators need to be far more aware of this and either choose another approach to privacy—i.e. entrust it to individuals—or regulate data-platforms, at least in terms of competition on top of their platforms, even more severely.[306]

In summary, Ben Thompson and James Allworth conclude, "this is smart strategy from Facebook and it's dressed-up as addressing privacy concerns . . . but they are not really addressing privacy concerns . . . we're just going to get more of what we've got and it's just going to be harder for someone to come along and challenge them."[307]

Zeynep Tufekci

Professor Zeynep Tufekci writes, "Why take seriously someone who has repeatedly promised—but seldom delivered—improvements to Facebook's privacy practices?"[308] Ms. Tufekci continues:

> This is a company, after all, that signed a consent decree with the Federal Trade Commission agreeing to improve how it handles the personal information of its users, after federal regulators filed charges against it for deceiving customers about their privacy. That was about seven years ago, and it has been one scandal after another since. . . .
>
> Here are four pressing questions about privacy that Mr. Zuckerberg conspicuously did not address: Will Facebook stop collecting data about people's browsing behavior, which it does extensively? Will it stop purchasing information from data brokers who collect or

[306] Thompson, *supra* note 301; *see also* Christopher S. Yoo, *When Antitrust Met Facebook*, 19 GEO. MASON L. REV. 1147 (2012) (discussing Facebook and antitrust).

[307] Ben Thompson & James Allworth, *Mark Zuckerberg's Projected Self*, EXPONENT, 165 (Mar. 3, 2019), https://itunes.apple.com/us/podcast/exponent/id826420969?mt=2&i=1000431353735.

[308] Zeynep Tufekci, Opinion, *Zuckerberg's So-Called Focus on Privacy*, N.Y. TIMES, Mar. 8, 2019, at A27.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> "scrape" vast amounts of data about billions of people, often including information related to our health and finances? Will it stop creating "shadow profiles"—collections of data about people who aren't even on Facebook? And most important: Will it change its fundamental business model, which is based on charging advertisers to take advantage of this widespread surveillance to "micro-target" consumers? . . .
>
> Sheryl Sandberg, Facebook's chief operating officer, likes to say that the company's problem is that it has been "way too idealistic." I think the problem is the invasive way it makes its money and its lack of meaningful oversight. Until those things change, I don't expect any shift by the company toward privacy to matter much.[309]

Mark Zuckerberg

And last, in an attempt to weigh the trustworthiness of his March 2019 change in strategy, it seems instructive to look at a prior statement by Mr. Zuckerberg, and weighing the importance of committing anything you think to email or text. *The New Yorker* reported during 2010 that:

> In another exchange leaked to Silicon Alley Insider, Zuckerberg explained to a friend that his control of Facebook gave him access to any information he wanted on any Harvard student:
>
> Zuck: yea so if you ever need info about anyone at Harvard
>
> Zuck: just ask
>
> Zuck: I have over 4000 emails, pictures, addresses, sns
>
> Friend: what? how'd you manage that one?
>
> Zuck: people just submitted it
>
> Zuck: I don't know why
>
> Zuck: they 'trust me'
>
> Zuck: dumb fucks[310]

[309] *Id.*

[310] *See* Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057 (2019) (citing Jose Antonio Vargas, *The Face of Facebook: Mark Zuckerberg Opens Up*, NEW YORKER (Sept. 20, 2010), https://www.newyorker.com/magazine/2010/09/20/the-face-of-facebook).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> *I had spent a career trying to draw smart conclusions from incomplete information, and one day early in 2016 I started to see things happening on Facebook that did not look right. I started pulling on that thread and uncovered a catastrophe. In the beginning, I assumed that Facebook was a victim and I just wanted to warn my friends. What I learned in the months that followed shocked and disappointed me. I learned that my trust in Facebook had been misplaced.*
>
> *Roger McNamee*
> *Silicon Valley Investor*[311]

### *A. The Dual-Class Stock Issue*

A reasonable question to ask is "What is unique about the governance of Facebook that results in this user privacy crisis and complicit role in global election meddling? One possibility may be the result over-time from Facebook's "dual-class capital structure, consisting of two classes of shares with differential voting rights."[312] Lucien A. Bebchuk and Kobi Kastiel observe that many "U.S. public companies—including such well-known companies as CBS, Comcast, Facebook, Ford, Google [Alphabet], News Corp., and Nike have dual-class structures. Furthermore, since Google decided to use a dual-class structure for its 2004 IPO, a significant number of 'hot' tech companies have followed. . . ."[313] The May 2019 initial public offering of Uber also featured an entity having a dual-class structure.[314] Facebook provides the following description of its "controlled company" status:

> Because we qualify as a "controlled company" under the corporate governance rules for Nasdaq-listed companies, we are not required to have a majority of our board of directors be independent, nor are we required to have a compensation committee or an independent nominating

[311] ROGER MCNAMEE, ZUCKED: WAKING UP TO THE FACEBOOK CATASTROPHE 2 (2019).

[312] Lucian A. Bebchuk & Kobi Kastiel, *The Untenable Case for Perpetual Dual-Class Stock*, 103 VA. L. REV. 585, 587 (2017).

[313] *Id.* at 591.

[314] Stephen Grocer, *A Cheat Sheet for the Hotly Anticipated Uber Public Offering*, N.Y. TIMES, May 6, 2019, at B3; *see also Examining Private Market Exemptions as a Barrier to IPOs and Retail Investment* 116th Cong. 2 (2018) (statement of Renee M. Jones, Professor of Law, Boston College Law School) (observing, "examples of how badly things can go awry when investors fail to monitor unicorn operations can be seen in the histories of Uber, Theranos and other unicorn firms"); Dual-Class Shares: A Recipe for Disaster (remarks by Rick Fleming, Inv. Advoc. at the SEC, addressed the practice at the ICGN Conf. in Miami) (Oct. 15, 2019); Itai Fiegenbaum, *The Controlling Shareholder Enforcement Gap*, 56(3) AM. BUS. L.J. 582 (Apr. 4, 2019).



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> function. In light of our status as a controlled company, our board of directors determined not to have a separate and independent nominating function and chose to have the full board of directors be directly responsible for nominating members of our board, and in the future we could elect not to have a majority of our board of directors be independent or not to have a compensation committee. Accordingly, should the interests of our controlling stockholder differ from those of other stockholders, the other stockholders may not have the same protections afforded to stockholders of companies that are subject to all of the corporate governance rules for Nasdaq-listed companies.[315]

Now that we have more than a decade of experience with this form of corporate governance, why might this be an important element in the Facebook governance failures? Bebchuk and Kastiel write, "Entrenchment insulates controllers [Zuckerberg] from the disciplinary force of the market for corporate control that otherwise might limit the ability of a poorly performing controller to continue leading the company."[316] In addition, "[t]he cost of a dual-class structure are likely to increase over time for two main reasons: the likely erosion of any superior skills that the controller might have had at the time of the IPO and the likely decrease in the controller's fraction of equity capital."[317] Consider:

> At any given time, the costs of providing a founder with a lock on control depends on the likelihood that the controller is no longer the most suitable person for this role. At the time of the IPO, the founder of a company may have the special skills and deep knowledge of a specific industry and business to make her uniquely fit to be at the helm. Therefore, supporters of dual-class often argue that it is preferable to let such a talented controller remain in control long after the IPO.
>
> However, this superior-controller argument does not provide a good basis for the use of a *perpetual* dual-class structure. While such an argument might justify the use of dual-class stock at the IPO stage, it loses most of its power with the passage of time. . . .
>
> Rather, many years after the IPO, there is a real possibility that the founder's superiority as the company leader will erode or even disappear. Over time, a once-successful founder may face natural limitations in a fast-

[315] 2018 Form 10-K, *supra* note 15, at 27.

[316] Bebchuk & Kastiel, *supra* note 312, at 602.

[317] *Id.* at 604.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> evolving technological or business environment. She could also simply lose her golden touch. If the founder stops being the most fitting (or even a fitting) leader, the expected costs from her lock on control could become significant. These expected costs are especially high in the case of a young founder: The longer her lock on control, the greater the risk that she would become an ill-fitting leader.[318]

Bebchuk and Kastiel write that Facebook "went public in 2012 with a dual-class structure that placed some limits on the ability of its founder, Mark Zuckerberg, to reduce his fraction of equity capital without relinquishing control."[319] Then, a reclassification plan was approved because of Zuckerberg's majority voting power in April 2016, "that would have enabled Zuckerberg to sell two-thirds of his Facebook shares—reducing his stake of equity capital to about 4% and possibly less—without losing his controlling voting power."[320] When faced with a shareholder lawsuit, Facebook announced during September 2017, "its decision not to proceed with the reclassification plan for the time being. Zuckerberg currently continues to face certain limits on his freedom to unload shares without losing his control."[321] In looking at dual-class capital structures (like Facebook) Bebchuk and Kastiel conclude:

> Over time, the potential benefits of dual-class structures can be expected to decline and the potential costs to increase. We have also shown that controllers have perverse incentives to retain dual-class structures even when those structures become substantially inefficient. Thus, as time passes from the IPO, there is a growing risk that a dual-class structure will become value decreasing and that public investors will find themselves subject to an inefficient structure with significant governance risks and costs. . . .
>
> Our key contribution . . . is to demonstrate that even those who believe that dual-class structures are often efficient at the time of the IPO, and the period following it, should have substantial concerns about dual-class structures that provide perpetual or lifetime control. . . .

---

[318] Bebchuk & Kastiel, *supra* note 312, at 604 (citing Ronald J. Gilson & Alan Schwartz, *Constraints on Private Benefits of Control: Ex Ante Control Mechanisms Versus Ex Post Transaction Review*, 169 J. INSTITUTIONAL & THEORETICAL ECON. 160, 168–69 (2013) (suggesting founders can serve as "high-powered" performance monitor).

[319] Lucian A. Bebchuk & Kobi Kastiel, *The Perils of Small-Minority Controllers*, 107 GEO. L.J. 1453–54 (2019).

[320] *Id.*

[321] *Id.*



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu

> Permitting IPOs with a dual-class structure that sunsets after a fixed period of time (such as ten or fifteen years) unless its extension is approved by shareholders unaffiliated with the controller. The case for indefinite dual-class structures is untenable. . . .[322]

Professor Soshana Zuboff provides the following example of Mr. Zuckerberg's "super voting power to reject a shareholder proposal that would have required the company to report on its management of disinformation and the societal consequences of its practices. . . ."[323] Facebook's most recent proxy statement lists Mark Zuckerberg's age at 33.[324] It is sometimes hard to believe that Mr. Zuckerberg was only nineteen years-old when Facebook launched,[325] and twenty-seven when the company had its successful initial public offering.[326] Accordingly, seasoned corporate directors and others active in the field of corporate governance might question whether Facebook's current privacy crisis is the result of a controlling shareholder who has not had the benefit of serving on and observing high functioning boards with independent directors exercising risk management and other best practices. Is an explanation for the Facebook privacy crisis as simple as a naive yet highly successful young entrepreneur?

## XII. CONCLUSION

As it stands, the degree to which the allure of advertising revenues blinded Facebook to their complicit role in offering access to Facebook users to the highest bidder is not fully known. This Article cannot be a complete chapter in the corporate governance challenge of managing, monitoring, and oversight of individual privacy issues and content integrity on prominent social media platforms. The full extent of Facebook's experience is just now becoming known, with new revelations yet to come. All interested parties: Facebook users; shareholders; the board of directors at Facebook; government regulatory agencies such as the Federal Trade Commission (FTC) and Securities and Exchange Commission (SEC); and Congress, must now figure out what has transpired and what to do about it.

---

[322] Bebchuk & Kastiel, *supra* note 312, at 631; *see also* Lucian A. Bebchuk & Kobi Kastiel, *The Lifecycle Theory of Dual-Class Structures* (Dec. 2018), http://dx.doi.org/10.2139/ssrn.3300841.

[323] *See* ZUBOFF, *supra* note 48, at 511 (citing Hannah Albarazi, *Zuckerberg Votes against Shareholder Push For Fake News Transparency*, CBS *SF Bay Area* (June 2, 2017), http://sanfrancisco.cbslocal.com/2017/06/02/zuckerberg-shareholder-fake-news-transparency.

[324] Facebook 2018 Proxy Statement, *supra* note 40, at 10.

[325] Tom Huddleston, Jr., *Here's How 19-year-old Mark Zuckerberg described 'The Facebook' in his first TV interview* (Apr. 17, 2018), https://www.cnbc.com/2018/04/16/how-mark-zuckerberg-described-the-facebook-in-his-first-tv-interview.html.

[326] Facebook, Inc., Registration Statement (Form S-1) (Feb. 1, 2012) at 95, https://www.sec.gov/Archives/edgar/data/1326801/000119312512034517/d287954ds1.htm#toc287954_12.



Volume XX – 2019-2020 ● ISSN 2164-800X (online)
DOI 10.5195/tlp.2020.234 ● http://tlp.law.pitt.edu