THE IMPACT OF THE FACEBOOK COURT ORDER & CCPA 2020: HELPING BUSINESSES AND ACCOUNTANTS MEET THE CHALLENGE OF THE NEW ERA OF PRIVACY COMPLIANCE

Patrick M. Ryle
Dalton State College

Brett L. Bueltel
University of Southern Indiana

A. Kelly Walker
Mississippi State University

Carl Gabrini
Dalton State College

Mark A. McKnight
University of Southern Indiana

Key Words: privacy, compliance, customer data, regulation

JEL Classification(s): L51, M41, M48

Abstract

The regulatory and compliance environment regarding privacy issues has changed drastically in the past few years. With the California Consumer Privacy Act becoming effective on January 1, 2020 and the Federal Trade Commission's imposition of a $5 billion fine on Facebook for privacy violations on July 24, 2019, companies that utilize customer data are now finding themselves reevaluating their privacy practices. This article provides businesses and accountants with solutions to address these new privacy issues. First, the paper analyzes the new legal framework

of the CCPA and the FTC's action. Next, advice is provided for businesses to comply with the CCPA and respond to consumer requests for information. The paper concludes with a practical implementation plan for businesses to adopt.

INTRODUCTION

The digital age is offering opportunities for companies to fundamentally transform how they are conducting business. B2B (business to business) and B2C (business to consumer) transactions are now completed with the click of a mouse. Software is no longer installed on a computer but accessed through cloud-based connections. The digital innovation has not occurred without a cost. Society has been witness to, and victim of, an increasing number of data thefts resulting from unauthorized access to the data-storehouses owned by the companies taking advantage of the new technologies. As companies increase their use of computer and online technologies new risks have surfaced that might not be adequately addressed by traditional risk management strategies. The age of "big data" has resulted in the accumulation and storage of massive amounts of personally identifiable data about businesses, employees, and consumers. The existence of this treasure chest of information has proven too tempting to criminals across the world. Companies such as Target, Marriott/Starwood, Yahoo, Adult Friend Finder, Ebay, Equifax, and Heartland Payment Systems have suffered major breaches in their data security systems resulting in the theft of hundreds of million individuals personal and transaction data leading to identify theft and fraudulent purchases.

In a period of 24 months, the big-data and privacy regulatory and compliance landscape has seen massive changes. During this time, the European Union passed the General Data Protection Regulation ("GDPR"), California passed the California Consumer Privacy Act ("CCPA"), and the Federal Trade Commission ("FTC") imposed severe sanctions on Facebook, including a $5 billion fine for privacy violations, the largest fine in

U.S. history related to a privacy violation (Romm, 2019). Additionally, in June of 2018 the Supreme Court decided Carpenter v. United States, "dramatically reshaping the law governing historical cell phone location data" (Baker, 2019, p. 2). Many new legal requirements are already in place or will be soon. The GDPR is already in effect and the CCPA goes live on January 1, 2020, with enforcement beginning on July 1, 2020 (California Consumer Privacy Act of 2018). Complicating things even further, the Facebook Court Order went into effect on July 24, 2019. Barrett (2019) argues that the GDPR and the CCPA are quickly becoming de facto global standards for data privacy and protection.

The purpose of this article is to examine the provisions of the CCPA and the recent FTC action against Facebook and discuss the specific actions companies will need to consider taking to reduce the risk of a data breach and avoid significant financial liabilities associated with failure to adequately address this risk. Internal and external accounting and financial professionals must become familiar with the new regulatory environment emerging in the wake of these two significant compliance actions taken at the state and Federal level to properly advise their employers or clients.

MEETING THE CHALLENGES OF THE CCPA

The CCPA broadly expands the rights of California residents and requires covered businesses to comply with strict requirements on how they collect, use, and disclose "personal information" of California residents. The CCPA applies to a wide variety of organizations and individuals. In general, the CCPA applies to organizations which are a defined by the Act as a "business" (California Consumer Privacy Act of 2018) which collect personal information (or has it collected by others).

The Act protects data from a broad array of categories of "personal information," and is notable for its expansive breadth. The CCPA coverage includes but is not limited to personal data, genetic data, biometric data, geolocation data and health related

data. Accordingly, the information covered by the CCPA is very broad and inclusive and this should serve as a warning to all who do business in California. Based on Barrett's (2019) assumptions, the California rule is effectively the de factor standard on which privacy and security issues should be based so it provides guidance for those businesses outside of California.

California's willingness to adopt this sweeping and comprehensive new regulation breaks new ground in establishing privacy rights and responsibilities. Next, we will examine the impact of the CCPA from the perspective of the individuals it was designed to protect (consumers), and from the perspective of those who must comply (businesses).

RIGHTS OF CONSUMERS UNDER THE CCPA

The CCPA establishes four significant new rights for citizens involving their personal and transactional data being collected and stored by their employers and other businesses they interact with. These new rights included in the Act are:

- Right to know what personal information is being collected about them,
- Right to access a copy of the information being collected.
- Right to know if (and when) one's personal information is disclosed (and to whom), and
- Right to know if one's personal information is sold and the option to opt out of the sale.

(California Consumer Privacy Act of 2018).

Consumers may now request that a business delete any personal information and have the option to opt-out of third-party transfers of information. Specifically, Section 1798.105(a) of the California Civil Code provides a consumer the right to "request that a business delete any personal information about the consumer which the business has collected from the consumer" and Section 1798.115(d) states, "A third party shall not sell personal information about a consumer that has been sold to the third party

by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt-out pursuant to Section 1798.120" (California Consumer Privacy Act of 2018).

REQUIREMENTS FOR BUSINESSES UNDER THE CCPA

The new regulations contained within the Act will impact the financial performance of companies. Companies will incur compliance costs as they work to develop and implement new data management policies and procedures along with the processes necessary for notifying and responding to consumer requests regarding their personal data. Potential costs are also possible in the form of penalties, fines, and losses associated with civil suits imposed by the courts in response to violations of the provisions of the Act.

The Act will affect the ability of companies to generate revenue and profit from the sale of consumer data. The CCPA and any future new state or Federal regulations that further strengthen data privacy rights will threaten the entire business model that arose around marketing and selling individuals' data. Gandi, Thota, Kuchembuck & Swartz (2018) assert that many companies already leave "money on the table" related to data monetization, but the new regulations will now make it more difficult to take advantage of this stream of potential revenue.

Companies are still able to collect, store, and sell individuals' data under the CCPA, but the Act imposes the obligation that they notify consumers and manage their opt-out election, if made. Gandi et. al (2019) identify two ways that businesses benefit from data monetization. First companies may focus on improving internal operations and productivity. Secondly, they may adopt an external focus to create revenue streams by making data available to customers and/or partners. Businesses who wish to collect personal information must provide consumers information about data collection and use practices and will also be responsible for honoring consumer choice on the right to forbid the sale of data and will be required to inform consumers of the right to opt out. Businesses must also afford consumers the

right to make privacy decisions fear of retaliation or being treated differently (California Consumer Privacy Act of 2018). These obligations imply a concomitant obligation to engage with consumers and respond to requests and inquiries (and the associated costs to provide these services). Moreover, affected businesses will need internet homepages to include a description of the consumer's rights, along with a separate link to the "Do Not Sell My Personal Information" Internet Web page in its online privacy policy (or policies) as applicable.

In addition, businesses must inform consumers the categories of personal information collected and must inform consumers of "the purposes for which the categories of personal information shall be used" (California Consumer Privacy Act of 2018). Moreover, the CCPA limits a business to collecting information for a specific purpose, as opposed to any legal purpose, and provides that a "business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section" (California Consumer Privacy Act of 2018). These requirements will certainly pose a major challenge to many companies with business plans that are based on the acquisition and resale of consumer data.

CCPA PENALTIES & RIGHTS OF ACTION

In general, the CCPA contains provisions for serious penalties for non-compliance, and even provides consumers with certain rights to liquidated damages. Section 1798.150 of the California Civil Code provides consumers with a private right of action to recover damages up to $750 per incident or actual damages, as well as injunctive relief or declaratory relief. The CCPA does require consumers to provide businesses with an opportunity to cure. Accordingly, any data breach impacting vast numbers of users could be a catastrophic event for any holder of personal information, further dis-incentivizing the collection and storage of any information not deemed necessary.

FACEBOOK: DEFINING THE CHALLENGE CREATED BY THE FTC

Further complicating the privacy compliance landscape is the groundbreaking Facebook Court Order/Consent Decree of July 24, 2019. In this Court Order, the FTC (the agency charged with primarily regulating commercial privacy practices in the United States), resolved several outstanding complaint issues with Facebook. The FTC sought an enforcement action against Facebook alleging numerous privacy violations and dishonest practices dating back to and before an already existing FTC/Facebook 2012 Consent Decree. Demonstrating the serious nature of the violations and the growing frustration with the privacy practices of many leading technology companies, Facebook was required to pay a record-shattering fine of $5 billion. Particularly frightening to the compliance and auditing community is that Facebook received this fine after having received a clean bill of health on privacy practices from independent assessor PricewaterhouseCoopers.

Perhaps more importantly for the market, Facebook was required to agree to several changes in how it manages its data and privacy obligations. According to Commissioner Rebecca Kelly Slaughter, the settlement "intends to signal to other would-be violators that the FTC is taking a more aggressive approach to privacy and order violations than it ever has in the past" (Slaughter, 2019).

Throughout the Facebook Order and Consent Decree, the FTC imposes methods and techniques for solid internal privacy control such as:

- Assignment of authority and responsibility,
- Establishment of a strong control environment through the requirement of a comprehensive privacy program, and

- The requirement of a sound "privacy by design" architecture, including physical and information processing controls,

- Information and communication strategies through mandatory communication feedback looks,

- Monitoring by internal staff, as well as external staff through independent third-party review professionals as well as the FTC, and finally

- Segregation of duties between custody, authorization and recording of data transactions.
  (Federal Trade Commission v. Facebook, 2019).

By observing the conditions imposed on Facebook through this Court Order, the FTC has made its perspective clear related to sound privacy practices. This can help guide practitioners and companies in their effort to come into privacy compliance. In the following sections, recommendations for practitioners are presented for complying with these new legal requirements and practical steps to implement these approaches.

CONSIDERATIONS FOR CCPA COMPLIANCE

Disclosure obligations are extensive within the CCPA compliance framework. Initially, the Internal and Online Privacy Policy must be implemented to the extent that organizations are compliant by (or prior to) January 1, 2020. Guidance related to disclosures includes four key points. Organizations must disclose:

- what personal information is to be collected and for what purpose (Section 1798.110(c)(3)),

- a statement of a consumer's rights including methods for submitting privacy related requests (Section 1798.110(c)(3)),

- the nature of personal information collected in the previous year (Section 1798.110(c)(3)), and

- the nature of personal data sold or disclosed for business purposes in the previous year.

(California Consumer Privacy Act of 2018).

RESPONDING TO CONSUMER REQUESTS FOR INFORMATION

The CCPA also provides an affirmative obligation to respond to consumer inquiries within 45 days. This, of course, requires companies to develop the ability to respond to consumer information requests quickly, effectively and efficiently. The information required to be answered in such responses. Companies must be capable the following:

- Providing consumers with a detailed list of categories of personal information collected in the previous 12 months.

- Providing a list of what data was sold or shared, and with whom it was shared, in the previous 12 months.

- Providing a list of locations in which companies obtained personal information and from whom it was collected.

- Sharing with consumers the reason and purpose for which data was collected, shared, or sold.

DATA PROCESSING ABILITIES & IT INFRASTRUCTURE REQUIREMENTS

The CCPA grants consumers with the right to access a copy of the specific personal information collected about them. Consumer information may be provided electronically or by mail. As a result, companies must build software and organizational capability to:

- Identify all personal information the business has collected, from across the entire organization, and then to compile this data into a portable format that can be provided to the consumer.

- Securely authenticate the consumer's identity.

- Retain personal information for 12 months with policies for secure disposal of data once it is no longer needed.

- After identifying personal data, a tool and procedure must enable deletion of personal information from business servers upon request from consumer.

HUMAN RESOURCES APPROACHES

The human resources function within organizations is an essential element related to almost any compliance or regulatory issue. Companies should continuously monitor and evaluate human resources practices and materials against current and evolving regulatory requirements and strive to maintain consistency as well as timeliness. Companies should impose strict human resources controls limiting access to personal data to only those necessary. Written procedures should be put in place for all IT applications (as well as other areas of the business). Training and ongoing competency management practices should be implemented, maintained, and regularly evaluated and updated, as necessary.

THIRD PARTY CONTRACT & PARTNERSHIP REVIEW

A company's data sharing practices likely involve multiple third parties. These agreements and arrangements should be thoroughly reviewed. A review of third-party contracts and partnerships should include the following steps:

1. Conduct a comprehensive review of third-party data sharing practices.

2. Obtain a firm understanding of a third-party's compliance practices, including an independently performed privacy assessment or certification such as a WebTrust Seal of Assurance.

3. Establish a process of onboarding, and ongoing evaluation of third-party partners for purposes of reviewing compliance, and process for aggressively terminating sharing practices until compliance is demonstrated.

4. Establish due diligence for ongoing third-party partners for purposes of ensuring compliance.

IMPLEMENTATION RECOMMENDATIONS FOR PRACTICE

Implementation when managing and coping with continuing regulatory change has been identified as one of the biggest compliance challenges when it comes to new compliance initiatives. (English & Hammond, 2018). In addition to the general guidance for compliance, we have provided practical steps for implementation. The following recommendations should help guide successful implementation of compliance areas related to consumer privacy.

1. Time for a Privacy Checkup - Considering the recent string of regulatory and administrative events, it is critical for accountants and their clients to review current data and

privacy practices for compliance with existing and emerging legal requirements.

2. Establish the "tone from the top" – Companies must build a solid privacy culture by setting a privacy related "tone from the top" by making an organizational commitment to be clear, open and honest with data subjects about corporate privacy practices, and by incorporating into corporate culture responsible privacy practices.

3. Build a Strong Privacy Team and Program – Firms should establish a corporate multi-disciplinary privacy team devoted to assessing the current compliance, including legal, information technology, computer science, compliance, and human resources/training staff.

4. Conduct a Full-Scale Privacy Policy Review/Assessment – Companies should immediately conduct a full-scale review of:
    a. the corporate privacy policy
    b. data management architecture
    c. corporate data privacy acquisition and management practices.

5. Build/Revisit an Accurate Organizational Data Map – Organizations need to develop a detailed map of current data and privacy architecture and a data process flow map, as well as an assessment of what data the organization currently possesses.

6. Identify Compliance Obligations - Based on a review of corporate privacy and data management practices, firms must develop a clear picture of compliance obligations imposed from relevant jurisdictional regulatory regimes (e.g., CCPA, GDPR, Graham Leach Bliley, implications of Facebook Decision).

7. Adopt a Data Minimization Posture - Based on the corporation's business model, companies should assess data collection needs, and consider revising corporate data collection practices by adopting a "lean data" acquisition posture. By collecting minimum information necessary to meet business objectives, companies can drive down compliance obligations and associated costs. Also, by utilizing innovative strategies, such as differential privacy, it may be possible to possess data, without said data qualifying as personal data, thus driving down compliance obligations and costs.

8. Strengthen Compliance Architecture and Capability – Firms must develop corporate information technology infrastructure and software ability to meet compliance obligations. Doing so at an affordable cost will be aided by a lean data acquisition posture.

9. Employ Human Resources Controls – Organizations should develop personnel processes, specify access controls, and develop training programs to implement privacy compliance.

10. Assess third parties – Managers must examine existing relationships with third-party partners in data transfer agreements, require said parties to certify to the organization their compliance with data and privacy requirements.

11. Develop Institutional Response Capability – Firms must develop a strong incident response team and protocols for events such as data breaches.

12. Develop Consumer Response Capability - New regulatory regimes require holders of data to be able to respond to

consumer demands for information within a very short time window. Companies must develop the capability to meet these requests considering potential consequences of non-compliance.

13. Choose a Compliance Strategy - With many different regulatory regimes with which to comply, organizations must decide upon a compliance strategy that is best suited to organizational needs. Companies can choose between a jurisdiction-by-jurisdiction approach, or can potentially reduce some complexity and associated costs by choosing in each policy instance, of complying with the most restrictive standard across an organization

14. Employ "Privacy by Design" – Executives must build corporate cultures focused on developing and maintaining a privacy architecture as corporations' most important form of internal privacy/data control, by designing control systems in such a way as to minimize required human decision-making.

15. Require Regular Privacy Compliance Certification by Management - CEO and CIO/CPO must regularly (at least annually) certify the effectiveness of its privacy architecture and control design. Also, firms must conduct Privacy Impact Assessment when any events occur which may impact privacy practices or obligations (such as new software acquisition, or a new regulatory obligation).

16. Develop by Corporate Charter, an Independent Privacy Committee on the Board of Directors - The creation of an independent privacy committee, (much like a required audit committee) should be composed primarily of independent members who should be responsible for organizational oversight of corporate privacy practices.

17. Require Appointment of Independent Assessor - An independent assessor should be appointed to report on privacy compliance every year.

18. Independent Assessor Should be Appointed by B.O.D. Privacy Committee - The Board of Directors Privacy Committee should appoint the intendent assessor and control compensation.

19. Whistleblower Protection - A mechanism for reporting privacy and data problems should be designed and implemented with protections for whistleblowers.

20. Clawback Provision - Corporations should include claw-back provisions holding executives responsible for privacy violations fueling incentive based compensation.

21. Segregate the Data Management Function. Segregate the data management/holding function from the revenue generation function. Also, corporations should put in place strong supports for independence of data management and privacy decisions (insulation from the revenue generation function), including having Chief Privacy Officer report to an independent committee of Board of Directors.

CONCLUSION

Companies are no longer going to be free to collect, store, sell, and purchase personal data of their customers as they wish. The passage of the California Consumer Privacy Protection Act in 2018 on the heels of the page of Europe's passage of the GDPR presents clear compliance challenges. The scope of the regulatory environment has been further complicated by the FTC decision against Facebook. Companies will need to carefully examine the new requirements and modify their policy and procedures over data management to ensure they adequately protect themselves from enforcement actions, fines, penalties, and civil damages

resulting from violations. Accountants and other financial professionals have an opportunity to add value to their employers and clients by providing them with sound advice as they move to change their data management processes. This article lists a series of suggestions to consider in making the necessary changes. Companies must also add data privacy rights enforcement to their enterprise risk management system to ensure it is continually examined.

REFERENCES

Baker, William B. 2019. A Big Year in Data Privacy and Security. Scitech Lawyer, 15(3): 2-3.

Barrett, C. 2019. Barrett, C. 2019. Are the EU GDPR and the California CCPA Becoming the de facto Global Standards for Data Privacy and Protection. *Scitech Lawyer, 15*(3): 24-29.

California Consumer Privacy Act of 2018, California Civil Code § 1798.100.

English, Stacey, & Hammond, Susannah. 2018. *Cost of Compliance 2018.* Thomson Reuters.

Federal Trade Commission v. Facebook. 2019.

Gandhi, Suketu, Thota, Bharath., Kuchembuck, Renata, & Swartz, Joshua. 2018, November 27. Demystifying Data Monetization. *MIT Sloan Management Review*. Retrieved online October 2019 from sloanreview.mit.edu.

Romm, Tony. 2019, July 24. U.S. Government Issues Stunning Rebuke, Historic $5 Billion Fine Against Facebook for Repeated Privacy Violations. *The Washington Post.* Retrieved October 2019 from www.washingtonpost.com

Slaughter, Rebecca Kelly. 2019. Federal Trade Commission v. Facebook: Dissenting Statement.