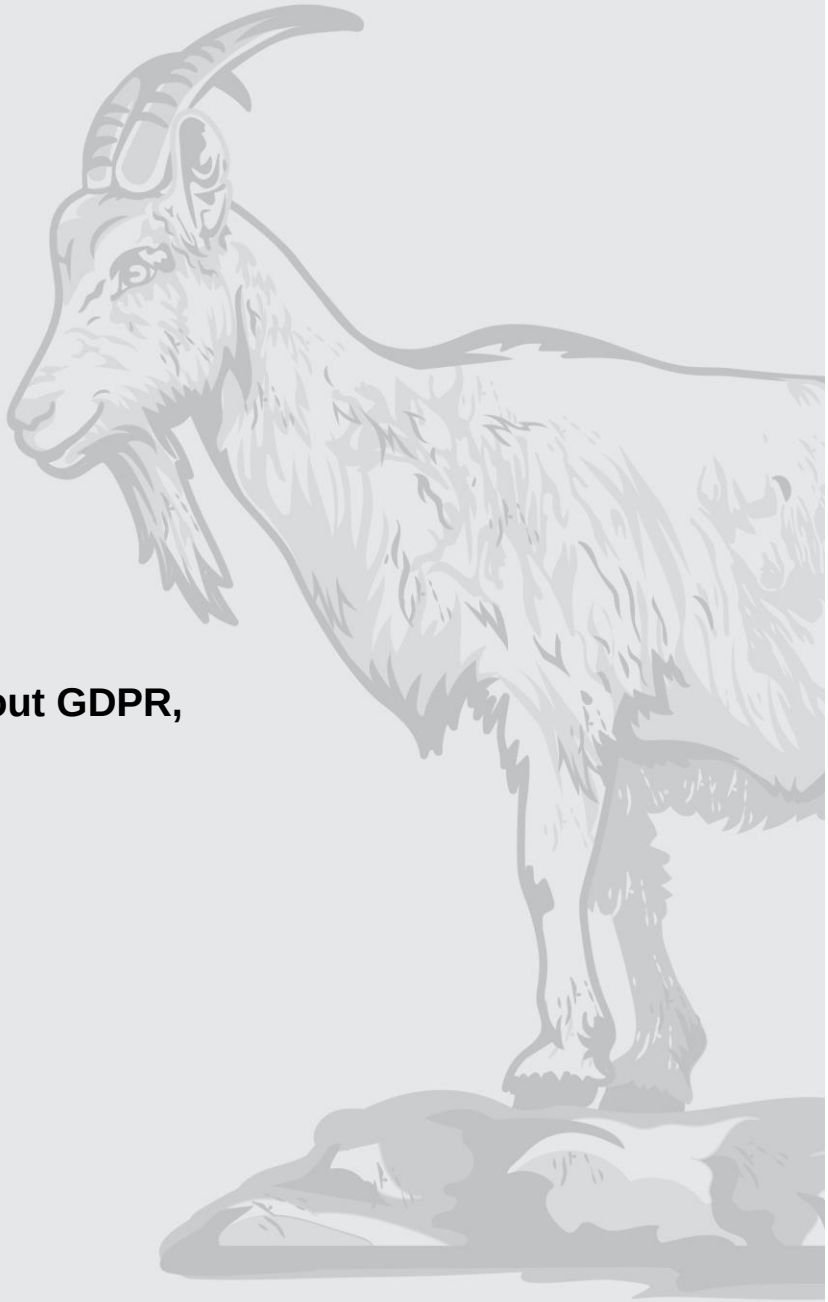


Data Privacy

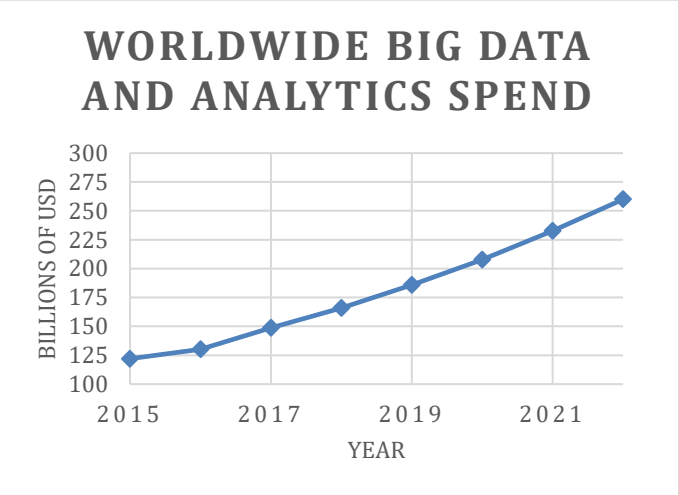
What You Need to Know About GDPR, CCPA, and Data Regulation

W. Capra
CONSULTING GROUP

221 NORTH LASALLE STREET, CHICAGO, IL 60601 | 312-873-3300 | INFO@WCAPRA.COM | WCAPRA.COM

Introduction

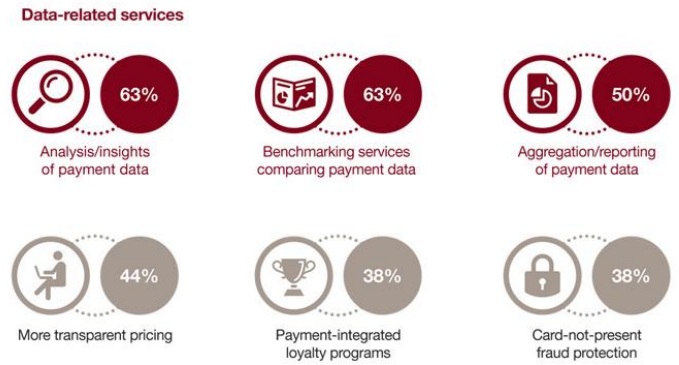
Were you one of the 90 million Facebook users that had to log back into their account following the data breach announced at the end of September? Data breaches are becoming a near-daily part of the standard news cycle and they are becoming more prevalent as companies are collecting, storing and processing more data to support business goals. In addition, data breaches are having a greater impact due to the amount of data companies are collecting. Data analysis is an enormous industry worldwide and is continuing to grow; projections show worldwide spending on big data and analytics eclipsing $260 Billion by 2022.



[1]

Merchants, in particular, see immense value in data, and are constantly looking for new ways to leverage existing data, and looking for new, more robust, sources of data.

"In your view, what are the top three value-added services merchants would most like to see payment service providers offer?"



[2]

Data related services are the top three value add services Merchants want from payment providers, according to the PWC Consumer Payment survey.

In response to the increasing concern over consumer data privacy, numerous government entities are evaluating and drafting consumer data privacy protection laws. The European Union was a first mover in the space, as enforcement of the General Data Protection Regulation (GDPR) started in May of this year. California recently passed the California Consumer Privacy Act (CCPA) in June of this year with enforcement currently set for no later than January 1, 2020 and there are strong signs that more US states will follow suit. Add to this the prospect of privacy regulation at the US federal level, and US-based merchants will continue to be presented with more complexity in this already murky space. This paper will help break down what is in both the GDPR and CCPA, provide insights into future regulations and discuss the impacts data privacy laws have on merchants.

What is GDPR?

GDPR is a law passed by the European Union (EU) to protect the data privacy rights of all EU citizens. GDPR defines personal data as "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". Merchants that control or process personal data of EU residents must comply with GDPR – regardless of where the organization is based and conducts its business [3]. GDPR is an extensive regulation; the following highlights some of the actions merchants are now required to take:

- Ensure data is processed lawfully, transparently, and for a specific purpose.
- Record an active, deliberate action by the consumer to collect their data but must also allow individuals to withdraw their consent at any time. (i.e. – clear consent language with a customer-driven event, like depressing an "I Accept" button.)
- Respond to requests by consumers to provide information on how data is collected, the purpose of the data and how the data is processed
- Provide a mechanism (system or process) that enables individuals to request their data be deleted at any point (also known as "right to be forgotten") or request incorrect or incomplete information to be rectified
- Maintain a "data registry" – a record of what data the company possesses and the purpose of the data

Most importantly for merchants ("controllers" in GDPR terms), violations of GDPR come with hefty penalties, including up to 2% of annual revenue or €10 million (whichever is higher) for failing to report a data breach within 72 hours. This penalty doubles for breaches that include personal data [4]. Fines will be proportional to the size of the breach, which brings into question how these fines will be doled out. At the time of this writing, there have not been any fines collected for breaches of GDPR, but regulators expect the first round of sanctions by the end of the year [5].

Immediate Impacts of GDPR

While the EU has not yet publicly distributed any fines for infractions of GDPR, the establishment of new regulations has already made a significant impact on merchants. Many merchants chose to refresh consents to meet the affirmative action requirement of GDPR, leading to floods of emails to consumers in the lead up to the GDPR enforcement deadline. Some merchants have chosen to block EU users, either temporarily, until they are fully compliant, or indefinitely, to avoid GDPR regulation altogether [6]. It is clear that the potential for substantial fines are creating concern for merchants worldwide, causing them to re-evaluate their strategy regarding engagement with and services provided to EU citizens.

In addition to organizational changes, there are several ongoing complaints and investigations. A non-profit privacy organization launched complaints against popular companies such as Google, Facebook, WhatsApp and Instagram the first day that GDPR regulations came into effect. Meanwhile, another privacy advocacy group launched investigations into companies known for behind-the-scenes trading of personal data such as Acxiom, Criteo and Quantcast.[7][8][9] In June, an investigation into 400 public sector organizations in the Netherlands found that 4% of the organizations had not yet appointed a data protection offer (DPO), a requirement for all public sector organizations. In mid-July, the Dutch Data Protection Agenda (Dutch DPA) launched an "ex officio" investigation into 30 randomly selected large private companies (more than 250 employees) in various sectors regarding their data registries [10]. More recently, Facebook is facing an investigation related to the September 24th breach and Twitter is being investigated for refusal to give a user information about how it tracks users when they click links in other people's tweets.

The first GDPR Enforcement Notice issued by the Information Commissioner's Office (ICO) occurred on July 6th but was not publicly available until September. The enforcement notice was sent to AggregateIQ Data Services Ltd for failing to comply with Article 5 (1)(a)-(c) and Article 6 of the GDPR and is likely a response to their role in the of the Facebook unauthorized data-sharing scandal. The Enforcement Notice threatened administrative penalties however, as of September 25th the case has been appealed and is awaiting the first-level tribunal[11]. British Airlines is facing a potential $650 million class-action lawsuit, one of the first GDPR class-action lawsuits due to a data breach. The incident occurred August 21st – September 5th and customers were notified on September 6th, according to the company) [12]. According to the lawsuit and GDPR regulations, breach victims can seek 'Non-Material Damage' compensation in the case of data breaches. While we don't know if this case will turn into an arduous court battle or a financial settlement, this example shows that the GDPR administrative fees should not be the only concern for merchants. Even in the infancy of GDPR regulation taking effect, companies are already starting to feel a slew of impacts beyond administrative penalties.

Immediate Impacts of GDPR:

- Organizational changes
- Negative consumer experiences
- Lost sales
- Negative press coverage
- Formal investigations
- Class-action lawsuits

What is CCPA?

The California Consumer Privacy Act follows suit with many of the requirements of GDPR, except when it comes to penalties. CCPA applies to any company that processes or controls data on a California resident. As California represents 12% of the US population, CCPA applies to a large portion of companies that operate in the US. The main tenants of the CCPA are laid out as follows:

(1) The Right of Californians to know what personal information is being collected about them.
(2) The Right of Californians to know whether their personal information is sold or disclosed and to whom.
(3) The Right of Californians to say no to the sale of personal information.
(4) The Right of Californians to access their personal information.
(5) The Right of Californians to equal service and price, even if they exercise their privacy rights.

[13]

There is still considerable vagueness in the way CCPA was written and uncertainty for how it will be enforced. The CCPA was written and brought to law quickly with the intent of revisions and further clarifications from merchant feedback and lessons that are learned. The law includes the 'right to be forgotten,' as well as a wide definition of personal data, like GDPR. The CCPA calls for civil penalties up to $7,500 for each violation, which is a fraction of the penalties imposed in the GDPR. However, if a class action lawsuit is initiated, companies may be liable for "statutory damages between $100 - $750 per consumer per incident" depending on the severity of the breach [14]. The CCPA has wide reaching implications to businesses operating in the US and will increase the complexity for merchants adapting to GDPR regulations.

What does CCPA mean for merchants?

January 2020 may be over a year and a half away, but your organization's roadmap probably stretches beyond that date with little room in the budget for data privacy projects. It is critical to evaluate the scope of impact that CCPA has on your current business and future initiatives. Meeting CCPA requirements may demand significant investment of both time and budget.

Merchants should focus on the following areas in preparation for CCPA:

- Consent language on digital platforms
  - Example: Explain the purpose for collecting user data
- Enhanced security measures
  - Example: Utilize End-to-End Encryption or Tokenization to store payment data
- Disclosure and breach notification
  - Example: Establish a disclosure and breach notification plan to meet requirements
- Consumer-facing support
  - Example: Create processes for responding to consume requests for data or data deletion
- Legal and privacy preparation
  - Example: Engage legal experts to provide guidance on the vague aspects of data privacy laws

If data is a critical component of your business, the risk and costs associated with maintaining consumer data escalates substantially. If the CCPA isn't enough to turn your attention to data privacy, consumers' expectations and the potential fallout of a data breach should be. When it comes to data privacy, keeping your business out of the headlines should be the highest priority.

How do GDPR and CCPA Compare?

Comparison: GDPR to CCPA		
Area	**GDPR**	**CCPA**
Appoint Data Protection Officer	Required (Public sector and specific industries)	N/A
Affirmative consent action	Required	Required
Right to request data	Required	Required
Right to be forgotten	Required	Required
Right to refuse sale of personal information	Required	Required
Data Registry	Required	N/A
Equal service and price	N/A	Required
Administrative Penalties	Up to €20 million or 4% of global turnover, whichever is higher	Up to $7,500 per violation
Consumer Lawsuits	Right to receive compensation for damage suffered	$100 - $750 per consumer per incident

Conclusion

We are still at the beginning stages of data privacy laws, and we expect many more regulatory bodies to enter this space in short order. Expect more countries and US states to begin adopting their own regulation with varying levels of severity, which undoubtedly will create a complex web of data protection laws that multi-national companies will find difficult to navigate and/or abide by. Domestically, anticipate more states passing laws similar to CCPA until broader regulation passes through the federal system. Congress has held hearings with top technology executives from firms such as Facebook, Google, and Twitter as it relates to breaches and data privacy, which signals that federal regulation may be on the horizon. As the complexity of compliance increases, so will the cost and risk of non-compliance. Organizations must thoroughly prepare for the current regulations and be agile enough to consider regulations yet to come.

We urge companies to start now and stay ahead of data privacy regulation to protect against the negative impact of regulations and consumer lawsuits. Implementing agile, streamlined processes to meet the strict requirements from various levels of government is essential to reducing the risk and repercussions of data privacy regulation. Start by ensuring your organization has a plan in place for compliance with GDPR and CCPA, and continue to re-evaluate internal processes and decisions as new regulations are implemented. Data privacy requires resources from both business and technical perspectives, but also subject matter experts and legal perspectives. Data is extremely valuable, but it will become a liability for your organization if you do not act quickly.

If you have additional questions regarding data regulation and its implications, please contact Danny Omiliak (domiliak@wcapra.com, 312-873-3300).

Sources:

[1] http://www.pressreleasepoint.com/worldwide-semiannual-big-data-and-analytics-spending-guide
[2] https://www.strategyand.pwc.com/reports/serving-connected-customers
[3] http://www.itpro.co.uk/it-legislation/27814/what-is-gdpr-everything-you-need-to-know
[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
[5] https://www.cnbc.com/2018/10/09/reuters-america-exclusive-eu-privacy-chief-expects-first-round-of-fines-under-new-law-by-year-end.html
[6] https://www.theguardian.com/technology/2018/may/24/sites-block-eu-users-before-gdpr-takes-effect
[7] http://fortune.com/2018/05/25/google-facebook-gdpr-forced-consent/
[8] https://www.theguardian.com/technology/2018/oct/03/facebook-data-breach-latest-fine-investigation
[9] http://fortune.com/2018/10/12/twitter-gdpr-investigation-tco-tracking/
[10] https://iapp.org/news/a/dutch-dpa-launches-ex-officio-gdpr-compliance-investigation/
[11] https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf
[12] https://www.bankinfosecurity.com/british-airways-faces-class-action-lawsuit-over-data-breach-a-11478
[13] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
[14] https://www.clarip.com/data-privacy/california-consumer-privacy-act-fines/

About W. Capra

W. Capra Consulting Group is an industry leader in providing IT and business focused advisory and professional services in retail technology. Since the year 2000, we have helped organizations of all sizes understand, develop, and execute strategies to solve the toughest challenges related to payment acceptance, technology adoption, and data security. Our team is composed of industry experts who possess deep insight and experience across the industries that we serve.