# Making Privacy Operational

**Talya C. Parker**

**INTRODUCTION:** The nature of the privacy profession as a legal and compliance discipline has changed. While the core of privacy professionals who are compliance and legal continues to grow, the roles of technologists, marketing, human resources, member services and data analytics are all potential newcomers to the profession. At this moment in time, the privacy profession has become very multi-faceted. In fact, adapting to such changes will play an incredibly important role in ensuring organizations are properly protected against privacy risks. [24] With the growth of technology, and company desire to maintain their competitive advantage through trends such as big data; consumers are bombarded with a number of products and advertisements in a very invasive way.

- Companies are finding creative ways to market to their employees as consumers; and
- Social media have added an interesting flavor to the world of privacy, especially as it relates to cookies

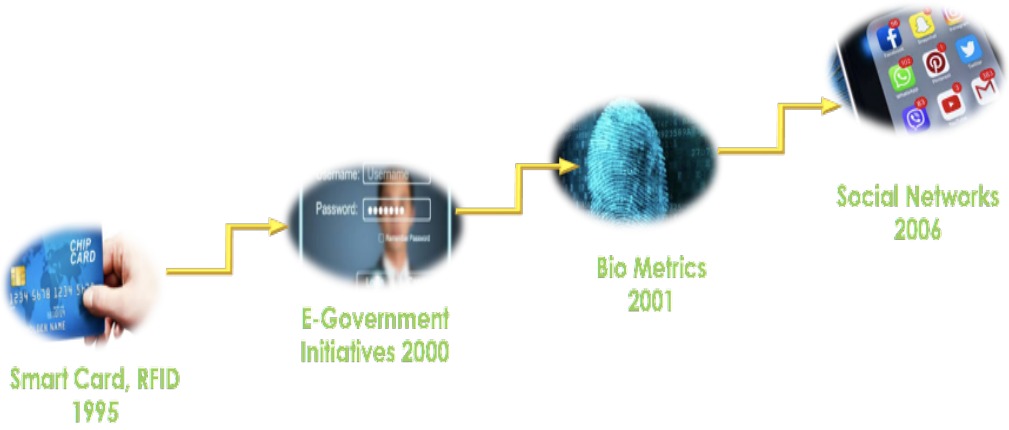
All of these changes and innovative ways we conduct business in the 21st century, have impacted privacy laws over the years, and along with it, the growth of public concern around the use of computers to process and store personal data.

**CHALLENGE**: While the enforcement of new laws is great, it's also challenging to interpret, understand its applicability, and quickly implement them throughout the business. If your privacy program is limited to address only the legal aspects of privacy, essentially, the message is the prioritization of protecting the business. While that's absolutely necessary, one may also want to factor in the group that enables your business and makes it profitable; your customers. Having a program that is more holistic, inclusive and expands its reach throughout the enterprise — shifts the messaging to one that also prioritizes its clients and consumers.

What does this mean for the "potential newcomers" to privacy who sits in marketing, human resources and technology? Organizations such as the International Association for Privacy Professionals (IAPP) was created to address the evolving need for training and education within the privacy profession. "With each passing year, new technologies prompted new concerns:

- Smart card technologies first appeared in 1995, along with loyalty card schemes and RFID technology

- E-Government initiatives became a discussion point in 2000, and biometric systems appeared in several annual reports from 2001 onwards; and
- Meanwhile, social networking was first broached in 2006." [8]




As a result, to these changes, consumers are demanding more transparency, the right-to-be-forgotten and access to the data organizations collect on them; and quite frankly, lawmakers are listening. While trying to keep the pace of changes in privacy law, how can organizations maintain their competitive advantage when the laws and regulations are changing quicker than it can be implemented? How are organizations and privacy professionals positioning themselves to address the evolving needs of privacy? My research consisted of a number of approaches:

- ***Research Question 1:*** *How are privacy organizations such as the IAPP leveraging their programs and certifications to operationalize privacy in a more inclusive and holistic way?*
- ***Research Question 2:*** *What types of training and privacy education are currently being used to address growing business needs? What privacy curriculums are being produced by Universities, if any? My objective is to identify the gaps and propose a holistic view.*

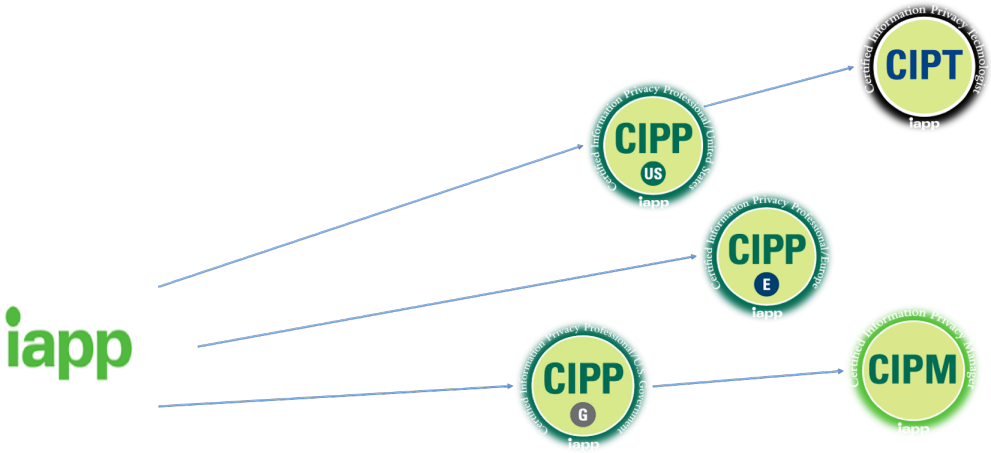
**Research #1:** The IAPP has developed many certifications to address privacy laws by sector, industry, and country.

- **CIPP/US:**
  - The U.S. Private-sector Privacy Certification is one of the most highly valued privacy certifications. Its credentials demonstrate that you have a strong foundation in U.S. privacy laws and regulations and an understanding of the legal requirements for the responsible transfer of sensitive personal data to/from the U.S., the EU and other jurisdictions. While this serves very foundational in understanding how the laws of privacy influence internal rules for our

organizations, it doesn't address how to perform such duties as a privacy professional in the 21st century. More interestingly, what does this mean to the "new comers" of privacy with no legal background?

- **CIPP/E:**
    - According to the IAPP, this credential demonstrates comprehensive GDPR knowledge, perspective and understanding to ensure compliance and data protection success in Europe. This certification is structured very similar to the CIPP/US, heavily influenced by laws and regulations. While this outline provides a deep understanding of European law as it relates to Privacy, it doesn't internalize its' applicability for the business in an operational context.
- **CIPP/G**:
    - According to the IAPP, CIPP/G's focused on U.S. government privacy laws, regulations and policies specific to government practice. Over the past few years, the CIPP/G enrollment has been on a decline. Pulling in single-digit numbers monthly for test takers in comparison to CIPP/E at 500 test takers a month, and the CIPP/US pulling in between 200 and 300 and month. The volume demonstrates value and is also a reflection of the emphasis the current Administration places on privacy. Having a more holistic and more operational approach to these certifications may prove more valuable as policies and laws are constantly changing.
- **CIPT:**
    - The IAPP designed a certification that would be more inclusive of technology pros. I always found this to be the most valuable as a cybersecurity and data privacy professional. According to the IAPP, this credential demonstrates you have the required knowledge to build your organization's privacy structure from the ground up. Privacy-by-design is a huge factor when building products and services, and as a result, the job market for privacy-trained IT professionals has increased.
- **CIPM**:
    - The Certified Information Privacy Manager is considered to be more closely aligned to an operational design. The IAPP recognized that it was quite daunting for privacy professionals to wrap their heads around the laws, regulations and policies in this field. The purpose of this

certificate was designed to be more operationally focused, and to address the evolution of business management practices. The minor challenge here, is that it narrows it focus on roles such as chief privacy officers, corporate privacy managers, compliance officers, risk managers, information security and auditing professionals. What about the "new comers"? How much applicability does this have to the marketing and data analytics teams who are marketing to consumers and designing innovative ways to use data in order to increase gross profits?




While these resources have proven invaluable, companies are still struggling with the development of their internal privacy programs. However, I'm hopeful, the IAPP continues to drive many efforts and partnerships to address these challenges. With privacy heavily influenced by law, privacy programs are often aligned with their legal departments; in some cases, technology. Through the review of existing privacy curriculums via the IAPP and additional resources, my findings suggest curriculums are disproportionately structured to focus on privacy law or in one-off cases, computer science. While privacy can be preferential and driven by business, personal or professional needs, privacy spans across many disciplines and should not be limited to law or technology. This paper highlights the shifting landscape of privacy as it relates to current trends and my proposal towards a more holistic - educational approach. Additionally, I've proposed a framework that could potentially influence the way we teach privacy (*in corporate or at the collegiate level*) and influence more diverse learning opportunities through privacy education.

**Research #2:** According to the National Center for Education Statistics (NCES), there were 1,895,000 bachelor's degrees conferred between the year 2014–15 with the highest number resulting in the field of business (364,000). Consecutively, in 2015-16 the highest degrees conferred were in the field of business (371,694). [1] There is an

uptick in this area of study, and while this is just one example of many disciplines that could have privacy baked-in, I find it significantly valuable to explore and strategically build privacy modules that could easily be embedded into a variety existing business curriculum including: marketing, human resources and data analytics.

Based on research, the School of Business continues to provide a significant lead on a number of degrees acquired at the graduate and undergraduate level. With core undergraduate courses such as business law, communications, marketing, and management; privacy is an important element to any degree program and should serve foundational to core curriculums. MBAs from top reputable institutions, allow students to exercise the leadership skills they will practice in business and beyond; and leave with lessons in leadership that are practical, priceless and most importantly, real. At Harvard's School of Business, MBA students are required to focus on leadership, organizational behavior, and corporate accountability. Each of these areas fosters an environment conducive to building and embracing leaders — the leaders who become influential board members or executives within their organization. Why not reach them in the classroom and at a level where they can be most influential with driving privacy education? Privacy professionals should understand how an entire enterprise function which builds on the concept of privacy-by-design. Privacy should be baked-in at every level and every aspect of an enterprise and one can accomplish this, by enabling "newcomers" to become more privacy aware and educated in their daily roles. Alternatively, leaders who serve their enterprise in influential ways should also understand how privacy applies to their business and establish a culture of privacy that matriculates from the top-down. As a previous consultant, currently serving as a privacy industry professional, I have observed how organizations rely heavily on vendors to operationalize their business and cut cost for a variety of reasons. Privacy is becoming more about operational data risk management and designing an approach that enables increased monitoring and tracking business processes, internal auditing, and working with internal teams to mitigate or remediate current and future state risks.

**Observations**: Organizations are becoming data-driven by increasing the collection of data in order to learn more about their consumers. In order to achieve this, companies can become very vendor reliant; vendor reliance means sharing the data you've collected from your consumers as a result of consumer trust. Even with third-party contractual agreements, brand reputation is always at risk when data leaves your organization. In rare cases, vendors receive blame or suffer from brand damage as the result of a breach, Target is the perfect example. Compliance with

privacy law does not mean security. And while organizations are scrambling to remain compliant, there is a significant opportunity for privacy to become an enabler of the business.

**Use Case:** Apple does an excellent job leveraging this approach, and although, I'm partially biased as an Apple user, I believe this makes them a differentiator in the market. Apple creates innovative ways to safeguard consumer data on their device; they are very transparent about how they personalize user experience and how they protect the data we freely give. Apple have mastered skills such as differential privacy to improve user experience while implementing the necessary protections, and providing notice, choice, and transparency.

- Functionalities such as Apple Pay, allows users to add their credit, debit or prepaid card and actual numbers are never stored on the device or Apple's servers. Instead, a unique device account number is generated and encrypted in a way that not even Apple could decrypt. The device account number is stored locally but walled off from user operating systems. Apple does not track what users are buying, so they cannot build a purchase history to serve ads, a function that most corporations would leverage.

This is the perfect demonstration of how privacy can be used to enable the business. And when you extend your privacy program beyond complying with the law but include the concerns of your clients and customers, you become the differentiator in the market amongst competitors.

**Research #2:** My approach to making privacy operational includes an assessment of educational curriculums that addresses privacy. I reviewed resources to identify if there were existing curriculums or training to address this. The IAPP has developed a program called, "Privacy Pathways" which enables them to partner with many schools and universities to enhance privacy education and to assist students in certifying as IAPP privacy professionals. "The Santa Clara University School of Law's first-of-its-kind privacy law certification is an example of the IAPP's success in this area. The organization's VP of Research and Education Omer Tene states, "we're at a time when data is becoming quite valuable in currency, the need for well-qualified professionals who understand global information management practices and the need to safeguard data are growing exponentially." I agree, there is an increased value in data and companies who were not data driven in the past, are considering how they can be.

Unfortunately, the majority of these partnerships through the IAPP are driven by law schools. While valuable, it's extremely limiting to the privacy profession of the 21st century. I would strongly encourage the IAPP to expand its Privacy Pathways program to other non-legal academic programs. [11] We envision tomorrow's privacy managed teams to be comprised of an organization's business centers, i.e., finance, marketing, human resources, information technology, information security, etc. "We envision tomorrow's CPOs working with the organization's senior executives to manage the organization's strategic information privacy program. They will ensure privacy is interwoven into every facet of the strategic plan's enterprise and mission objectives." [11] I've illustrated a break-down of the IAPP's participating Universities, the department that owns and drives privacy education courses within that school and a summary of their curriculum. Through my research, the theme of 'law' driven privacy curriculum is evident and pretty consistent across the board.

**University Curriculums**:

Privacy Law Certificate

[As submitted to the faculty May 2014]

**Requirements.** A Privacy Law Certificate candidate must satisfy the following requirements:

1. *Coursework.* A candidate must complete, with a C or better (or P, where pertinent): (1) Privacy Law, (2) a Comparative Privacy Law, and (3) at least 3 elective courses from the following list:

| | |
|---|---|
| Advanced Torts | Health Law I |
| Advertising & Marketing Law | Intellectual Property |
| Consumer Protection | Internet Law |
| Criminal Procedure: Investigations | Legal Issues of the 21st Century |
| Employment Law | Rights of Publicity |
| E-Discovery | Technology Licensing |

Not all of these courses are regularly offered. The Certificate Supervisor may designate or approve other elective courses that have a substantial focus on privacy issues.

Privacy Law and Comparative Privacy Law must be taken on a graded basis. The electives may be taken on a P/NP basis.

2. *Paper.* A candidate must publish a paper on a privacy-related topic in a publication likely to be read by privacy professionals. The paper can range from a law review article to a blog post or newsletter entry. Topics and publication venues require Certificate Supervisor pre-approval.

3. *International Association of Privacy Professionals (IAPP) Certification.* At graduation, a candidate must have one of the following IAPP certifications in good standing: CIPP/US (the recommended choice), CIPP/IT or CIPM.

4. *Experiential Learning.* The candidate must complete an externship or clinic, pre-approved by the Certificate Supervisor, that relates substantially to privacy issues. Alternatively, the candidate may satisfy this requirement through a pre-approved paid job (at least 150 working hours) during law school focused on privacy issues.

**Other Details**

Carnegie Mellon University

Master of Science in Information Technology

privacy ENGINEERING

Introducing a one-year Master's degree to train privacy engineers

The **Master of Science in Information Technology – Privacy Engineering** degree is a one-year graduate program for computer scientists and engineers who wish to pursue careers as privacy engineers or technical privacy managers. Designed in close collaboration with industry and government, this program is intended for students who aspire to play a critical role in building privacy into products, services, and processes.

This first-of-its-kind program responds to the rapidly growing need for technical privacy expertise. Both industry and government organizations have created positions for people responsible for **ensuring that privacy is an integral part of the design process.** Privacy engineers work as part of multi-disciplinary teams. They have to **understand technology** and be able to **integrate perspectives that span product design, software development, cyber security, human-computer interaction, as well as business and legal considerations.** Organizations are reporting a shortage of people who are adequately trained to play this increasingly crucial role.

The MSIT-Privacy Engineering program is a full-time masters program for students at Carnegie Mellon's Pittsburgh campus. It requires 192 units to complete and offers two tracks: 12-months (Privacy Engineering) and 16-months (Privacy Engineering Practice). The 12-month program concludes with a summer long, learning-by-doing capstone project, where students will be brought in as privacy consultants to work on client projects. Students in the 16-month track will gain work experience through summer internships and complete the capstone project in the fall.

Training students for jobs in industry and government

Students who complete the program will be well prepared for jobs as privacy engineers and technical privacy managers. Our graduates work for Google, Oracle, eBay, Adobe, and other companies. Students will be trained to:

- design cutting-edge products and services that leverage big data while preserving privacy
- identify points where privacy may be at risk, and propose and evaluate solutions to mitigate these risks;
- understand the capabilities and limitations of privacy enhancing technologies;
- use techniques to aggregate and de-identify data, understand the limits of de-identification and how data might be re-identified, and understand concepts such as k-anonymity and differential privacy;
- understand the current privacy regulatory and self-regulatory frameworks;
- understand current technology related privacy issues including tracking for online behavioral advertising, location

in Information Privacy Law

| UNIVERSITIES | SCHOOL | CURRICULUM |
|---|---|---|
| Carnegie Mellon University | School of Computer Science and College of Engineering | • CMU created a CyLab and researchers work to ensure that as new devices and technologies are created, digital privacy remains protected.<br>• CMU also has a Master of Science in Information Technology – Privacy Engineering program which is intended for students who aspire to play a critical role in building privacy into future products, services, and |

| | | |
|---|---|---|
| | | processes. |
| University of Maine | School of Law | • The University of Maine has a Certificate in Information Privacy Law and its' curriculum is inclusive of an experiential learning component. The curriculum is heavily influenced by law. |
| High Tech Law Institute Santa Clara Law | School of Law | • This Institute focuses on advertising law, consumer protection, healthcare regulation, internet law and the legal issues of the 21st century. |
| Indiana University | School of Law and Business | • IU provides a graduate certificate in information privacy law and policy. Topics include: cybersecurity, health privacy law, information privacy and security management practicum and information security law. |
| Queen Mary University of London | School of Law | • This program introduces a number of areas that focuses on a variety of laws, including curriculums that introduces students to the critical role played by regulators in global markets. |
| University of Minnesota | School of Law | • This program introduces a number of specialty areas including but not limited to:<br>○ Business Law<br>○ Civil Litigation<br>○ Health Law & Bioethics<br>○ Human Rights Law<br>○ Intellectual Property & Technology Law |

| | | |
|---|---|---|
| Northeastern University | School of Law | • This University have a number of dual concentrated programs. Their program expand upon a wide range of interdisciplinary and research projects, including the Center for Health Policy and Law, the Program on Human Rights, the Global Economy and the IP CO-LAB. |
| Saint Louis University | School of Law | • This program is inclusive of J.D., dual-degree, part-time and L.L.M programs. law students at SLU may also earn a concentration in the following areas:<br>○ Employment Law<br>○ Health Law<br>○ Intellectual Property Law<br>○ International and Comparative Law |
| Duke University | School of Law | • Duke has a well-respected Law program and it offers a number of courses as it relates to privacy law. |
| University of North Carolina | School of Law | The LL.M program is currently suspended as the university undergo a study on restructuring and growing the program. Currently, this program addresses legal areas in which LL.M. students may concentrate their law studies in |
| New York Law School | School of Law | New York Law School's curriculum targets growing sectors of the economy:<br>• Business and Financial Service<br>• Intellectual Property, Media, Technology and applied sciences |

| | | |
|---|---|---|
| | | • Government and Public Interest Law |

**Conclusion:** Technology companies took plenty of hits on privacy last year; Facebook remained the theme for most of 2018. From May 25, 2018 the European Union began enforcing a new law that allows consumers the right to request their online data and restrict how businesses obtain and handle the information. In June, California passed its law that gives people the right to know what information companies are collecting about them, why the companies are collecting that data and with whom they are sharing it with — this sets a significant privacy benchmark for the United States. [20] "Companies like IBM and Salesforce, sell data storage and software to other businesses and were more willing to accept consumer privacy laws. Social media and other companies that relied primarily on advertising for revenue, like Facebook and Google, were adamant and believe they should fight the new California Law. Interestingly, Facebook and Google appear to have softened their resistance to the idea of implementing a federal privacy law, as long as they are deeply involved in writing the rules." [20]

The private sector seeks to gain some control by influencing their own set of privacy laws; for some, the participation in writing some of these laws, all in the faith of overriding the influence of the new California Law. Unfortunately, it's only a matter of time before there is an uproar about the way we treat the data of American citizens, and we can't simply wish away the new California privacy law. Much of that effort should be directed towards information sharing and privacy education in order to successfully drive these changes within their organizations. Companies can plan to make the necessary modifications to their business model, and the way they approach consumers across geography. Privacy professionals are often concerned with data, who has it, where it's going, who has access to it, and how it will be used.

Education and training should be inclusive of understanding databases, how they work, how we share data with advertising companies and social media, and perhaps, how to read code. It will be challenging to address and understand the privacy implications of large-scale data processing without a more diverse education. Privacy intersects with many fields and many companies, whether internet, retail or technology — they all rely on the

collection and analysis of data to better aid their targets with online advertisements in order to increase their revenue.

**Solutions:** Every organization is different and face a variety of challenges based on industry they serve, the culture and consumer base — it's essential to prevent being too stratified in any privacy training or education model. I created a sample framework that is more holistic and applicable to a specific group of "newcomers". Marketing has evolved, "of the hundreds of areas, big data and analytics will revolutionize marketing and sales — It will influence how prices are defined, managed, propagated through selling networks and optimized. [21] For marketing organizations, big data is the first consequence of the new marketing landscape, born from the digital world we now live in. The term "big data" doesn't just refer to the data itself; it also refers to the challenges, capabilities, and competencies associated with storing and analyzing such huge data sets to support a level of decision making that is more accurate and timelier than anything previously attempted. [22]

Many marketers may feel like data has always been big — and in some ways, it has. But the customer data businesses collected 20 years ago — the point of sale transaction data, responses to direct mail campaigns, coupon redemption, etc.; compared to the customer data collected today – online purchase data, click-through rates, browsing behavior (cookies), social media interactions, mobile device usage, geolocation data, etc. Comparatively speaking, there's no comparison." [22] By combining big data with an integrated marketing management strategy, marketing organizations can make a substantial impact in these critical areas.

As a result of these findings, I've drafted an outline of modules that could be selected based on on-off corporate training needs or coupled with existing business programs based on the structure of their curriculum. Some subjects could be leveraged to meet my proposed modules aimed at Corporate Marketing Professionals or MBA Marketing professionals. The CMU Privacy Engineering program (*see chart above*) has excellent course work that would pair seamlessly with my outline. This framework is inclusive of a variety of modules that could be customized and selected to be incorporated into other MBA programs or corporate trainings. My objective is to design a selection of modules to address:

- The design of cutting-edge products and services that leverage big data while preserving privacy

- Propose and evaluate solutions to mitigate privacy risks in marketing and analytics
- Understand how privacy by design can be leveraged to create a more privacy aware culture
- How to leverage and create internal rules to address privacy throughout an enterprise

**Research #1 Corporate Training for Marketing Professionals**

Customizable Privacy Modules for marketing professionals who serve in roles similar to Digital Marketing Specialist, Brand Marketing Specialist and Analytics.

**Research #2 MBA: Marketing**

Customizable Privacy Modules for Q3 and Q4 MBA Programs; 3 Credits

**Career Focus:** This MBA program is designed to attract 8-10-year professionals who are leading the business, understand enterprise risks and want to learn how to engage privacy. These professionals may serve as Chief Marketing Officers (CMO), Chief Privacy Officers (CPO), Digital Marketing Specialist, Brand Marketing Specialist and Analytics. Organizations want to be more objective and data-driven, and now fully embracing the power of data and technology. Businesses apply analytics to the data they collect in order to gain insights and uncover trends. In the past, this involved capturing numbers on a spreadsheet and manually examining the numbers. Fortunately, big data analytics now uses advanced software systems; this allows companies to reduce the time spent on analytics for speedy decision making, and to increase efficient analytical procedures. This ability to work faster and achieve agility offers a competitive advantage to businesses but comes with much-needed privacy considerations. In the meantime, the ability to shift leadership thinking from "data value" to be inclusive of "data risk" is the first step to shaping this approach to privacy in education.

**Training Objectives:** This course will equip students and professionals to be influential leaders within their boards, organizations, and teams to drive performance, evangelize privacy and the benefits of embedding privacy throughout the innovation of business solutions. Participants are required to have foundational knowledge of enterprise risks, privacy and marketing.

**Course Content:** This course is intended to shift the way marketing professionals view privacy and how privacy considerations can enable and protect their goals for the business. The world of marketing has evolved; the field values data and being able to collect as much as possible in order to provide the best services amongst competitors. They accomplish this through tasks such as brand innovation, digital marketing -- all of which ties back to personalization and analytics. This course will pair marketing strategies with privacy considerations which ultimately enables the way you do business.

**Module 1:** Intro to Privacy

In this module we will introduce privacy laws and regulations that are usually considered for marketing to consumers: FTC, FIPP, GDPR, Privacy Shield, COPPA, CAN-SPAM

**Module 2:** A Privacy by Design Approach to Marketing & Innovative Strategy

Customers are an essential asset to any business. When companies are slow to learn what consumers are looking for, it is effortless to begin offering poor quality products. In this module, we would address the world of marketing as a current state and what trends we've identified for the future of marketing. Marketing has taken a very innovative approach to data, and it's essential to include privacy considerations and how laws will impact the way organizations do business.

**Module 3:** Personalization, Data Analytics & Privacy Considerations

This module will address personalization and analytics. Companies are more strategic about tracking observed behaviors and real-time events through machine learning. In turn, this data is used to recommend the best products and/or services based on the profiles built on consumers. We will explore the innovation and trends in this space and how privacy considerations can enable these processes.

**Module 4:** Privacy & Cookies (*see appendix a for module sample*)

In this module, we'll discuss different types of cookies (*functional, performance, and marketing*) and how to embed privacy processes in the way cookies are used across platforms. Cookies are often used by third-party advertising agencies such as Facebook, Pinterest and Snap Chat. We'll dive into a variety of use cases that highlights:

- How cookies are used to track and market to our consumers across platforms
- How third-parties market to potential customers on your organizations behalf who have not yet crossed your business platforms
- We'll discuss privacy risks, how to evaluate and assess these types of partnerships; and
- How to read cookie JavaScript codes in order to verify partners are only collecting the data we want to share with them

**Module 5:** Privacy and Communications

In this module, we'll discuss the various types of marketing communications.

- We'll dissect transactional emails vs. marketing emails and the various types of privacy considerations for each.
- We'll take a look at consent language and notice
- We'll discuss concepts such as soft-opt ins and how to monitor internal teams and their process to ensure you have privacy baked-in from end-to-end

**Module 6:** Privacy at the Boards, Data Governance, Ethics, and Compliance

In this module, we will discuss the ethics behind the use of personal data.

- We will highlight data governance structures such as: data quality, data architecture, data storage, operations, data security, data integrations, document and content management, data warehousing and meta-data collecting and use
- We'll discuss what it looks like to brief board of directors on information privacy. A board's interest in InfoSec is heightened not only by public breach disclosures but also by a company's external auditors. In this module, you'll learn how to establish a framework that will allow you to apply team scoring throughout various parts of the business. This aids in putting a pulse on the privacy maturity of the business

and how that should be reported back to the board in a way that increases awareness and gain additional buy-in towards privacy enhancements.

**Appendix [A]**

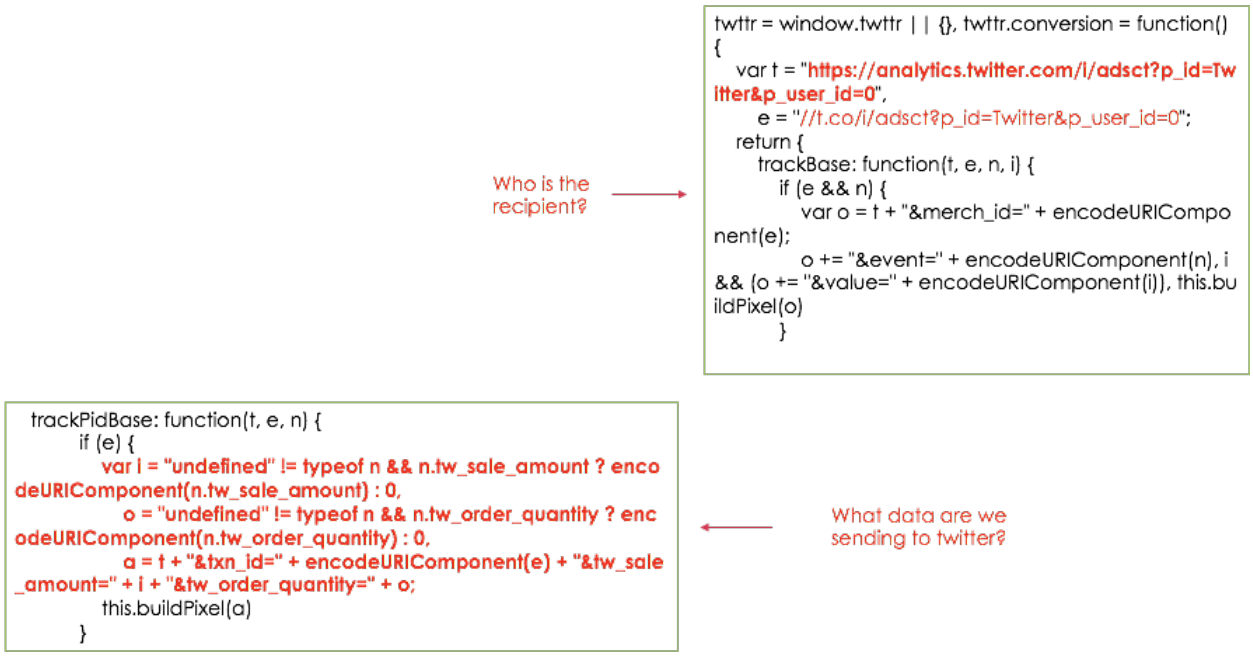
**Module 4:** Privacy & Cookies


**Intake Process:**

- New Tag
- Edit Existing Tag
- Page Types (Homepage, Checkout, Category Details
- How data will be collected

**Review Process:**

- Why do we need this?
- Where does it fire?
- How long is it needed?
- What's being sent?
- What does the source script contain?
- How does the recipient or the data represent their use of the data?
- How old is the company?
- What kind of company?




**Notes**

[1] U.S. Department of Education, National Center for Education Statistics. (2018). Digest of Education Statistics, 2016 (NCES 2017-094) Chapter 3. https://nces.ed.gov/fastfacts/display.asp?id=37

[2] U.S. Department of Education, National Center for Education Statistics, Higher Education General Information Survey (HEGIS), "Degrees and Other Formal Awards Conferred" surveys, 1970-71 through 1985-86; Integrated Postsecondary Education Data System (IPEDS), "Completions Survey" (IPEDS-C:91-99); and IPEDS Fall 2000 through Fall 2016, Completions component. (This table was prepared August 2017.) https://nces.ed.gov/programs/digest/d17/tables/dt17_322.10.asp?current=yes

[3] (ISC)2, (ISC)2 Study: Workforce Shortfall due to Hiring Difficulties Despite Rising Salaries, Increased Budgets, and High Job Satisfaction Rate. 2015, http://blog.isc2.org/isc2_blog/2015/04/isc-study-workforce-shortfall-due-to-hiring-difficulties-despite-rising-salaries-increased-budgets-a.html.

[4] Heimes, Rita. Top 10 Operational Impacts of the GDPR: Part 1 – Data Security and Breach Notification. IAPP, 2016, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/.

[5] Accenture. Value of Data: 2018 and Beyond. https://www.accenture.com/no-en/topic-accenture-value-of-data

[6] Harvard Business School. MBA Experience. https://www.hbs.edu/leadership/mba-experience/Pages/default.aspx

[7] John Kopanakis. 5 Real-world Examples of How Brands are Using Data Analytics. https://www.mentionlytics.com/blog/5-real-world-examples-of-how-brands-are-using-big-data-analytics/

[8] Harvard Business School. Course Catalog. https://www.hbs.edu/coursecatalog/2028.html

[9] https://www.dw.com/en/france-maintains-long-tradition-of-data-protection/a-14797711

[10] https://www.siliconrepublic.com/enterprise/gdpr-history-data-protection-ireland-eu

[11] A Proposed Career Roadmap for the Next Generation Privacy Professional. IAPP. June 11, 2014. Christopher Stevens and Stephen Holland. https://iapp.org/news/a/a-proposed-career-roadmap-for-the-next-generation-privacy-professional/

[12] MSIT in Privacy Engineering. Carnegie Mellon University. http://privacy.cs.cmu.edu/

[13] Certificate in Information Privacy Law. University of Maine School of Law. https://mainelaw.maine.edu/academics/academic-program/certificate-information-privacy-law/

[14] Privacy Law at Santa Clara Law. http://1x937u16qcra1vnejt2hj4jl-wpengine.netdna-ssl.com/wp-content/uploads/HTLI-PrivacyLaw_FINAL.pdf

[15] https://www.apple.com/privacy/approach-to-privacy/

[16] https://www.qmul.ac.uk/postgraduate/taught/coursefinder/courses/191253.html

[17] https://www.northeastern.edu/law/why/interdisciplinary/index.html

[18] https://law.duke.edu/academics/course/browser/curriculum/upperclass-2l-3l/

[19] http://www.law.unc.edu/academics/degreeprograms/dualdegree/

[20] https://www.nytimes.com/2018/08/26/technology/tech-industry-federal-privacy-law.html

[21]https://www.forbes.com/sites/louiscolumbus/2016/05/09/ten-ways-big-data-is-revolutionizing-marketing-and-sales/#107d7fc021cf

[22] https://www.sas.com/en_us/insights/big-data/big-data-marketing.html

[23] https://www.isaca.org/Journal/archives/2014/Volume-3/Pages/Data-Privacy-and-Big-Data-Compliance-Issues-and-Considerations.aspx#1

[24] https://iapp.org/news/a/50-shades-of-the-privacy-profession/

[25] https://iapp.org/media/pdf/certification/CIPP_US_BoK_2.2.0.pdf

[26] https://iapp.org/media/pdf/certification/CIPM_BoK.pdf

[27] https://iapp.org/media/pdf/certification/CIPP_C_BoK_2.1.0.pdf

[28] https://iapp.org/media/pdf/certification/CIPP_Asia_BOK_1_0_0_Final[4].pdf

[29] https://iapp.org/media/pdf/certification/CIPP_E_BoK_1.2.0.pdf

[30] https://iapp.org/media/pdf/certification/CIPT_BOK_2.1.2.pdf