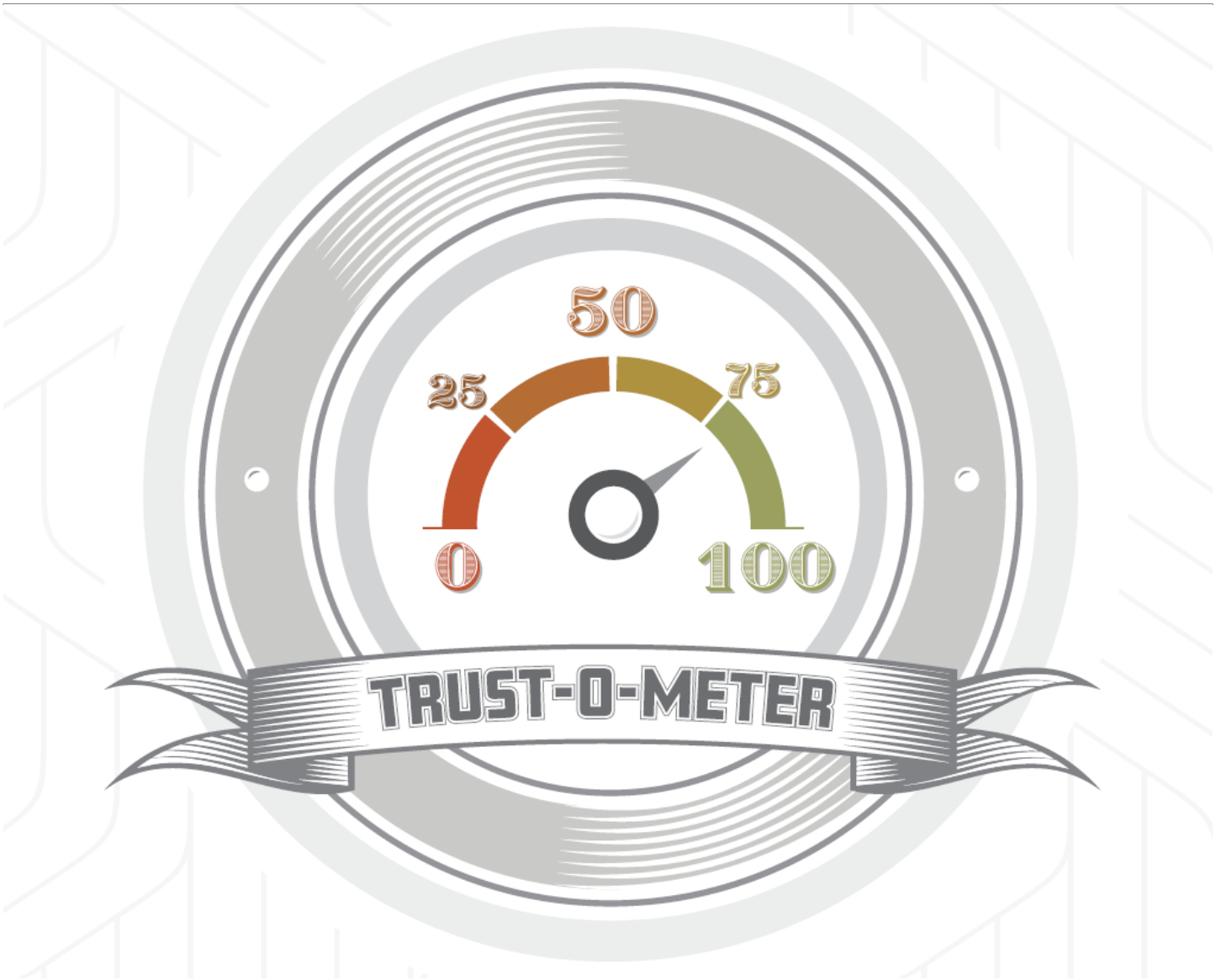
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Turning Consumer Privacy Expectations Into Trust

Technology, Privacy, and eCommerce


50
25
75
0
100
TRUST-O-METER



CHEAT SHEET

- ***A foundation of trust.*** The amount of data that consumers are comfortable sharing is dependent on how much they trust the company. By increasing trust, companies can receive more personal data and better customize products and experiences for the consumer.
- ***Increase transparency.*** Use required disclosures and notices about personal data collection as an opportunity to explain the who, what, where, and why — and emphasize the benefits — of collection in a user-friendly way to consumers.
- ***Train and educate.*** When training staff on the regulatory and operational requirements of managing consumer data, also focus on the impact requirements have on consumer rights and expectations.
- ***Optimize efficiency.*** Use technology to meet consumer expectations and regulatory requirements, for example, implement a self-service portal for consumers to exercise their rights of deletion and access.

Consumer expectations concerning the use of their personal data are rapidly evolving as evidenced by the uptick in privacy-related news, regulations, and a general increase in understanding of the personal data lifecycle. Laws such as the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) — regulations uniquely borne out of a private citizen's desire for more personal data privacy are introducing never before seen rights to consumers. Consumer awareness and understanding of these rights will be accelerated through platforms, such as social media, and through mainstream activists.

> Legal counsel should be proactive and flexible in working with operations and compliance departments to identify ways to increase transparency, train and educate employees, create operational efficiencies, and automate technological solutions to meet compliance requirements, where appropriate.

As more and more laws are developed to create and address the privacy rights of consumers, as well as the duties and liabilities surrounding data breaches, understanding your consumers and their respective privacy expectations has become a business imperative. Gaining insight into specific consumer expectations can be a starting point to understanding the risks and the management steps needed to mitigate or eliminate these risks.

Consumer expectations

Every company has at least a baseline understanding of their consumer, typically categorized by various demographics. But with the rapid growth of privacy requirements around the world, coinciding with everyday technological advances, in-house counsel can greatly benefit by staying informed about their company's consumer insights and expectations, as this can help better implement privacy regulatory requirements across all facets of a company's operations.

In a recent survey, 63 percent of consumers state that personalization is now part of the standard service they expect. In order for companies to provide the level of personalization expected, they must collect personal data able to be analyzed to provide the right level of insight into the individual's wants, needs, and overall preferences. This typically requires a fundamental understanding of more than simply the consumer's demographics. It includes such insights as their purchase history, preferences for communication, the level of control over their data they expect, and their overall behavior, both online and offline.

However, multiple surveys exist to show that a majority of consumers will respond negatively when asked if they want companies to track their behavior on devices, social media, or company websites. Device and location tracking has many legitimate purposes, including fraud prevention, assisting in public safety issues, and providing real-time offers. Unfortunately, this generalized negative consumer sentiment around tracking obviously conflicts with the ability of companies to meet a consumer's desire to receive personalized offerings, products, and services. This is a challenge that must be taken head on with solutions that not only address consumer expectations, but also fit within the confines of regulatory and company requirements and obligations. Legal counsel should be proactive and flexible in working with operations and compliance departments to identify ways to increase transparency, train and educate employees, create operational efficiencies, and automate technological solutions to meet compliance requirements, where appropriate.

Consumers have shown little faith and trust in a company's ability not only to meet their

personalization expectations, but also to protect their data. A recent survey of 2,000 US consumers over the age of 18 showed that only 25 percent believe most companies handle their sensitive personal data responsibly, and just 15 percent think companies will use that data to improve their lives. Consequently, 88 percent of these consumers say the amount of data they share with a company is dependent on how much they trust it. Instead of viewing this as a negative, in-house counsel should see the opportunity to differentiate their company from their competitors by earning that rare consumer trust with respect to data privacy.

By targeting the areas below, in-house counsel can help lead the charge in meeting consumer expectations and in identifying competitive differentiators while also mitigating and eliminating some of the more pressing privacy risks that companies face today.

Transparency

Many of the concerns consumers express around the use of their personal information can be alleviated or mitigated through taking advantage of opportunities to be more transparent to the consumer. Seventy-three percent of consumers state that it is “very important” for companies to explain how their information is being used. In-house counsel, in crafting their required disclosures and notices, should embrace opportunities to tactfully explain the benefits to the consumer of the company’s data collection and processing practices. A simple clause such as “We collect your location data as part of using our service” can be easily enhanced by explaining that location data is collected because it not only is a necessary part of delivering the service, but that it also allows the company to offer personalized rewards, services, offerings, etc.

Essentially every organization that has a consumer-facing website also has a privacy notice, usually in the form of an external-facing Privacy Policy. Typically, this notice is found in a size nine or 10 font, toward the bottom of a site, and aligned within a list of other links consumers rarely make their way to. Companies that believe most of their consumers read their notice are either lying to themselves or are extreme optimists. While the drafting of a thorough and complete privacy notice along with properly crafted opt-in and opt-out consent mechanisms can serve to meet regulatory disclosure and notice requirements, having these notices should not be considered all that is necessary to meet consumer expectations.

Consideration should be given to offering consumers easy-to-digest information on what personal data is collected, how it is processed, who it is shared with, and arguably most importantly, why it is collected. For example, consider suggesting your company develop a video or flow-chart for consumers to view at the time of collecting consent that describes the data lifecycle journey and also emphasizes the benefits to the consumer; this in turn provides greater assurance that the consumer (1) has a better understanding of what is collected and why, and (2) is receiving the personalized and targeted experience they desire. Thus, the company will not only meet regulatory requirements, but also improve upon consumer expectations and understanding.

Given the unique requirements found in regulations such as CCPA and GDPR around notice and disclosure to consumers, companies should consider creating a “consumer-friendly” privacy site that explains in easy-to-digest terms the necessary information around collection and processing of personal data. Developing an easy-to-use, self-service portal for consumers to exercise their rights, such as deletion and access, is another important way to show to consumers that you care about their privacy. Only 10 percent of consumers feel they have complete control over their personal data. A self-service portal can be a part of the overall effort to bring value to the consumer by explaining their privacy rights and your company’s role as well as putting the consumer back in control and

meeting their expectations.

Educating and training your workforce

In developing internal training and educational materials, in-house counsel should focus on translating the regulatory and operational requirements into concise and easy-to-understand language that not only explains the rules and regulations the company must follow, but the impact these requirements have on the consumer's rights and expectations. The immediate benefit of having a well-trained and educated workforce with respect to privacy is that this helps to minimize the likelihood of employee caused data breaches or other misuse of consumer data. However, the importance of understanding privacy laws as part of the product or service design lifecycle should not be underrated.

> Only 10 percent of consumers feel they have complete control over their personal data.

While the GDPR has specific privacy-by-design requirements that companies must adhere to, even companies that do not have to follow these requirements should consider the operational and competitive advantage of having similar processes and efficiencies in place. Arming your design team with the details of the privacy landscape and the expectations of the consumer will help ensure that privacy is an important consideration, and potentially a differentiator, in your company's product or service offering.

How to measure your privacy policy's readability

Privacy notices, typically in the form of an online "Privacy Policy" to consumers, have evolved from being a mere few sentences in the 1990s to some of the more complex notices today, with some reaching more than 4,000 words. Additionally, many companies have developed standalone cookie notices as an extension to their privacy notice. While the increase in privacy regulatory requirements has necessitated some level of increase, the corresponding effect is legitimate readability concerns for consumers.

Many studies have shown that the average adult reads at around a seventh or eighth grade level. Fortunately, several tools and formulas exist in order to assist in crafting a privacy or cookie notice that aligns with a readability level consistent with a company's consumer base. One example of an automated type approach is using a tool such as the Automatic Readability Checker. This tool will assess your content against seven commonly used readability formulas and indexes.

Another approach is to take the data from website analytics cookies and develop an understanding of how quickly individuals click away or exit from the privacy notice or cookie policy page and compare that against the average time it takes to read the content in its entirety. Regardless of your approach, some factors to focus on include sentence and word length, amount of syllables, paragraph length, and native language.

Most practitioners know that the sharing of personal data with vendors and service providers is

essential as part of offering a service or product. Fifty-seven percent of consumers stated they would be less likely to shop or use services in the future if a company sends their personal data to other companies. Knowing that consumers are becoming more and more frightful of companies sharing their personal information with third and sometimes even fourth parties, design teams can identify ways to either eliminate third-party sharing, or identify opportunities for transparency to the consumer and consolidation of vendor services, where appropriate.

> Fifty-seven percent of consumers stated they would be less likely to shop or use services in the future if a company sends their personal data to other companies.

An added benefit of a well-trained and educated workforce is arming employees with the knowledge to identify areas to promote data minimization practices, thus decreasing many risks that lead to serious and deeply consequential data breaches. Without that understanding of the importance of consumer privacy, employees cannot be expected to take it into consideration with respect to the development or design of the process or product they are responsible for.

While the focus on the above has primarily been on educating and training the workforce, it is prudent to also ensure that the C-suite and board of directors are also properly informed and made aware of the exact risks that privacy laws create. Privacy laws are relatively new and have only truly come into a level of significant impact to companies in recent years. With this recent emergence comes the reality that many board members and executives today do not have the same years of experience addressing privacy risks as they would, for example, addressing other consumer protection or financial risks. With the potentially large fines for GDPR infringements as well as the potential volume of litigation stemming from CCPA, both from regulators and individuals, the board and executive team must be made aware of the privacy landscape and what it means to the company.

The communication to the board and C-suite should be in a manner that is relatable to their experiences throughout their careers. GDPR, CCPA, and potential future privacy federal legislation can be explained as having a similar significance to historical laws such as Dodd-Frank or Section 5 of the Federal Trade Act. These laws are great examples of regulations that forced companies to complete thorough gap assessments of most, if not all, processes and implement remedial activities to reach a compliant state or face major financial, reputational, and business consequences. For those companies and counsel that have been through GDPR assessments and implementation efforts, this is easier to understand. However, the full impact may not quite be appreciated yet as we still await the large GDPR enforcement fines as well as the 2020 effective date of CCPA. Therefore, regular communication is a necessity going forward.

The trend of privacy laws increasing both in volume and complexity is expected to continue, and thus boards and executives must understand the corresponding increase in risks as well as any potential opportunities to develop competitive differentiators. Furthermore, maintaining a level of privacy awareness throughout the workforce will help serve as an accelerator for individual departments to implement or enhance privacy-related improvements to processes and controls owned by their respective teams.

Improving and automating technology solutions

Consumers are showing a tendency to be unforgiving if a company does not protect their data, especially where a competitor’s readily available service or product offerings exist: 89 percent of consumers are at least somewhat likely to switch brands if a company is hacked and their basic

personal data is compromised, and 86 percent of these same consumers would at least be likely to switch if a company sells their data to other companies for marketing purposes without their permission. This example demonstrates the importance of identifying gaps in processes and implementing the right controls and other remedial technological solutions to meet consumer expectations that also align with regulatory requirements.

Most in-house counsel have experienced the headaches that come with enhancing or improving existing processes and controls, or even a total creation from scratch, in order to meet regulatory requirements. Implementing automated solutions creates a consistent process that can help eliminate and mediate some of those headaches, as well as the risks that are more prevalent for manually controlled processes. Fortunately, many privacy compliance tools and solutions are rapidly being developed that bring at least some level of automation. Furthermore, automated solutions to help prevent and detect incidents and breaches involving personal data have become essentially mandatory for all companies. But in-house counsel should also explore the automated solutions that both exist out of the box or as a customizable solution to help address the rights of consumers and are tailored to meet their expectations. These solutions could include, as mentioned previously, a self-service portal that serves as the platform for the consumer to exercise their rights. An automated solution can provide the consistency in not only the delivery of the request from an individual, but also in the communication, and importantly, the timing of the response to the individual. Companies that can rapidly triage a request and provide a response can not only satisfy regulatory requirements, they are also able to prove to consumers that they care about their privacy rights. This type of solution would also prove to regulators that your company takes these rights seriously and strives to offer consumers a simple and transparent manner for them to exercise their rights. This type of goodwill can go a long way should the need arise to present a case to the regulators of proving a good faith effort in developing and implementing your compliant data privacy program.

The competitive advantage

The companies we serve are at a unique crossroads where consumer expectations are not being met and consumers do not trust most entities to protect their data; all the while, privacy regulations are increasing both in volume and complexity. The above strategies not only serve as opportunities to improve functions, processes, and offerings, but to also earn goodwill from our consumers and regulatory bodies in the event mistakes arise, and we must face the demands of both.

While the challenges are significant, so is the opportunity. By ensuring there is a foundational understanding of both the consumer and the regulatory requirements with respect to consumer personal data, in-house counsel can serve as a leader of their company’s efforts to not only meet consumer privacy demands, but to develop privacy notice and disclosure differentiators to compete successfully in the marketplace.

ACC EXTRAS ON… Consumer privacy

ACC Docket

Negotiating Data Privacy in Multivendor Technology Contracts (Aug. 2019).

Privacy Trends: The California Consumer Privacy Act is a Harbinger of New Regulations (March 2019).

The Chief Privacy Officer: The New “Must Have” (Dec. 2018).

Sample Forms, Policies, and Contracts

Notice of Privacy Practices (July 2017).

Further Reading

RedPoint Global, The Harris Poll. “Addressing the Gaps in Consumer Experience.” Survey. Jan. 28, 2019.

PricewaterhouseCoopers. “Consumer Intelligence Series: Protect.me.” Survey. September 2017.

Jim Sturm

Associate Counsel, privacy and compliance

Margaritaville Enterprises