Privacy law case study and analysis

LEGAL BULLET-PROOFER

We comply and stay up to date with global laws and frameworks

Comprehensive Compliance: We make concerted efforts to stay informed and compliant with prominent email and data privacy regulations across the globe, including but not limited to California's CCPA/CPRA and the federal CAN-SPAM Act.

US Exclusive Operations: Currently, we process and return email addresses of US visitors only. Based on our understanding, the US predominantly operates under an opt-out system. Hence, we do not engage in practices that would fall under GDPR/CASL jurisdictions.

Consumer Privacy Requirements: We mandate our users to update their privacy policies to include our specific "Consumer Privacy & Third-Party Cookies Notice" verbiage, ensuring transparency to end consumers.

Unsubscribe Practices: We emphasize and require that all email marketing endeavors include a clear unsubscribe link in every email. All unsubscribe requests by recipients must be honored promptly.

Enterprise-Grade Preparedness: Our processes are 100% enterprise-grade ready.

Legal case study

PREFACE.

Using existing software-as-a-service (referred to herein as “Software”), companies are able to obtain email addresses of visitors to websites who have not and do not proactively disclose their email address to the website owner, even if explicit consent was granted by the visitor to receive email via the network. Users are always explicitly given the choice to opt-out too. This case study analyzes the potential legal considerations relating to the usage of such software-as-a-service.

Based on our extensive analysis of the use-case, these are the known topics relating to the legality of using Software:

- GDPR LIMITATIONS OF SCOPE
- CAN-SPAM ACT
- CALIFORNIA PRIVACY LAWS
- VIRGINIA PRIVACY LAWS
- COLORADO PRIVACY LAWS
- ADPPA

NOTICE & DISCLAIMER.

This case study is intended solely for educational and/or informational purposes and is not intended to constitute formal legal advice or imply an attorney-client relationship between our Legal Counsel and the recipient of this case study analysis.

GDPR limitations of scope

The General Data Protection Regulation (EU) (GDPR) is a regulation in EU law on data protection and privacy in the European Union (EU) and the European Economic Area (EEA).

GDPR stipulations apply when the personal data of a data subject, who is located in an EU country at the time, is processed.

GDPR also applies to organizations that handle such data whether they are EU-based organizations or not, known as “extra-territorial effect.”

Furthermore, GDPR does not apply to EU citizens in the US. The location of the data subject, rather than their citizenship, determines whether GDPR applies.

For example, EU citizens traveling to or living in the US are not protected by the GDPR. Thus, GDPR does not touch the scope in which Software provides service at all.

The CAN-SPAM Act

Opt-Out – Not Opt-In. While certain jurisdictions outside of the United States (e.g. the European Union and Canada) require an affirmative opt-in in order to send marketing or commercial emails, the US has been, since the passage of CAN-SPAM Act of 2003, an opt-out jurisdiction.

This means marketing emails can be sent to recipients unless and until they have opted out of receiving marketing emails from the sender.

Accordingly, a user of the Software can send emails to email addresses acquired through the Software provided that the recipient has not previously opted-out to receiving marketing emails from the Software user / sender.

The sender of marketing emails acquired using the Software should include an unsubscribe link or other opt-out mechanism in all marketing emails and promptly honor all opt-outs.

Prohibition on Email Harvesting: The Software does not collect or distribute email addresses that were harvested, irrespective of a website's specific policy. The CAN-SPAM Act prohibits sending unsolicited emails to addresses acquired through techniques like harvesting.

Compliance with CAN-SPAM

The CAN-SPAM Act of 2003 establishes requirements for companies that send commercial emails. The law covers email whose primary purpose is advertising or promoting a commercial product or service. This includes content on a Website.

A “transactional or relationship message” – an email that facilitates an agreed-upon transaction or updates a customer in an existing business relationship – may not contain false or misleading routing information, but otherwise is exempt from most provisions of the Act.

Violations of the Act can result in civil fines and criminal liability. The Act applies to consumer and business recipients and makes no exceptions for business-to-business emails.

Prior express consent or opt-in consent is not required in order to send commercial emails. Commercial emails may not, however, be sent to recipients who have opted-out or unsubscribed from receiving commercial emails from the sender.

Section 7704(a)(3) of the Act requires that marketing messages contain an opt-out or unsubscribe mechanism.

In general, if a recipient makes a request not to receive some or any commercial electronic mail messages from such sender, then it is unlawful:

(i) for the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message that falls within the scope of the request.

(ii) for any person acting on behalf of the sender to initiate the transmission to the recipient, more than 10 business days after the receipt of such request, of a commercial electronic mail message with actual knowledge,or knowledge fairly implied on the basis of objective circumstances, that such message falls within the scope of the request for any person acting on behalf of the sender to assist in initiating the transmission to the recipient, through the provision or selection of addresses to which the message will be sent, of a commercial electronic mail message with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such message would violate clause (i) or (ii)

Or, (iv) for the sender, or any other person who knows that the recipient, has made such a request, to sell, lease, exchange, or otherwise transfer or release the electronic mail address of the recipient (including through any transaction or other transfer involving mailing lists bearing the electronic mail address of the recipient) for any purpose other than compliance with this Act or other provision of law.

Thus, the Act does not contain any requirements or reference to opting-in to receive marketing email messages.

As required by the Act, the FTC recently reviewed the law and accepted public comments in order to determine whether the law was still appropriate as written.

On February 12, 2019, the FTC confirmed: The Act does not require that recipients affirmatively consent or opt-in to receiving commercial emails. Rather, each email must contain a clear and conspicuous notice the recipient can opt-out of receiving more commercial email from the sender.

Commercial emails must contain a return email address or another Internet-based response mechanism that allows the recipient to indicate it does not want future email messages to that email address.

It is permissible to create a “menu” of choices to allow a recipient to opt-out of certain types of messages, but the email must include the option to end any and all commercial messages from the sender.

California privacy laws

California Privacy Rights Act (CPRA) amending the California Consumer Privacy Act (CCPA). The CPRA, a ballot initiative passed by voters in November 2020, amends the CCPA and renames the CCPA to the CPRA. The CPRA includes additional privacy protections for consumers as outlined in the following.

Opt-Out of Sharing for Targeted Advertising. The CPRA extends a consumers right to opt-out of sales to include a right to opt-out of the sharing of the consumer's personal information for targeted advertising (defined as "cross-contextual behavioral advertising"), whether such sharing is made with or without consideration.

The CPRA contains an opt-out requirement for the sharing or sales of personal information, with the exception of the sharing or sales of personal information relating to children under the age of 16.

Children aged 13 to 16 must provide opt-in consent for the sale of their personal information. Website owners collecting, using, selling, or sharing personal information relating to children under the age of 13 must obtain verifiable parental opt-in consent to do so.

The CPRA does not outright prohibit the sharing of personal information. Rather, if a company shares personal information for targeted advertising the company must provide notice of this to the consumer and give the consumer at least 2 methods for opting-out of the sharing of personal information for targeted advertising, one of which must be an interactive webform to opt-out requests.

Use of the Software to acquire email addresses and send emails to those addresses is sharing under the CPRA, which would require notice and the ability to opt-out of such sharing.

There are few exclusions from a “sharing” of personal information triggering the opt-out requirements, including when a Software user directs the Software provider to intentionally disclose personal information with one or more third parties.

If the Software user desires to permit the Software provider or any other third party to use the personal information for their own purposes outside of providing services to the Software user, the Software user should comply with the notice and opt-out requirements under the CPRA relating to the sharing of personal information for targeted advertising.

CPRA Notice. One of the primary requirements of the CPRA is the obligation to provide a “Do Not Sell or Share My Personal Information” and a privacy notice or privacy policy to website visitors complying with the requirements of the CPRA. All of the various notice requirements required under the CPRA are outside the scope of this summary.

With respect to the Software, generally speaking the CPRA requires notice to website visitors if personal information that identifies or can be reasonably used to identify them is collected by the website owner, the purposes for collecting, selling, or sharing the personal information, and the categories of third parties to whom the personal information is disclosed.

On its website homepage, a user of the Software should provide a clear and conspicuous link titled “Do Not Sell or Share My Personal Information” that enables a user to opt-out of the sharing of a visitor’s personal information.

In its CPRA privacy notice, a user of the Software should disclose and describe that, among other things, the website owner uses visitor tracking Software to collect identifiable information about visitors (e.g., an email address), how it uses the information and that it shares the information with third parties (e.g., with the Software provider to identify plaintext email addresses of visitors). Details will vary depending on the nature of the website.

Colorado privacy laws

On July 7, 2021, Colorado Governor Polis signed the Colorado Privacy Act ("CPA") into law. This legislation is set to go into effect on July 1, 2023.

The CPA applies to businesses that target Colorado consumers and that collect and store data on at least 100,000 consumers or earn revenue from selling data of at least 25,000 consumers.

Certain types of data are excluded, including personal data governed by certain federal or state laws such as GLBA, and data that is made available in public records. The definition explicitly excludes de-identified information or publicly available information.

Some obligations under CPA; Controllers must provide consumers with a clear and meaningful privacy notice. The notice must be reasonably accessible and must include:
(a) the categories of personal data collected or processed;
(b) the purposes for which the personal data is processed;
(c) a description of the consumer rights described above and how a consumer can exercise them; (d) the categories of personal data that are shared with third parties; and (e) the categories of third parties with whom the personal data is shared.

Controllers are prohibited from processing personal data in violation of federal or state laws that prohibit unlawful discrimination against consumers.

Virginia privacy laws

On March 2, 2021 Virginia's governor Northam signed the Consumer Data Protection Act ("CDPA") into law. The CDPA contains elements of the newly passed California Privacy Rights Act which revised the California Consumer Protection Act of 2018 ("CCPA").

CDPA gives consumers broad rights to access and obtain, correct, delete, and opt-out of certain processing of their personal data, protects against non-discrimination, and provides consumers with the right to appeal a businesses' denial of a consumer right.

CDPA becomes effective January 1, 2023. There is no private right of action, but CDPA does provide for statutory penalties after a 30-day cure period.

Since a consumer under the CDPA is defined strictly as a Virginia resident, and there is no broad CCPA-like revenue trigger (businesses must comply with the CCPA if they have over $25 million in revenue per year), the CDPA has a much more narrow application.

The practical implication is that fewer smaller and mid-size businesses may be subject to the CDPA; however, certain industries which rely on the sale of personal data will be subject to the CDPA regardless of the size of the entity.

If relevant, controllers will need to be substantially more transparent about their collection and use of personal information and must provide consumers with notice (in their privacy policies) of their new rights under the CDPA.

The American Data Privacy and Protection Act (ADPPA)

The draft American Data Privacy and Protection Act (ADPPA) is a landmark data privacy bill that was being considered by the US congress to be passed in 2023, having received strong bipartisan and bicameral support. H.R. 8152, the ADPPA represents a 20-year effort to develop a national data security and digital privacy framework that would establish new protections for all Americans at the federal level.

However, California Privacy Protection Agency argues the that, with the ADPPA:

- California's unique "floor" to privacy protections as set forth in the CPRA would be preempted.
- Californians would be prevented from strengthening privacy laws in the future.
- ADPPA does not allow California to recover the monetary penalties associated with its enforcement of the federal law whereas the CCPA currently allows recovery of significant penalties for the violations of the CCPA / CPRA
- ADPPA effectively removes the opt-out option of automatic decision-making;
- ADPPA narrows the definition of "personal information" as defined in the CCPA because the ADPPA's "Covered Data" "may include derived data and unique identifiers".
- Granted, this definition is much narrower than that of the original CCPA, which in contrast, includes "inferences drawn from any of the information identified.", a broader definition for businesses to comply by.
- Moreover, the CCPA includes obligations for a broader set of service providers that are not even specified in the new ADPPA:

The ADPPA removes the mechanism for global opt-out requests; under the original CCPA, businesses must honor global privacy controls for opt-out requests such that consumers seeking to opt out do not have to initiate opt-outs for 100s or 1000s of sites.

However, under the new ADPPA, consumers will be required to unsubscribe one service at a time individually.

ADPPA would greatly narrow the need of data protection impact assessments ("DPIAs") in comparison to the original CCPA.

SoVi Digital

Contact us

For any further legal inquiry:

CONTACT@SOVIDIGITAL.COM

WWW.SOVIDIGITAL.COM