



Cookies Law 2023

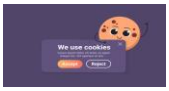
I've noticed, over the past year, an unfading increase in request to 'accept' cookies. In the past it been a much more random askance, however, growing concerns over how websites obtained data relative to their customer or visitor base. Their care for developing marketing reference data and generating familiarity of it's consumers, in duality, can become a recognized violation of ones 'privacy'. In a pressured awareness of our online privacy, cookies acceptance is suggested. It simply gives the website owner the right to survey your habits within their website product offers, materials, and supplemental information customers are provided with. Often, they resell the user's data and access the means to track them across the internet. It gives the visitor more control over the use of their information. As most cookies are in the form of a 'pop-up' you may respond 'yes' or ignore it a proceed with you website searching. It is not a standardized practice, but, it gives you 'say so' about retaining your sense of privacy.

Most of us, in a flippant sense, often ask ourselves, "Exactly, what are cookies?" Cookies are small files that website send to your device so the site can retain information pertaining to you. It remembers your shopping cart, things you've selected to view, or your log in data. They are pieces of information about your online presence accumulated as you browse. The question then becomes whom do you entrust with protecting as well as owning data?

European Online Data Law

Europe seems to be the primary country whose implemented The General Data Protection Regulation (GDPR), a privacy law the European Union established May 2018 accompanying the 2009 updated ePrivacy Regulation Directive. This 'cookie law' regulates privacy for tracking, confidentiality, and monitoring online.

In response to the imposed European privacy law, the public has probably received, same as I, a heap of updated privacy policy emails and terms of agreement from varied websites, apps, or company sites. It gives us a chance to consent to an erroneous request in sharing our information. For example, from google you may receive updates of your online tracking in websites and locations of internet use. This is the same means of communication other browsers and web sources may utilize to inform the consumer of it's data retention practices.



Likewise, it is assumed that other unknown bodies can also pay for a said information regarding you habits. Good or bad, it seemed your response to the 'cookies' question is attributable to the legitimacy of the websites ability to use your information for marketing or sale it to outside sources. No consent denies access of all interested parties.

Most people fail to notice whether or not a 'locked' icon (encrypted) appears at website address locations or to read 'terms and agreement' documents and comply in a rushed, uncaring fashion onto agreement in an effort to readily fulfill their task.

On the other hand, return visitors are confronted with a sense of ease as these sites remember their previous visits, purchases, shopping cart saves, log in passwords etc…just as the history prompt within most computers or tablet programming. This memory concept is typically well received and not assumed relative to the natural 'privacy' violations the data protection and privacy laws indicate. But it is!

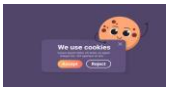
At home or office workplace online users might consider the use of software such as antivirus or Norton Anti-Track, which aide in protecting your online activity, browsing habits, settings and personal information through tracker blockades and disguising your digital finger print.

American Technology Laws

In the of January 2022, the global energy that pilots the plight for 'privacy' was shown as lawsuits were said to have been filed against giants such as Google for violation of consumer rights. This is at the urgent efforts of those few who understand the conditions placed upon their safety inside the surveillance activity's of those agency's whom purchase and use data for marketing research. Information is juggled amongst numerous third party's.

The simplistic cookies imposed 'agreement/acceptance' is the understatement of the nature of the beast customers are inviting into their personal space. The cookies prompt is a 'neutral' attachment, irritating pop-up, or a thing that I go along with to get onto and into a websites stuff. This manipulation is the 'fee' for service, a condition of full use, and the cost of having become a online user or net junky.

This same cost can also become attributable to the demise of some who have participated in indecent acts, dating habits, sharing personal sensitive app info therapy, group chats etc…..It can cause rate or pricing adjustments, targeted ads, and race or culture research data gathering.

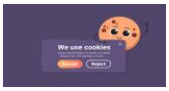


Currently, there are several initiatives in varied states in alignment with the European interest of General Data Protection, however, the strength of it's verbiage, and data regulation is in close proximity and in others sketchy and diluted. Within the boundaries of a host of acronyms, we find GDPR, ECPA, COPPA, HIPAA. These are General Data Protection Regulation, Electronic Communications Privacy Act, Children's Online Privacy Protection Rule, and Health Insurance Portability and Accountability Act. The U.S. Senate has introduced the Consumer Online Privacy Rights Act (COPRA). And, the California Consumer Privacy Act (CCPA) is a sole state level law in effect beginning January 1

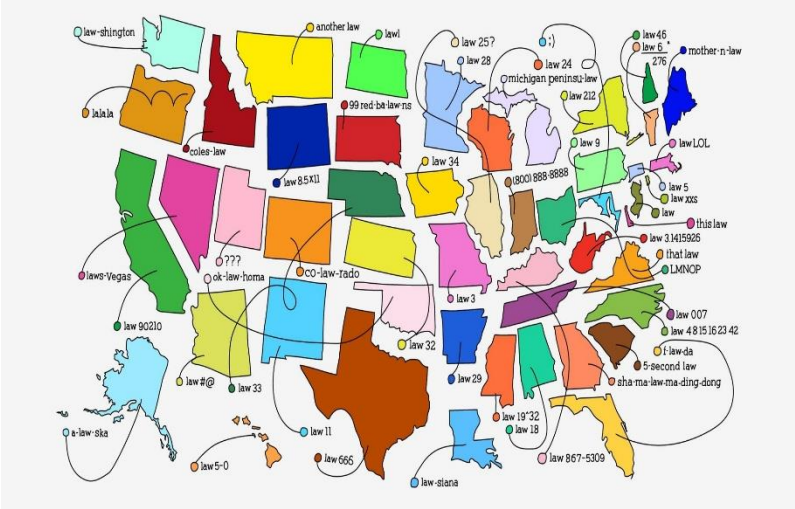
The patchy depiction of control for the HIPAA concludes with shared information between doctors, hospitals, pharmacies and insurance but falters in it's inclusion of devices and health trackers such as fit bits, virtual workouts, distance readers etc….. The ECPA regulates use of employers monitoring boundaries, governmental use of listening devices or wiretaps, but not dated surveillance techniques of servers, cloud storage, etc….as it was passed in 1986. COPPA stipulates limits upon data retention of under 13 year olds without parental consent and between 13 and 15 without user consent. It too is outdated and lacks the intensity to buck against modern online invasions. Thence, GDPR holds the floor globally as the most modern sense of law toward online control.

Selectively, inside these laws, is the ability to 'opt out' of cookies and information sharing and with others the ability to assume control of your data and location access through notice. This approach allows for customers to see the data collected as a review of monthly or yearly updates. California and approximately four other states have consumer data privacy law at the 'review' stage by appropriate authoritative bodies. Illinois in solo, protects public biometric (face scans, finger prints) data rights. Others are within the early stage of active laws. California, however, offers consumers a privacy 'private right of action' enabling legal rights against companies who violate it's law.

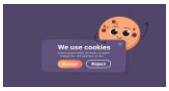
Funding for these state initiatives is well into the millions as proper care must be taken to savor the sense of creativity of which internet and website use are grounded in. Hindering the tech industry's progress should not be the focal zone, but, enforcement of privacy protection. State law provides a foundation in generating slated controls against online privacy violations, this U.S. is in dire need of federal law and regulations which pose a greater momentum of interest, consistency and understanding of public rights. There also needs to be an inclusive statement regarding 'data breach notification'. Most clients are unaware of such unless they capture an informed media resource (s) such as television news, talk radio, or written communication forms leaking such facts onto the public.



Currently, a voice from the FTC has proposed the Global Privacy Control (GPC) which has opt out but this is at the localized level and, as of yet, not a global rule. This is repetitive of the technology industry's 'The Internet Association' which consist of tech companies such as Amazon, Google, and Facebook, has proposed it's own 'consent and private right of action' regulations to New Jersey legislature. They have sought support of the Chamber of Commerce and Institute for Legal Reform to path toward neutral legal reforms which honor innovation while disabling consumer rights to sue.



*** states working on some variation of 'privacy' law***



References

Johansen, Alison Grace. us.norton.com, NortonLifeLock. August 15, 2022 accessed Jan 24, 2023

Klosowski, Thorin. Wirecutter/realtalk, The State of Consumer Data Privacy Laws in the US (And Why It Matters). PUBLISHED SEPTEMBER 6, 2021. Accessed 1/30/2023

Nocera, Joe. nytimes.com/dealbooknewsletter. How Cookie Banners Backfired, Updated Jan. 30, 2022 and accessed 1/30/2023

Stewartemily, Emily. Stewart@vox.com, Why every website wants you to accept its cookies. Cookie alerts are supposed to improve our privacy online. But are they? Dec 10, 2019, 8:00amEST