Sen. Cantwell Leads With New Consumer Data Privacy Bill | Electronic Frontier Foundation

Search

Email updates on news, actions, and events in your area.

Join EFF Lists

Electronic Frontier Foundation

Donate

Podcast Episode: Open Source Beats Authoritarianism

Electronic Frontier Foundation

Sen. Cantwell Leads With New Consumer Data Privacy Bill

DEEPLINKS BLOG

By Adam SchwartzDecember 3, 2019

Sen. Cantwell Leads With New Consumer Data Privacy Bill

There is a lot to like about U.S. Sen. Cantwell's new Consumer Online Privacy Rights Act (COPRA). It is an important step towards the comprehensive consumer data privacy legislation that we need to protect us from corporations that place their profits ahead of our privacy.

The bill, introduced on November 26, is co-sponsored by Sens. Schatz, Klobuchar, and Markey. It fleshes out the framework for comprehensive federal privacy legislation announced a week earlier by Sens. Cantwell, Feinstein, Brown, and Murray, who are, respectively, the ranking members of the Senate committees on Commerce, Judiciary, Banking, and Health, Education, Labor and Pensions.

This post will address COPRA's various provisions in four groupings: EFF's key priorities, the bill's consumer rights, its business duties, and its scope of coverage.

EFF's Key Priorities

COPRA satisfies two of EFF's three key priorities for federal consumer data privacy legislation: private enforcement by consumers themselves; and no preemption of stronger state laws. COPRA makes a partial step towards EFF's third priority: no "pay for privacy" schemes.

Private enforcement. All too often, enforcement agencies lack the resources or political will to enforce statutes that protect the public, so members of the public must be empowered to step in. Thus, we are pleased that COPRA has a strong private right of action to enforce the law. Specifically, in section 301(c), COPRA allows any individual who is subjected to a violation of the Act to bring a civil suit. They may seek damages (actual, liquidated, and punitive), equitable and declaratory relief, and reasonable attorney's fees.

COPRA also bars enforcement of pre-dispute arbitration agreements, in section 301(d). EFF has long opposed these unfair limits on user enforcement of their legal rights in court.

Further, COPRA in section 301(a) provides for enforcement by a new Federal Trade Commission (FTC) bureau comparable in size to existing FTC bureaus. State Attorneys General and consumer protection officers may also enforce the law, per section 301(b). It is helpful to diffuse government enforcement in this manner.

No preemption of stronger state laws. COPRA expressly, in section 302(c), does not preempt state laws unless they are in direct conflict with COPRA, and a state law is not in direct conflict if it affords greater protection. This is most welcome. Federal legislation should be a floor and not a ceiling for data privacy protection. EFF has long opposed preemption by federal laws of stronger state privacy laws.

"Pay for privacy." COPRA only partially addresses EFF's third priority: that consumer data privacy laws should bar businesses from retaliating against consumers who exercise their privacy rights. Otherwise, businesses will make consumers pay for their privacy, by refusing to serve privacy-minded consumers at all, by charging them higher prices, or by providing them services of a lower quality. Such "pay for privacy" schemes discourage everyone from exercising their fundamental human right to data privacy, and will result in a society of income-based "privacy haves" and "privacy have nots."

In this regard, COPRA is incomplete. On the bright side, it bars covered entities from conditioning the provision of service on the individual's waiver of their privacy rights in section 109. But COPRA allows covered entities to charge privacy-minded consumers a higher price or provide a lower quality. We urge amendment of COPRA to bar such "pay for privacy" schemes.

Consumer Rights Under COPRA

COPRA would provide individuals with numerous data privacy rights that they may assert against covered entities.

Right to opt-out of data transfer. An individual may require a covered entity to stop transferring their data to other entities. This protection, in section105(b), is an important one. COPRA requires the FTC

to establish processes for covered entities to use to facilitate opt-out requests. In doing so, the FTC shall "minimize the number of opt-out designations of a similar type that a consumer must take." We hope these processes include browser headers and similar privacy settings, such as the "do not track" system, that allow tech users at once to signal to all online entities that they have opted-out.

Right to opt-in to sensitive data processing. An individual shall be free from any data processing or transfer of their "sensitive" data, unless they affirmatively consent to such processing, under section 105(c). There is an exception for certain "publicly available information.

The bill has a long list of what is considered "sensitive" data: government-issued identifiers; information about physical and mental health; credentials for financial accounts; biometrics; precise geolocation; communications content and metadata; email, phone number, or account log-in credentials; information revealing race, religion, union membership, sexual orientation, sexual behavior, or online activity over time and across websites; calendars, address books, phone and text logs, photos, or videos on a device; nude pictures; any data processed in order to identify the above data; and any other data designated by the FTC.

Of course, a great deal of information that the bill does not deem "sensitive" is in fact extraordinarily sensitive. This includes, for example, immigration status, marital status, lists of familial and social contacts, employment history, sex, and political affiliation. So COPRA's list of sensitive data is under-inclusive. In fact, any such list will be under-inclusive, as new technologies make it ever-easier to glean highly personal facts from apparently innocuous bits of data. Thus, all covered information should be free from processing and transfer, absent opt-in consent, and a few other tightly circumscribed exceptions.

Right to access. An individual may obtain from a covered entity, in a human-readable format, the covered data about them, and the names of third parties their data was disclosed to. Affirming this right, in section 102(a), is good. But requesters should also be able to learn the names of the third parties who provided their personal data to the responding entity. To map the flow of their personal data, consumers must be able to learn both where it came from and where it went.

Right to portability. An individual may export their data from a covered entity in a "structured, interoperable, and machine-readable format." This right to data portability, in section 105(a), is an important aspect of user autonomy and the right-to-know. It also may promote competition, by making it easier for tech users to bring their data from one business to another.

Rights to delete and to correct. An individual may require a covered entity to delete or correct covered data about them, in sections 103 and 104.

Business Duties Under COPRA

COPRA would require businesses to shoulder numerous duties, even if a consumer does not exercise any of the aforementioned rights.

Duty to minimize data processing. COPRA, in section 106, would bar a covered entity from processing or transferring data "beyond what is reasonably necessary, proportionate, and limited" to certain kinds of purposes. This is "data minimization," that is, the principle that an entity should minimize its processing of consumer data. Minimization is an important tool in the data privacy toolbox. We are glad COPRA has a minimization rule. We also are also glad COPRA would apply this rule to all the ways an entity processes data (and not just, for example, to data collection or sharing).

However, COPRA should improve its minimization yardstick. Data privacy legislation should bar companies from processing data except as reasonably necessary to give the consumer what they asked for, or for a few other narrow purposes. Along these lines, COPRA allows processing to carry out the "specific" purpose "for which the covered entity has obtained affirmative express consent," or to "complete a transaction … specifically requested by an individual." Less helpful is COPRA's additional allowance of processing for the purpose "described in the privacy policy made available by the covered entity." We suggest deletion of this allowance, because most consumers will not read the privacy policy.

Duty of loyalty. COPRA, in section 101, would bar companies from processing or transferring data in a manner that is "deceptive" or "harmful." The latter term means likely to cause: a financial, physical, or reputational injury; an intrusion on seclusion; or "other substantial injury." This is a good step. We hope legislators will also explore "information fiduciary" obligations where the duty of loyalty would require the business to place the consumer's data privacy rights ahead of the business' own profits.

Duty to assess algorithmic decision-making impact. An entity must conduct an annual impact assessment if it uses algorithmic decision-making to determine: eligibility for housing, education, employment, or credit; distribution of ads for the same; or access to public accommodations. This annual assessment—as described in section 108(b)—must address, among other things, whether the system produces discriminatory results. This is good news. EFF has long sought greater transparency about algorithmic decision-making.

Duty to build privacy protection systems. A covered entity must designate a privacy officer and a data security officer. These officers must implement a comprehensive data privacy program, annually assess data risks, and facilitate ongoing compliance with COPRA's section 202. Moreover, the CEO of a "large" covered entity must certify, based on review, the existence of adequate internal controls and reporting structures to ensure compliance. COPRA in section 2(15) defines a "large" entity as one that processes the data of 5 million people or the sensitive data of 100,000 people. These COPRA rules will help ensure that businesses build the privacy protections systems needed to safeguard consumers' personal information.

Duty to publish a privacy policy. A covered entity must publish a privacy policy that states, among

other things, the categories of data it collects, the purpose of collection, the identity of entities to which it transfers data, and the duration of retention. This language, in section 102(b), will advance transparency.

Duty to secure data. A covered entity must establish and implement reasonable data security practices, as described in section 107.

Scope of Coverage

Consumer data privacy laws must be scoped to particular data, to particular covered entities, and with particular exceptions.

Covered data. COPRA, in section 2(8)(A) protects "covered data," defined as "information that identifies, or is linked or reasonably linkable to an individual or a consumer device, including derived data." This term excludes de-identified data, and information lawfully obtained from government records.

We are pleased that "covered data" extends to "devices," and that "derived" data includes "data about a household" in section 2(11). Some businesses track devices and households, without ascertaining the identity of individuals.

Unfortunately, COPRA defines "covered data" to exclude "employee data," meaning personal data collected in the course of employment and processed solely for employment in sections 2(8)(B)(ii) and 2(12). For many people, the greatest threat to data privacy comes from their employers and not from other businesses. Some businesses use cutting-edge surveillance tools to closely scrutinize employees at computer workstations (including their keystrokes) and at assembly lines (including wristbands to monitor physical movements). Congress must protect the data privacy of workers as well as consumers.

Covered entities. COPRA, as outlined in section 2(9) applies to every entity or person subject to the FTC Act. That Act, in turn, excludes various economic sectors, such as common carriers, per 15 U.S.C. 45(a)(2). Hopefully, this COPRA limitation reflects the jurisdictional frontiers of the various congressional committees—and the ultimate federal consumer data privacy bill will apply across economic sectors.

COPRA excludes "small business" from the definition of "covered entity" under sections 2(9) & (23). EFF supports such exemptions, among other reasons because small start-ups often are engines of innovation. Two of COPRA's three size thresholds would exclude small businesses: $25 million in gross annual revenue, or 50% of revenue from transferring personal data. But COPRA's third size threshold would capture many small businesses: annual processing of the personal data of 100,000 people, households, or devices. Many small businesses have websites that process the IP addresses of 300 visitors per day. We suggest deleting this third threshold, or raising it by an order of magnitude.

Exceptions. COPRA contains various exemptions, listed in sections 110(c) through 110(g). Importantly, it includes a journalism exemption in section 110(e): "Nothing in this title shall apply to the publication of newsworthy information of legitimate public concern to the public by a covered entity, or to the processing or transfer of information by a covered entity for that purpose. This exemption is properly framed by the activity of journalism, which all people and organizations have a First Amendment right to exercise, regardless of whether they are a professional journalist or a news organization.

COPRA, in section 110(d)(1)(D), exempts the processing and transfer of data as reasonably necessary "to protect against malicious, deceptive, fraudulent or illegal purposes." Unfortunately, many businesses may interpret such language to allow them to process all manner of personal data, in order to identify patterns of user behavior that the businesses deem indicative of attempted fraud. We urge limitation of this exemption.

Conclusion

We thank Sen. Cantwell for introducing COPRA. It is a strong step forward in the national conversation over how government should protect us from businesses that harvest and monetize our personal information. While we will seek strengthening amendments, COPRA is an important data privacy framework for legislators and privacy advocates.

Related Issues
Privacy

Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

Don't fill out this field (required)

Thanks, you're awesome! Please check your email for a confirmation link.

Oops something is broken right now, please try again later.

Related Updates

Deeplinks Blog
by Adam Schwartz
| February 27, 2024
Sen. Wyden Exposes Data Brokers Selling Location Data to Anti-Abortion Groups That Target Abortion Seekers

This post was written by Jack Beck, an EFF legal internIn a recent letter to the FTC and SEC, Sen. Ron Wyden (OR) details new information on data broker Near, which sold the location data of people seeking reproductive healthcare to anti-abortion groups. Near enabled these groups to send...

Deeplinks Blog
by Saira Hussain, Sophia Cope
| February 27, 2024
EFF to D.C. Circuit: The U.S. Government’s Forced Disclosure of Visa Applicants’ Social Media Identifiers Harms Free Speech and Privacy

Special thanks to legal intern Alissa Johnson, who was the lead author of this post.EFF recently filed an amicus brief in the U.S. Court of Appeals for the D.C. Circuit urging the court to reverse a lower court decision upholding a State Department rule that forces visa applicants to...

Deeplinks Blog
by Jason Kelley, Aaron Mackey, Joe Mullin

| February 15, 2024
Don’t Fall for the Latest Changes to the Dangerous Kids Online Safety Act

The authors of the dangerous Kids Online Safety Act (KOSA) unveiled an amended version this week, but it’s still an unconstitutional censorship bill that continues to empower state officials to target services and online content they do not like.

Deeplinks Blog
by Mario Trujillo
| February 14, 2024
EFF to Court: Strike Down Age Estimation in California But Not Consumer Privacy

The Electronic Frontier Foundation (EFF) called on the Ninth Circuit to rule that California’s Age Appropriate Design Code (AADC) violates the First Amendment, while not casting doubt on well-written data privacy laws.

Deeplinks Blog
by Jason Kelley
| February 13, 2024
Privacy Isn't Dead. Far From It.

Welcome! The fact that you’re reading this means that you probably care deeply about the issue of privacy, which warms our hearts. Unfortunately, even though you care about privacy, or perhaps because you care so much about it, you may feel that there's not much you (or anyone) can really...

Deeplinks Blog
by Karen Gullo
| February 7, 2024
Protect Good Faith Security Research Globally in Proposed UN Cybercrime Treaty

Statement submitted to the UN Ad Hoc Committee Secretariat by the Electronic Frontier Foundation, accredited under operative paragraph No. 9 of UN General Assembly Resolution 75/282, on behalf of 124 signatories. We, the undersigned, representing a broad spectrum of the global security research community, write to express our serious concerns...

Deeplinks Blog
by Karen Gullo
| February 7, 2024
Draft UN Cybercrime Treaty Could Make Security Research a Crime, Leading 124 Experts to Call on UN Delegates to Fix Flawed Provisions that Weaken Everyone’s Security

Security researchers’ work discovering and reporting vulnerabilities in software, firmware, networks, and devices protects people, businesses and governments around the world from malware, theft of critical data, and other cyberattacks. The internet and the digital ecosystem are safer because of their work.The UN Cybercrime Treaty,...

Press Release
| January 31, 2024
Dozens of Rogue California Police Agencies Still Sharing Driver Locations with Anti-Abortion States

California Attorney General Rob Bonta should crack down on police agencies that still violate Californians' privacy by sharing automated license plate reader information with out-of-state government agencies, putting abortion seekers and providers at particular risk, the Electronic Frontier Foundation (EFF) and the state's American Civil Liberties Union (ACLU) affiliates urged...

Deeplinks Blog
by Paige Collings
| January 31, 2024
EFF and Access Now's Submission to U.N. Expert on Anti-LGBTQ+ Repression

As part of the United Nations (U.N.) Independent Expert on protection against violence and discrimination based on sexual orientation and gender identity (IE SOGI) report to the U.N. Human Rights Council, EFF and Access Now have submitted information addressing digital rights and SOGI issues across the globe. The submission addresses...

Deeplinks Blog
by Karen Gullo
| January 29, 2024
In Final Talks on Proposed UN Cybercrime Treaty, EFF Calls on Delegates to Incorporate Protections Against Spying and Restrict Overcriminalization or Reject Convention

UN Member States are meeting in New York this week to conclude negotiations over the final text of the UN Cybercrime Treaty, which—despite warnings from hundreds of civil society organizations across the globe, security researchers, media rights defenders, and the world's largest tech companies—will, in its present form, endanger...

Discover more.
Email updates on news, actions, events in your area, and more.

Email Address

Postal Code (optional)

Anti-spam question: Enter the three-letter abbreviation for Electronic Frontier Foundation:

Don't fill out this field (required)

Thanks, you're awesome! Please check your email for a confirmation link.

Oops something is broken right now, please try again later.

Share It
Share on Twitter
Share on Facebook
Copy link

Related IssuesPrivacy

Back to top

Follow EFF:

x
facebook
instagram
youtube
flicker
linkedin
mastodon
tiktok
threads

Check out our 4-star rating on Charity Navigator.

Contact
General
Legal
Security
Membership
Press

About
Calendar
Volunteer
Victories
History
Internships
Jobs
Staff
Diversity & Inclusion