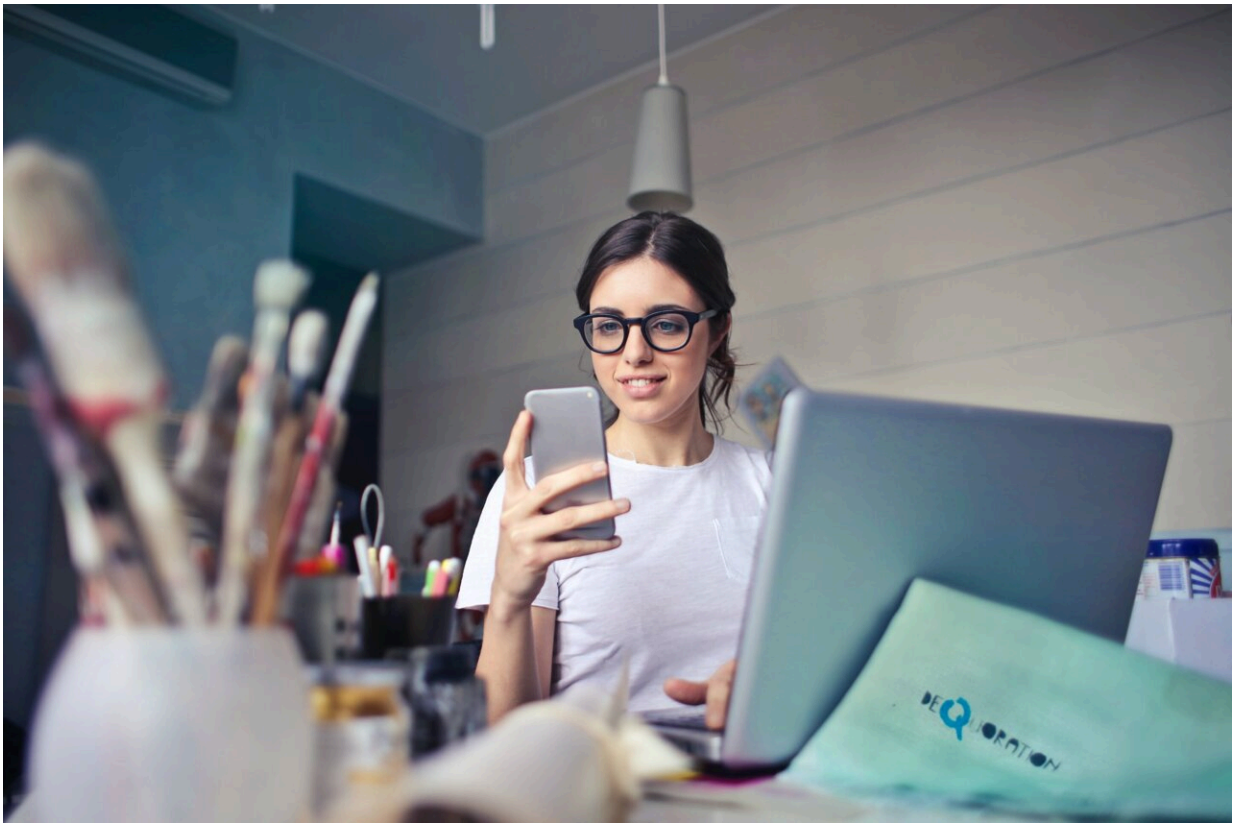
Privacy advocates demand rules for mobile providers on data use

September 6 2022, by Keith Lewis



Credit: Unsplash/CC0 Public Domain

Privacy advocates are demanding standards for mobile service providers' handling of sensitive customer information, especially location data, after a Federal Communications Commission inquiry into the top 15

carriers revealed a huge variation within the industry's data retention and consumer privacy protocols.

T-Mobile U.S. Inc. stores customer data, including location information, for up to 24 months, it told the regulator. AT&T Mobility, including its subsidiary Cricket Wireless, stores locations and most other user data for 13 months, but it stores some call records for up to five years, it reported.

Verizon Wireless, the nation's largest carrier, stores users' personal data, including locations, for one year, although it said its on-board vehicle diagnostic application stores it for up to five years. Mint Mobile LLC, the prepaid budget virtual mobile provider, stores data, including location information, for up to 18 months, it said.

Not all carriers sell location data to third party marketing firms, but those that do outlined unique processes that consumers have to navigate to opt out of authorizing their data to be sold, sometimes with different rules applying to call record details and location data.

The carriers' responses were "all over the map," according to Harold Feld, senior vice president at Public Knowledge, a Washington public interest group focused on digital privacy.

"The only 'industry standard' appears to be that there is no standard at all for how long carriers retain data, how they protect it, or how hard they make it for their customers to invoke their rights," Feld added.

Public Knowledge is urging the commission to pass strong data privacy regulations to protect so-called customer proprietary network information.

'Mobile phones know a lot about us'

"Customer proprietary network information," as defined by Section 222 of a 1996 law (PL 104-104), includes any data that mobile carriers are required to safeguard, such as numbers dialed, call duration, and, perhaps most sensitive, the locations the user visited while their device was pinging a cell tower.

"Our mobile phones know a lot about us," FCC Chairwoman Jessica Rosenworcel said in an Aug. 25 statement. "That means carriers know who we are, who we call, and where we are at any given moment. This information and geolocation data is really sensitive. It's a record of where we've been and who we are."

"That's why the FCC is taking steps to ensure this data is protected," she added.

Rosenworcel, a Democrat, appears poised to crack down on data policies for mobile carriers and follow through on her sharp dissent in a 2020 FCC decision to fine the four largest carriers at the time. She argued the commission's collective $200 million fine against T-Mobile, Sprint, AT&T, and Verizon for selling users' data to third parties without their consent didn't resolve the problems.

The then-Republican-controlled commission reduced the fine from a potential $40,000 per day fine for the duration of the violation to $2,500 per day. Rosenworcel wrote in dissent that the commission's "bureaucratic math" aiming to ease the punishment was unwarranted.

With Rosenworcel now at the commission's helm and a Democratic majority in sight if Biden's controversial FCC pick Gigi Sohn is confirmed by the Senate, the FCC is now more likely to tighten the rules around mobile carriers' management and authority to sell consumer data.

Congress could beat them to it, but only if it overcomes a dispute about

the interaction of federal and state authority on privacy regulation.

The House is working on bipartisan legislation that would establish clearer standards for data privacy, but its provisions may not satisfy the staunchest privacy advocates unless it clearly allows states like California the ability to be more strict, according to some lawmakers.

A bill was approved, 53-2, by the House Energy and Commerce Committee on July 20. It is sponsored by Chairman Frank Pallone Jr., D-N.J., and co-sponsored by ranking member Cathy McMorris Rodgers, R-Wash. Leaders of the Subcommittee on Consumer Protection and Commerce, Chair Jan Schakowsky, D-Ill., and ranking member Gus Bilirakis, R-Fla., are also backing it.

House Speaker Nancy Pelosi, D-Calif., said Sept. 1 that lawmakers would need to work on the bill, saying it doesn't provide the same consumer protections as existing California law.

The House bill, with more than 20 amendments adopted in committee, may also not gain the approval of Senate Commerce Chair Maria Cantwell, D-Wash. Cantwell and some progressive Democrats don't want federal law to preempt states from passing stricter data privacy laws.

Republicans, on the other hand, are worried that a state-by-state patchwork of rules, rather than a national standard, could make compliance too onerous on businesses.

Partisan division means the bill faces a slim chance of passage in the evenly split Senate.

Provisions of the House legislation include ensuring a "clear and conspicuous, easy-to-execute means" for customers to easily withdraw their consent to the sale of their personal data.

Carriers would be entirely banned from selling data related to minors under age 17 or using children's information for any targeted marketing purposes.

It would also require the Federal Trade Commission to adopt regulations within two years that establish more specific data privacy safeguards that include certain minimum standards, training obligations and requirements for written retention and corrective action plans. Carriers would have a duty under the law to mitigate "reasonably foreseeable risks or vulnerabilities."

Reproductive privacy

Privacy concerns grew more urgent in the eyes of many after the Supreme Court overturned a constitutional right to abortion in the Dobbs v. Jackson Women's Health Organization case in June. For Democrats, the ruling encouraged them to back stronger privacy protections amid fears that user locations and other data could be used to spy on individuals seeking abortion services in states that restrict it.

Many privacy advocates raised alarms in the wake of the Dobbs decision about the sensitive nature of personal data stored on menstrual-tracking applications used by millions of women.

Cantwell is among a dozen co-sponsors of a bill introduced after a draft of the Dobbs opinion leaked in May. The bill would prohibit organizations that collect information about individuals' sexual or reproductive health from disclosing it to third parties unless doing so is essential for medical care.

The bill, which includes a private right to sue, would apply to a broad range of companies, including mobile communications providers and technology companies that operate menstrual-tracking apps.

Even though Congress may be unable to agree on robust data privacy protection legislation right now, the FCC "can and should do more" to protect consumers, according to Public Knowledge's Feld.

"Right now, customers must negotiate a confusing maze of carrier practices and notifications," Feld said. "The FCC is more than an enforcer; it is a regulator. The FCC should set new rules of the road so that subscribers have the privacy we need and deserve."