July 22, 2024

The Honorable Maria Cantwell
Chair
U.S. Senate Committee on
Commerce, Science & Transportation
Washington, DC 20510

The Honorable Ted Cruz
Ranking Member
U.S. Senate Committee on
Commerce, Science & Transportation
Washington, DC 20510

RE: Follow-up to Hearing on "The Need to Protect Americans' Privacy and the AI Accelerant"

Dear Chair Cantwell and Ranking Member Cruz:

The Main Street Privacy Coalition (MSPC)[1] and its 20 national trade association members wrote to you earlier this month in connection with the Senate Commerce Committee's July 11 hearing on privacy. We wanted to send this brief letter reiterating some of our views in light of the breach of "nearly all" AT&T wireless customers' data that became public following the hearing.[2]

As explained in the press reports to date, the breach began through illicit access to an account with a cloud data storage company. In fact, more than 100 of the businesses that use that cloud data storage provider have had their data compromised in the past few months. Based on the reporting, the wireless network itself was not breached. Instead, just the cloud data storage provider – the 'service provider' in the parlance of the draft American Privacy Rights Act (APRA) – was breached.

The recent Microsoft system outage impacting businesses, airlines and banks around the world provides another salient example of the key role played by 'service providers' in nearly every aspect of our economy.[3] In that example, problems with a cybersecurity software company used by large numbers of American businesses had a crippling impact on very diverse operations for businesses that relied on that service, including Main Street businesses' payments systems.

The data breach and widespread outages enhance the importance of several MSPC principles that we recommended to you in our previous letter. In particular, as we noted in that letter, service providers and third parties must have direct statutory obligations protecting the privacy and security of each covered entity's data they process in federal privacy legislation. And, on top of that, all businesses – whether they are categorized as covered entities, service providers, or third

[1] The Main Street Privacy Coalition website and member list may be accessed at: https://mainstreetprivacy.com.
[2] Joseph Menn and Aaron Gregg, "AT&T says hackers stole call records of 'nearly all' wireless customers," Washington Post (July 12, 2024)(available at AT&T says hacker stole call records of 'nearly all' wireless customers - The Washington Post).
[3] Gareth Vipers and Sam Schechner, "Major IT Outage Grounds Flights, Hits Banks and Businesses Worldwide," Wall Street Journal (July 19, 2024) (available at Major IT Outage Grounds Flights, Hits Banks and Businesses Worldwide - WSJ)

parties – must be accountable for their own actions. If that does not happen, the rights and protections of consumers will be compromised. Any category of business that can create a loophole such that it isn't legally required to follow federal regulations or that it is not held responsible or accountable for its own shortcomings with respect to following those regulations will inevitably become a weak spot in the chain of data that can be easily exploited.

The data breach affecting AT&T wireless customers and the Microsoft system outage impacting millions of Americans remind us once again that consumers' data is shared across a broad ecosystem and that every part of that data ecosystem must be subject to equivalent regulation in order to protect that data.

To demonstrate the shortcomings of the House-introduced version of the APRA (H.R. 8818) on this count, we previously sent you the attached chart. It clearly shows how the APRA disproportionately impacts Main Street businesses compared to service providers and third parties: notably, *all* of the subsections of the bill enforceable by a private right of action (PRA) apply to our businesses as "covered entities," however *only 3* PRA-enforceable subsections apply to Big Tech "service providers" such as cloud data storage businesses and *none of them* apply to Big Tech "third parties." Moreover, section 111(a)'s and (b)'s direct requirements for Big Tech service providers and third parties, respectively, are <u>not</u> subject to the PRA.

This simply isn't right and there could not have been clearer proof of that then the stories about the wireless breach and outage that quickly followed the Committee's hearing and impacted millions of consumers. As in the past, we urge the Committee to craft legislation, consistent with our principles, that would hold Big Tech service providers and third parties accountable to the *same* extent as Main Street businesses by carefully aligning the APRA's service provider requirements to match the more consumer-protective provisions adopted in nearly every one of the 19 enacted comprehensive state privacy laws.

Improving the APRA this way would protect Americans against loopholes that leave consumers unprotected when their personal data is handled by these business partners that most covered entities cannot police through contracts alone given the imbalance in negotiating leverage.

We appreciate your consideration of our views on federal data privacy and security legislation. We also stand ready to work constructively with you to ensure legislation adopted by this Committee reflects our principles, avoids disproportionately impacting Main Street businesses compared to other industry sectors, and properly holds Big Tech service providers accountable to an equivalent level under the law.

Sincerely,

The Main Street Privacy Coalition

Attachment
cc: Members of the U.S. Senate Committee
on Commerce, Science & Transportation

Disproportionate Impact of APRA's Private Rights of Action ("PRA") on Main Street Businesses ("Covered Entities")[1]

APRA Sections Subject to PRA	Covered Entities (X = section applies)	Service Providers (N/A = not applicable)	Third Parties (N/A = not applicable)
Data Minimization (§102)			
• §102(b) Sensitive Data Transfers	X	N/A	N/A
• §102(c) Biometric Info and Genetic Info (e.g., includes collection, processing, retention, transfer, etc.)	X	N/A	N/A
Transparency (§104)			
• §104(a) Privacy Policy Publicly Available	X	X	N/A
• §104(e) Material Changes to Privacy Policy (including Notice and Opt Out)	X	N/A	N/A
Individual Control Over Covered Data (§105) (e.g., consumer rights of access, correction, deletion, and portability of covered data):			
• §105 (all subsections)	X	N/A	N/A
Opt-Out Rights and Universal Mechanism (§106)			
• §106 (a)	X	N/A	N/A
• §106 (b)(2)	X	N/A	N/A
Interference with Consumer Rights ("Dark Patterns Prohibited") (§107)			
• §107 (all subsections)	X	N/A	N/A
Prohibition on Denial of Service and Waiver of Rights (including, "Service or Pricing" in "Bona Fide Loyalty Programs") (§108)			
• §108 (all subsections)	X	N/A	N/A
Data Security and Protection of Covered Data (§109)			
• §109 (a) – "to the extent such action alleges a data breach arising from a violation of subsection (a)"	X	X	N/A
Service Providers and Third Parties (§111)			
• §111(a) Service Provider Requirements – **NOT subject to the PRA**		N/A	
• §111(b) Third Party Requirements – **NOT Subject to the PRA**			N/A
• §111(d) Reasonable Care in Selecting Service Providers or Transfers of Data to Third Parties	X	X	N/A
Data Brokers (§112)			
• §112(c)(4) – "Do Not Collect" and "Delete My Data" Requests	X *(a data broker is a "covered entity" that meets the definition of a "data broker")*	N/A	N/A

[1]*Chart prepared by Main Street Privacy Coalition based on section 117(a)(1) of H.R. 8818, the American Privacy Rights Act (APRA).*