

A person wearing a blue button-down shirt is seated at a desk, typing on a silver laptop. The scene is brightly lit by natural light from a window in the background, creating a soft, professional atmosphere. The person's hands are positioned on the keyboard, and the laptop is open in front of them.

ISSUE BRIEF: Q1 2020

A COMPREHENSIVE APPROACH TO CONSUMER DATA PRIVACY

► **BUSINESSFORWARD**

INTRODUCTION

Business Forward has organized hundreds of briefings across the country on technology and innovation, collecting recommendations from local business leaders on a range of issues, from how to protect IP to helping small businesses use the internet to find new markets. Few issues are as important as data privacy. This issue brief explains why data privacy matters and outlines a comprehensive approach to protecting it.

At our briefings, business leaders often recommend “going back to Obama’s approach.” With data privacy, these business leaders typically refer to one of two Obama-era policy frameworks. In 2012, an administration-wide review managed by Cameron Kerry, general counsel of the U.S. Commerce Department, produced a “Consumer Privacy Bill of Rights.” That same year, the FTC, chaired by Obama-appointee Jon Leibowitz, published its “Protecting Consumer Privacy in an Era of Rapid Change” report.

This issue brief relies on both reports, as well as recent commentary from Kerry (now at the Brookings Institution).

“

We know how polarized Congress is and how dysfunctional our politics can be, but I think in this moment both parties have an incentive to show that they can get something done.¹

”

- CAMERON KERRY

1

CURRENT PRIVACY LAWS CANNOT KEEP UP

Today's reliance on "consumer notice and consent" is unworkable. The terms and conditions we agree to when we click "accept" are too long to read, difficult to understand, and offer little protection. We must establish affirmative duties that shift responsibility from consumers to the businesses collecting and using their data.

2

THE DANGER TO CONSUMERS AND SMALL BUSINESSES IS IMMENSE – AND HIGHLY PERSONAL.

Traditionally, laws have focused on "personally identifiable" data (like Social Security numbers) and "sensitive" data (like health records). But as companies track more of your actions online and over your phone, and build ever-richer data "profiles" on you, privacy laws need to be updated to reflect this new reality.

3

A COMPREHENSIVE APPROACH IS CRITICAL AND GROWING MORE POPULAR

Our network generally prefers a "tech neutral" approach that treats application providers, data brokers, broadband providers, and retailers alike – so that no player gets a free pass. Most favor a national standard over 50 individual state standards.

4

AS PUBLIC CONCERN GROWS, A DEAL BECOMES MORE LIKELY

Privacy advocates are growing more powerful. Tech executives, adapting to privacy regulations in Europe and facing a growing number of state privacy bills, are looking for certainty here in the U.S. Republicans in Congress have grown more open to regulations they blocked during the Obama Administration.

WHO'S WHO IN DATA PRIVACY

When you search with Google, surf the web, purchase something on Amazon, order an Uber, or browse videos on YouTube, **you share information about yourself that other companies are willing to buy.**

When you visit a website, sign up for a service, or download an app on your smartphone, you're typically asked to "accept" terms and conditions that govern whether and how the provider may **collect, use, and share information** about you that it gathers. At any one time, dozens of companies could be tracking the location of your smart phone, or what you're typing on it.

Finally, some **companies collect data about you when you may not expect it.** Retailers use "beacons" that track your smartphone signal as you walk their aisles. Other businesses deploy cameras using facial recognition or license plate reading software to identify you as you walk or drive by.

Thanks to (1) billions of new devices, (2) thousands of new applications, (3) greater bandwidth that moves data faster, and (4) increasingly cheap data storage, the world's consumers will produce **463 exabytes of data every day by 2025.**² (One exabyte is 1,000,000,000,000,000,000 bytes.) The global volume of data doubles every two years.

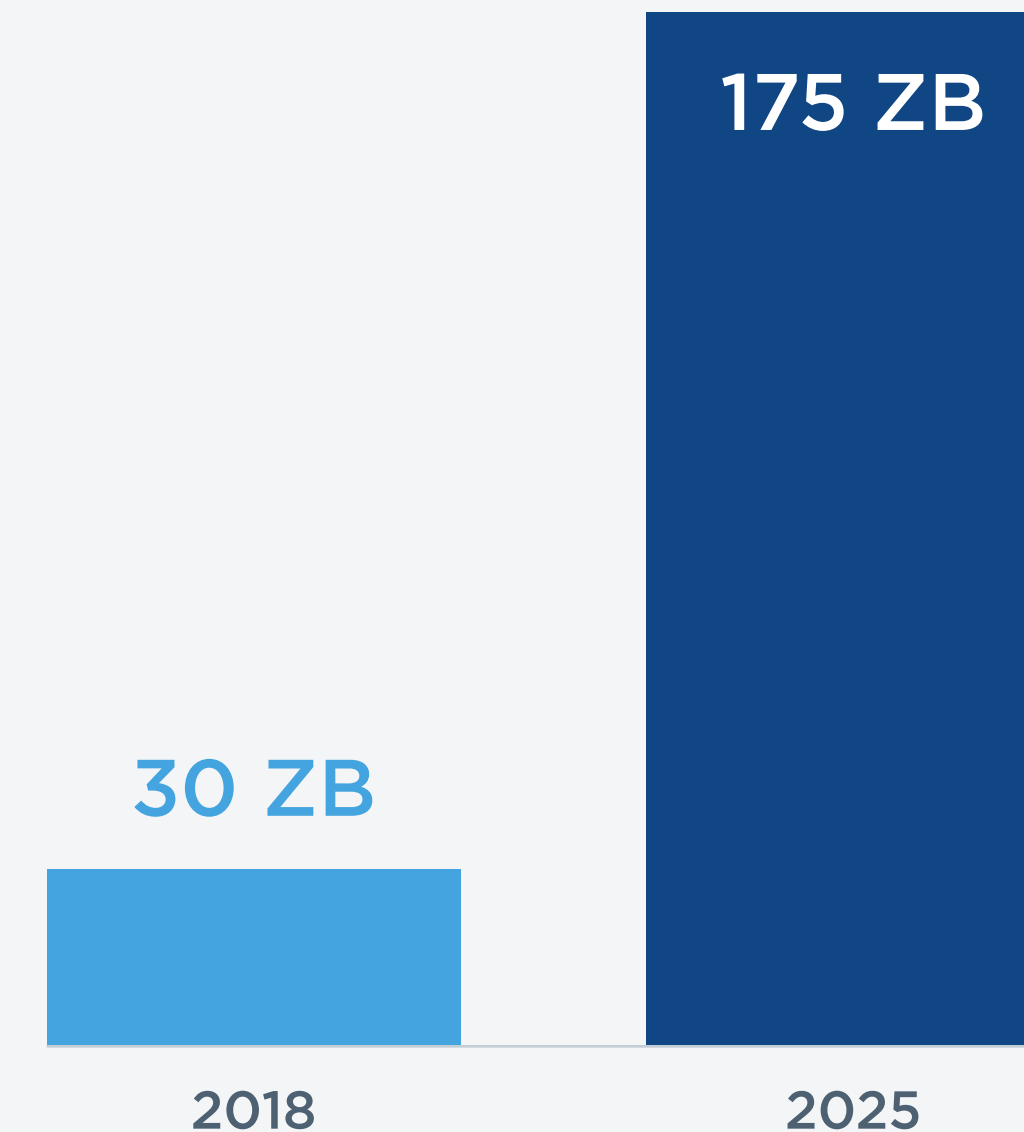


AS DATA VOLUME GROWS, DATA RISK RISES

The range of information that companies collect that can uniquely identify you is growing very quickly. Individual data points that may not be sensitive on their own can be aggregated to form detailed, highly personal profiles. This makes defining “personal information” or “sensitive information” more difficult.

When a company that collects your data shares it with a third party, your risks grows even more. Most proposals would allow companies to share data only if it is necessary for them to execute the job you’ve tasked them to perform – and provided the third party agrees to the same privacy and security obligations as the first company. These third parties should not be allowed to use the data for new or additional purposes.

THE ANNUAL SIZE OF THE GLOBAL DATASPHERE WILL REACH 175 ZB BY 2025³



CURRENT LAWS CANNOT KEEP UP

Our current data privacy rules rely on “notice and choice,” the idea that consumers can read privacy policies and make their own decision about whether sharing their data is worth the service they obtain in return. This puts the burden on consumers, not the companies competing for their business.

“

More and more data about each of us is being generated faster and faster from more and more devices, and we can’t keep up. It’s a losing game both for individuals and for our legal system. If we don’t change the rules of the game soon, it will turn into a losing game for our economy and society.⁴

”

- CAMERON KERRY

OLD PARADIGM	PROBLEM	NEW PARADIGM
Rely on consumer notice and consent.	Today’s consumer warnings are obscure, complex, and impossible to read on a smartphone.	Shift more responsibility to businesses through duties of care and loyalty.
Focus on deceptive practices.	FTC’s focus on deception allows consumers to give away too much control to businesses.	Prevent worst data practices outright. Limit third parties’ ability to use data for other purposes. Create a data broker registry.
Focus on sensitive, personally identifiable data and create rules on a case-by-case basis.	Buckshot approach to privacy cannot keep up with new types of data, new uses for data, and aggregation of data across devices.	The context in which data was shared should govern the uses to which data can be put.

“BACK TO OBAMA” = CONSUMER PRIVACY BILL OF RIGHTS

We worked with hundreds of Obama Administration officials, organized hundreds of briefings on technology and innovation, and brought thousands of business leaders to the White House to meet with the President Obama’s economic advisors. At briefings over the past two years, we’re leaders in our network often recommended, “Let’s go back to Obama’s approach.”

Cam Kerry, general counsel of the Department of Commerce during Obama’s first term, led an administration-wide effort that produced a Consumer Privacy Bill of Rights. It articulated seven principles, which operate as a good start for new legislation.⁵

1

INDIVIDUAL CONTROL

Consumers should be able to control the personal information that is shared and disseminated by data organizations.

2

TRANSPARENCY

Consumers should be able to understand data organizations’ practices.

3

RESPECT FOR CONTEXT

Consumers have a right to expect that organizations use their data in ways that are consistent with how it was originally collected.

4

SECURITY

Consumers have a right to expect that organizations handle their data responsibly.

5

ACCESS & ACCURACY

Consumers have a right to access and correct their data when appropriate (if its incorrectness poses a risk to consumers).

6

FOCUSED COLLECTION

Consumers have a right to request reasonable limits on the volume of data that organizations collect.

7

ACCOUNTABILITY

Consumers have a right to be assured that companies are being held accountable to the standards set forth in the Bill of Rights.

WHAT VOTERS THINK

PERSONAL CONTROL IS IMPORTANT TO AMERICANS⁶

Controlling what information
is collected about you:



Being able to share confidential
matters with someone you trust:

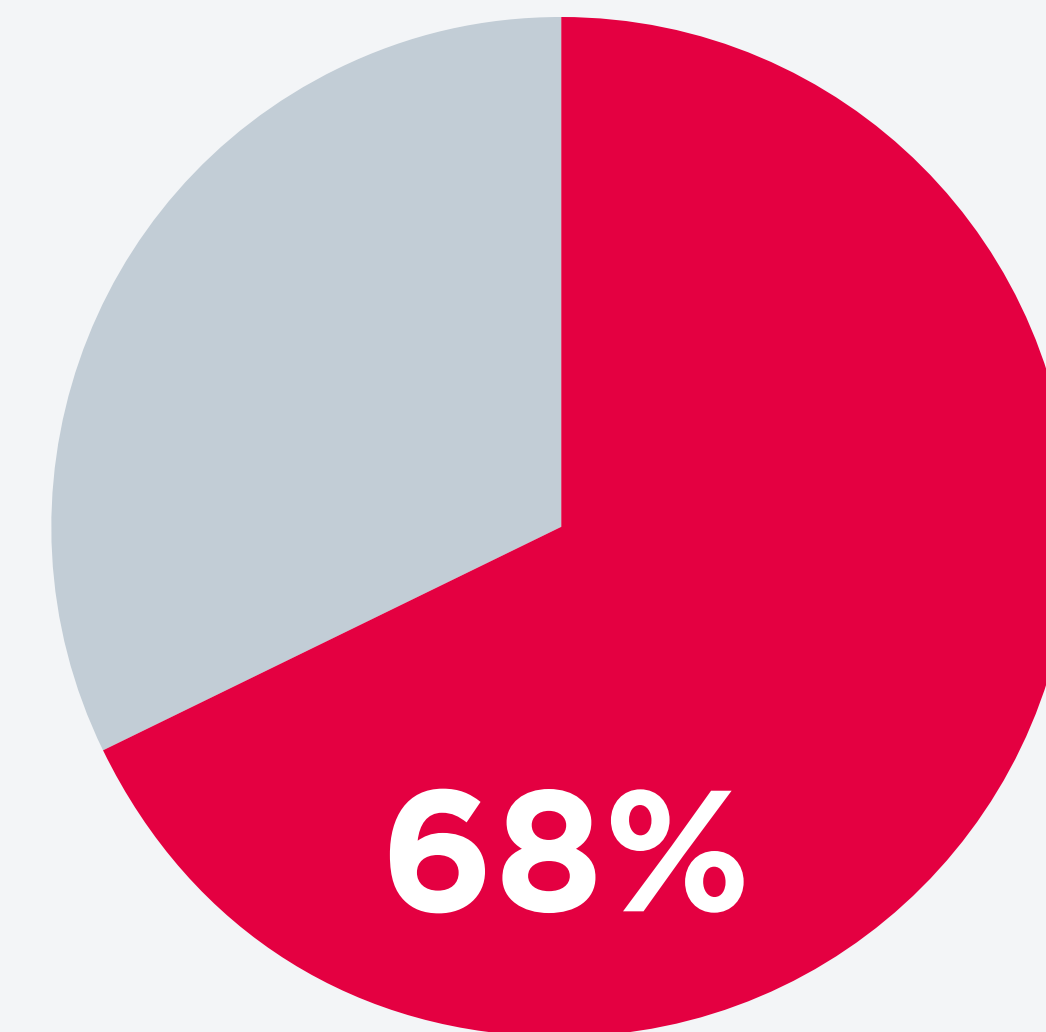


Being in control of who can
get info about you:



■ VERY IMPORTANT ■ SOMEWHAT IMPORTANT

THE PUBLIC WANTS THE GOVERNMENT TO ENACT LAWS THAT PROTECT PRIVACY⁷



OF INTERNET USERS BELIEVE
CURRENT LAWS ARE NOT
GOOD ENOUGH TO PROTECT
PRIVACY ONLINE.

PRIVACY REFORM BASICS

SHIFT FROM CONSUMER NOTICE TO BUSINESS BEHAVIOR

Identify and ban clearly unreasonable practices.

ESTABLISH DUTIES, APPLY THEM UNIFORMLY ACROSS PLAYERS

Your rights shouldn't depend on where or how your info gets collected.

REDUCE UNCERTAINTY AND RISK WITH A NATIONAL STANDARD

Floor or ceiling? Ceiling is better if it's high enough.



Federal preemption: privacy laws are like seat belts and pacemakers



CONTEXT OF HOW AND WHY DATA WAS COLLECTED SHOULD MATTER

You have the right not to be surprised by how your data is used. For example, Uber needs your location data to help drivers reach you, but you don't expect them to track you for the rest of the day.



“

We need to move from the system of a completely fictional consumer choice to a system that deals with how businesses behave.⁸

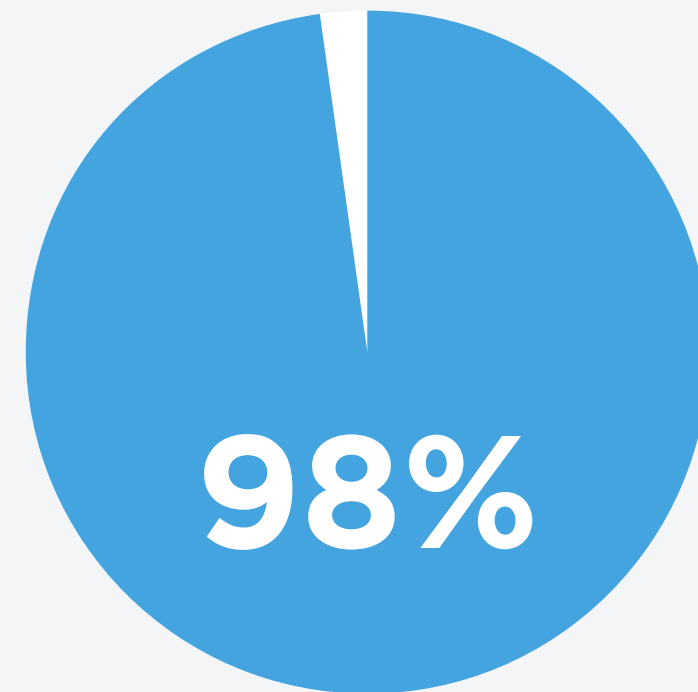
”

- CAMERON KERRY

WHAT SMALL BUSINESS OWNERS THINK

SMALL BUSINESSES FACE THE SAME CHALLENGES CONSUMERS DO

Few businesses have the IT expertise necessary to negotiate better terms than individuals do.



of America's 25 million companies have fewer than 20 employees.⁹

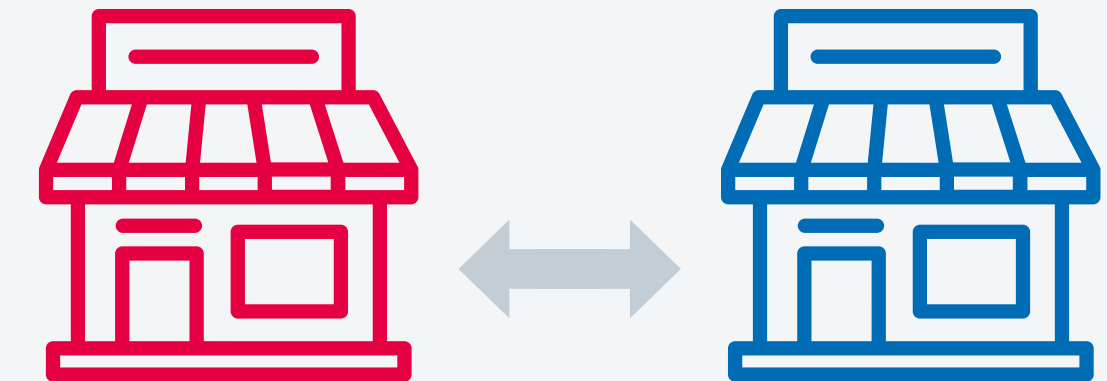
SMALL BUSINESSES WORRY ABOUT REGULATORY BURDEN AND WANT WORKABLE SOLUTIONS THEY CAN MANAGE AND AFFORD

Dry cleaners cannot afford HIPAA-like oversight.



SMALL BUSINESSES PREFER A NATIONAL STANDARD THAT APPLIES TO ACTORS IN ALL 50 STATES

Even small business owners do business across state lines.



WHAT SMALL BUSINESS OWNERS ARE SAYING

“

I believe we need to address...
privacy matters at the national
level so all states have uniformity
of rules and regulations.

”

- KAREN FOUAD
VICE PRESIDENT, BIOTRON,
FARMINGTON, UT

“

Privacy should be a priority,
and the internet should be fair
to all, not denied or given
inadequate service to the poor.

”

- LYNNETTE MYLAND
BLUEWATER AWNINGS,
ABSECON, NJ

“

Legislative solutions should...
provide for harsh penalties for clearly
defined abuses, such as...
breaches of privacy rights, and sharing
information in ways that threaten
national security.

”

- CLIFF BRUSH
CONTRACTOR,
LAKE OSWEGO, OR

KEY CONCEPTS

1

SHIFTING THE BURDEN FROM CONSUMERS TO BUSINESSES

Both major proposals in the Senate Commerce Committee (Sen. Wicker's draft bill and Sen. Cantwell's bill) shift at least part of the burden from consumers to the businesses collecting, using, and sharing their data.¹⁰

“

We need to move the responsibility off of individuals and onto the companies that are collecting and using the data and understand it.¹¹

”

- CAMERON KERRY

2

RESPECT FOR CONTEXT

If you share your location with Uber to allow Uber's driver to find you, Uber should not be able to track and share your location between rides with third parties that have nothing to do with its ride sharing service.

“

What should [privacy boundaries] be? Limiting the collection to what [businesses] really need and limiting the uses of that data to those purposes.¹²

”

- CAMERON KERRY

3

ENSURING TECH NEUTRALITY

Kerry and leaders in Congress generally agree that privacy laws should focus on what information is collected and how it is used, not who collects it.

Consumer privacy rules should apply to all companies, from broadband providers to edge providers, big box retailers to data brokers. Their technology- and industry-neutral approaches treat all data collectors the same.

Consumers seem to agree. A 2016 survey by Peter Hart found that 94% of internet users want all companies collecting their data online to follow the same rules.¹³

KEY CONCEPTS CONTINUED

4

DECIDING HOW EXEMPTIONS ARE MADE

A uniform, tech neutral approach is optimal, but allowances could be made for (1) highly sensitive data (like your health records) or (2) specific uses we need to protect (like allowing your car company to contact you about a recall).

“

A federal law that authorizes the Federal Trade Commission and state attorneys general to enforce it would give the United States the strongest privacy enforcement regime in the world... [It could] accomplish more than merely streamlining a patchwork of state laws.¹⁴

”

- CAMERON KERRY

5

PRE-EMPTING STATE LAWS

Leibowitz argues that privacy is a “quintessentially interstate issue.” “Put simply, data knows no state boundaries. A proliferation of differing state privacy rules would be infeasible to implement, and [it] would create inconsistent privacy protections for consumers based on where they live, work, or happen to access online services.”¹⁵ Under Leibowitz’s analysis, a Maine wireless customer visiting Texas should not have different privacy protections than a Texas wireless customer visiting Maine. Nor should a Maine resident have fewer privacy rights when traveling in New Hampshire.

6

DECIDING WHETHER TO INCLUDE A PRIVATE RIGHT OF ACTION

Consumers generally have had to rely on the FTC and state attorneys general to enforce privacy laws. Some privacy proposals would create a private right of action, which would allow consumers to sue a company if it violates its duty of care and it results in consumer damages. For example, the California Consumer Protection Act allows consumers harmed by a data breach to seek \$100-\$750 in financial compensation from the company that allowed the breach to occur.¹⁶ However, in many cases, consumers already have private rights of action under other laws (e.g. Fair Credit Reporting Act).

WHY A DEAL IS POSSIBLE

Having failed to pass legislation during the Obama Administration, Kerry is now optimistic: “This time, proposals may land on more fertile ground.”

“Tech companies, worried about growing consumer interest in privacy in the U.S. and complying already with new privacy laws in Europe, have grown more receptive.” They “see value in a common baseline that can provide people with assurance about how their data is handled and protected against outliers and outlaws... An increasing spread of state legislation on net neutrality, drones, educational technology, license plate readers, and other subjects and, especially broad new legislation in California pre-empting a ballot initiative, have made the possibility of a single set of federal rules across all 50 states look attractive.”¹⁷

“

There are things that are almost givens in this conversation that would have been off the table a few years ago.¹⁸

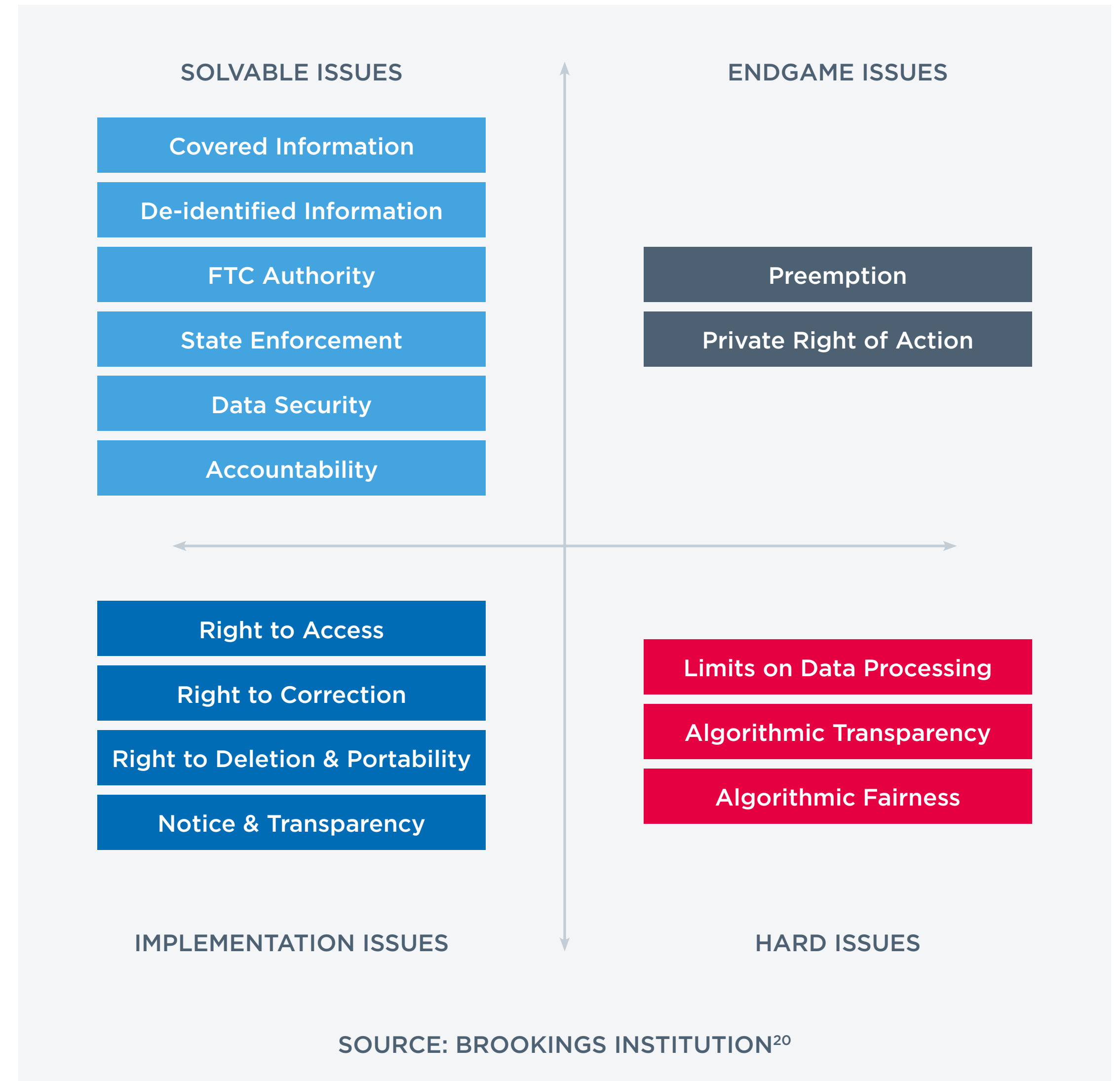
”

- CAMERON KERRY

WHAT A SENATE BILL MIGHT LOOK LIKE

Senate Commerce Committee chairman Roger Wicker (R-MS) and ranking member Maria Cantwell (D-WA), have put forth separate bills that could be the basis for bipartisan legislation.

Both proposals establish common ground by providing strong individual rights and setting boundaries on how businesses can use consumer data. However, the proposals diverge on certain issues, most notably the ability to sue companies for privacy violations (Cantwell's bill allows individual lawsuits for damages, while Wicker's bill avoids it altogether) and state preemption (Cantwell's bill only preempts directly conflicting state laws, whereas Wicker's bill preempts all state laws).¹⁹



REFERENCES

You can learn more about these frameworks and the data privacy debate below:

[“Why protecting privacy is a losing game today — and how to change the game”](#)

[“Rulemaking and its discontents: Moving from principle to practice in federal privacy legislation”](#)

[“Breaking down proposals for privacy legislation: How do they regulate?”](#)

1. Kerry, Cameron. 2020. “Briefing: Cameron Kerry on Privacy.” Interview by Ed Meier. Business Forward Podcast, Business Forward, February 12, 2020. Audio, 23:50. https://www.podomatic.com/podcasts/businessfwd/episodes/2020-02-19T10_59_46-08_00
2. DesJardins, Jeff. “How Much Data is Generated Each Day?” Visual Capitalist, April 15, 2019. <https://www.visualcapitalist.com/how-much-data-is-generated-each-day/>
3. Reinsel, David, Gantz, John, and John Rydning. The Digitization of the World From Edge to Core. Framingham, MA: IDC, November 2018. <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>
4. Kerry, Cameron. “Why Protecting privacy is a losing game today.” The Brookings Institution, July 12, 2018. <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>
5. The White House, Office of the Press Secretary. “We Can’t Wait: Obama Administration Unveils Blueprint for a “Privacy Bill of Rights” to Protect Consumers Online.” February 23, 2012. <https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights>
6. “The state of privacy in post-Snowden America.” Pew Research Center, September 21, 2016. <https://www.pewresearch.org/fact-tank/2016/09/21/the-state-of-privacy-in-america/>
7. Ibid.
8. Kerry, Cameron. 2020. “Briefing: Cameron Kerry on Privacy.” Interview by Ed Meier. Business Forward Podcast, Business Forward, February 12, 2020. Audio, 0:01. https://www.podomatic.com/podcasts/businessfwd/episodes/2020-02-19T10_59_46-08_00
9. “Facts & Data on Small Business and Entrepreneurship.” Small Business & Entrepreneurship Council, 2016. <https://sbecouncil.org/about-us/facts-and-data/>
10. Kerry, Cameron. “Game on: What to make of Senate privacy bills and hearing.” The Brookings Institution, December 3, 2019. <https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/>
11. Kerry, Cameron. 2020. “Briefing: Cameron Kerry on Privacy.” Interview by Ed Meier. Business Forward Podcast, Business Forward, February 12, 2020. Audio, 3:54. https://www.podomatic.com/podcasts/businessfwd/episodes/2020-02-19T10_59_46-08_00
12. Kerry, Cameron. 2020. “Briefing: Cameron Kerry on Privacy.” Interview by Ed Meier. Business Forward Podcast, Business Forward, February 12, 2020. Audio, 10:39. https://www.podomatic.com/podcasts/businessfwd/episodes/2020-02-19T10_59_46-08_00
13. “PRESS RELEASE: Consumers Want One Set of Rules Protecting Their Information.” Progressive Policy Institute, May 27, 2016. <https://www.progressivepolicy.org/press/press-releases/press-release-consumers-want-one-set-rules-protecting-information/>
14. Kerry, Cameron. “A federal privacy law could do better than California’s,” The Brookings Institution, April 29, 2019. <https://www.brookings.edu/blog/techtank/2019/04/29/a-federal-privacy-law-could-do-better-than-californias/>
15. U.S. Congress. Senate Committee on Commerce, Science, and Transportation. “America’s Privacy Moment: The Need For Strong Federal Privacy Protections That Give Consumers More Control Over Their Data.” Testimony of Jon Leibowitz, February 27, 2019. <https://www.commerce.senate.gov/services/files/3503047C-E9E6-4792-B079-4035D7197773>
16. Merken, Sara. “California Privacy Law May Spur Data Breach Lawsuit Wave,” Bloomberg Law, October 9, 2019. <https://news.bloomberglaw.com/privacy-and-data-security/california-privacy-law-may-spur-data-breach-lawsuit-wave>
17. Kerry, Cameron. “Why Protecting privacy is a losing game today.” The Brookings Institution, July 12, 2018. <https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/>
18. Carson, Angelique. “Cam Kerry leaves private practice to work on a federal bill full time,” IAPP News, March 26, 2019. <https://iapp.org/news/a/cam-kerry-leaves-private-practice-to-work-on-a-federal-bill-full-time/>
19. Kerry, Cameron. “Game on: What to make of Senate privacy bills and hearing.” The Brookings Institution, December 3, 2019. <https://www.brookings.edu/blog/techtank/2019/12/03/game-on-what-to-make-of-senate-privacy-bills-and-hearing/>
20. Chin, Caitlin and Maria Odell, “Highlights: Where stakeholders fall in the privacy debate.” The Brookings Institution, September 17, 2019. <https://www.brookings.edu/blog/techtank/2019/09/17/highlights-where-stakeholders-fall-in-the-privacy-debate/>



INFO@BUSINESSFWD.ORG

BUSINESSFWD.ORG

1155 CONNECTICUT AVENUE NW
SUITE 1000
WASHINGTON, D.C. 20036

202.861.1270

 **BUSINESSFORWARD**