SURVEY REVEALS AMERICANS OVERWHELMINGLY SUPPORT A NATIONAL DATA PRIVACY LAW

74% of Americans think it's time for a national privacy law -- yet only 27% of respondents believe the government is doing enough to protect data privacy, per PrivacyBee.com's latest National Privacy Survey of 1,001 Americans.

Atlanta, GA -- For 74% of Americans, "it's about time" that America has a national privacy law. Yet only 27% of respondents believe the U.S. government and regulators are doing enough to protect data privacy. This disconnect between what citizens and their representatives is in sharper focus during an election year that includes the Prop 24 privacy initiative on the California ballot. If the nation takes California's lead, what would a national privacy law look like?

What Americans expect from a national privacy law

Most Americans want more control over their data and their privacy. When it comes to what American expect from a national privacy law, they say the following rights are important or very important:

- ...the right **know how corporations use their personal data** (88%)
- ...the right to **know how corporations got their data in the first place** (88%)
- ...the right to **download personal data held by corporations** (84%)
- ...the right to **download personal data held by corporations** (84%)
- ...the right to **be forgotten** (83%)
- ...the right to **put an expiration date on personal data** (73%)

The right to an expiration date is especially notable. Some brands already

allow users to delete data after a certain point, such as Google's auto-delete controls for Location History and Web & App Activity. But the ability to choose how long personal data can be shared, held, or otherwise used by a corporation would be a big step towards complete data privacy control.

> *"The U.S. government and regulators have an opportunity to give citizens what they crave -- a national approach to privacy that offers consistency and control," says Privacy Bee CEO Harry Maugans.*

The current state of privacy

Everyone deserves their privacy. When it comes to privacy, Privacy Bee's survey found a disconnect between what consumers expect and what they're getting.

While 82% agree or strongly agree that privacy management should be convenient and easy, that's not what's happening.The most frequent words used to describe the state of privacy management were "difficult," "complicated," "confusing," and "powerless."

The vast majority of feelings were negative, underscoring just how frustrated Americans are with how difficult it is to take control of their personal data.

> *"It shouldn't be difficult or confusing to exercise your privacy rights," Maugans says. "But that's not what's happening: the majority of consumers feel that privacy management isn't living up to their expectations. There should be greater data controls, consistently and uniformly applied across the country."*

There's also low confidence among many consumers in the overall safety and privacy protection of our digital lives. And there's a large chunk of the country that isn't quite sure about their data's safety -- a warning sign that

corporations and governments aren't doing enough to protect consumers.

- **Only 31% are confident that their personal data is safe and protected while using computers and digital services. Interestingly enough, 26% are neutral, which underscores the continued importance of education around data protection best practices.**

The U.S. government could also do more to protect citizens. Politicians and regulators have an opportunity to give citizens what they crave -- a national approach to privacy that offers consistency and control.

- **51% disagree or strongly disagree that the government is doing enough when it comes to data privacy and protecting our personal data from hackers.**

Clearly, more must be done to legally empower citizens with rights to manage and protect their data privacy. It comes down to aligning incentives around data controls in the commercial context, says Lee Thien, Electronic Frontier Foundation's Legislative Director and Adams Chair for Internet Rights in response to the survey results:

> *"We share personal information with people as part of daily life. But the moment you shift to the commercial world, many companies have a bad business model for privacy because there are incentives to use and exploit the data. Even companies that don't have a strong incentive to do that still might have no strong incentive to protect users."*

Without that framework in place to balance incentives and tip the scales back in consumers' favor, there's going to be a continued disconnect between what Americans expect around data privacy and what their representatives deliver.

Download the full report **'What Americans Want from a National Data Privacy Law'** ***here:*** ***http://bit.ly/PrivacySurvey2020*****.**

QUOTES

Harry Maguans, CEO of Privacy Bee:

- "The U.S. government and regulators have an opportunity to give citizens what they crave -- a national approach to privacy that offers consistency and control."

- "It shouldn't be difficult or confusing to exercise your privacy rights. With proper privacy controls, consumers are empowered. But that's not what's happening: the majority of consumers feel that privacy management isn't living up to their expectations.And when companies like Apple try to streamline privacy for users, just look what happens -- immense industry blowback that puts corporate interests ahead of consumers."

- "The country is split as far as trusting companies to protect their data and privacy. The undecided middle could be swayed by being directly impacted by a data breach or identity theft. Companies must earn (and maintain) that trust and show consumers they care."

- "Most Americans don't feel like their privacy matters enough to the corporations that monetize it and governments that regulate it. Overall, there's low confidence among many consumers in the overall safety and privacy protection of our digital lives. And there's a large chunk of the country that isn't quite sure about their data's safety -- that's a warning sign too!"

Lee Thien, Electronic Frontier Foundation's Legislative Director

- "There are things we think are important in a national data privacy law. If such a law does not allow ordinary people to directly sue companies for data privacy and security violations/harms, then that law is deeply flawed."
- "We share personal information with people as part of daily life. But the moment you shift to the commercial world, many companies have a bad business model for privacy because there are incentives to use and exploit the data. Even companies that don't have a strong incentive to do that still might have no strong incentive to protect users."

- "The important thing here is that there's tremendous disagreement about a single thing: do I trust companies? Obviously, if you understand the advertising model, you know that the ad-based companies treat "you" (your attention") as the product. They make money from using/sharing/monetizing data about you. It is simply irrational and illogical to "trust" a for-profit company to protect *your* data/privacy when they're built to maximize shareholder value."

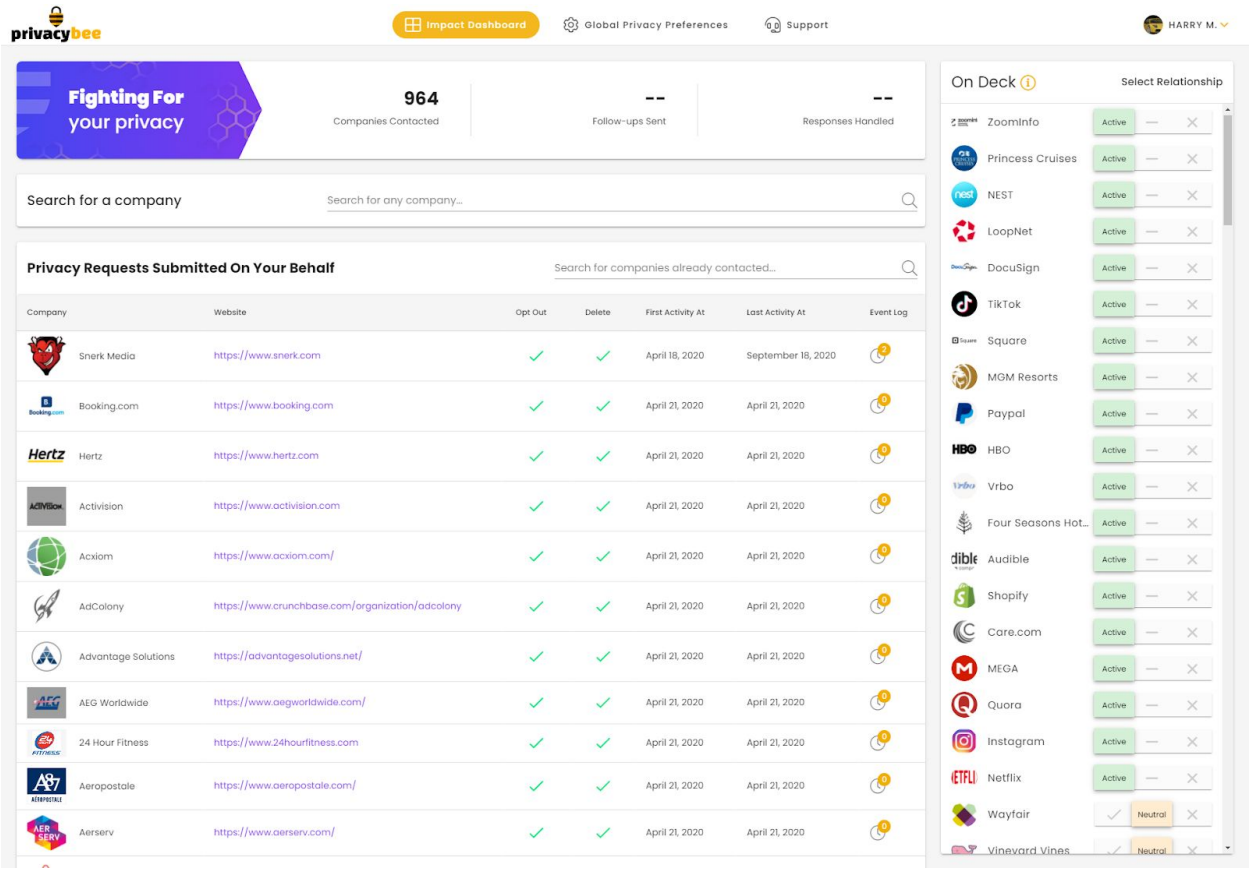
ABOUT PRIVACY BEE

Privacy Bee is a proactive privacy management service. We're your data protection co-pilot, scrubbing your personal information from corporate marketing databases so that it's less vulnerable to hackers. We accomplish this reaching out to corporations and make removal requests on your behalf. With each deletion, your personal data is no longer sitting on a bunch of servers waiting to be hacked!

Website: PrivacyBee.com

Twitter: @Privacy_Bee

Press Contact: Nick Vivion, nick@privacybee.com, +1 917 370-9447



The Privacy Bee data deletion request dashboard

DATA PROTECTION AND PRIVACY BACKGROUND

Companies' data privacy practices are often lacking and antiquated. The average time for companies to identify a breach in 2019 was 206 days, according to an IBM study. That same study found that 77% of security and IT professionals indicated they do not have a cybersecurity incident response plan applied consistently across the enterprise.

“The United States is one of the few developed countries in the world without a Data Protection Agency. The practical consequence is that U.S. consumers experience the highest levels of data breach, financial fraud, and identity theft in the world,” said Caitriona Fitzgerald, Policy Director and Chief Technology Officer of the Electronic Privacy Information Center, and Mary Stone Ross, Associate Director of the center in an op-ed published this year. “And U.S. businesses remain the target of cyber-attack by criminals and foreign adversaries, putting our identities and personal information at risk.”

With no national privacy law, and many companies exercising poor judgement and leaky cybersecurity practices, consumers’ personal information is left vulnerable to hackers across millions of databases and servers.

- By 2023, 65 percent of the world's population will have national privacy laws versus 10 percent today (Gartner)
- By 2025, the privacy management software market will exceed $3 billion a year (Market Study Report)
- 31% of data breach victims later have their identity stolen (8)
- 50% of user accounts are stale on average (1)
- 58% of companies found over 1,000 stale user accounts (1)
- Only 5% of a company’s folders are protected (1)
- 17% of all sensitive files were accessible to every employee (1)
- 86 percent of data breaches are for financial gain, an increase from 71 percent in 2019 (7) The average cost per lost or stolen record in a data breach is $150 (2)
- 38% of all users sampled have a password that never expires (1)
- The average time to identify a breach in 2019 was 206 days (2)
- The average time to contain a breach was 73 days (2)
- 71% of breaches are financially motivated (5)
- The global number of web attacks blocked per day increased by 56.1% between 2017 and 2018 (3)
- The global average cost of a data breach is $3.9 million (2)
- 77% of security and IT professionals indicated they do not have a cybersecurity incident response plan applied consistently across the

enterprise [2]

- 53% of companies found over 1,000 sensitive files accessible to every employee [1] 15% of companies found more than 1 million folders open to every employee [1] 43% of data breach victims are small businesses [5]
- Data breaches exposed 4.1 billion records in the first six months of 2019 [4]
- Over the past 10 years, there have been 300 data breaches involving the theft of 100,000 or more records [4]

Sources:

(1) 2019 Global Data Risk Report From The Varonis Data Lab
(2) IBM Security Cost of a Data Breach Report 2019
(3) Statista.com
(4) Forbes
(5) Verizon 2019 Data Breach Investigations Report
(6) New York Times
(7) Verizon Business 2020 Data Breach Investigations
(8) Experian Identity Theft Statistics