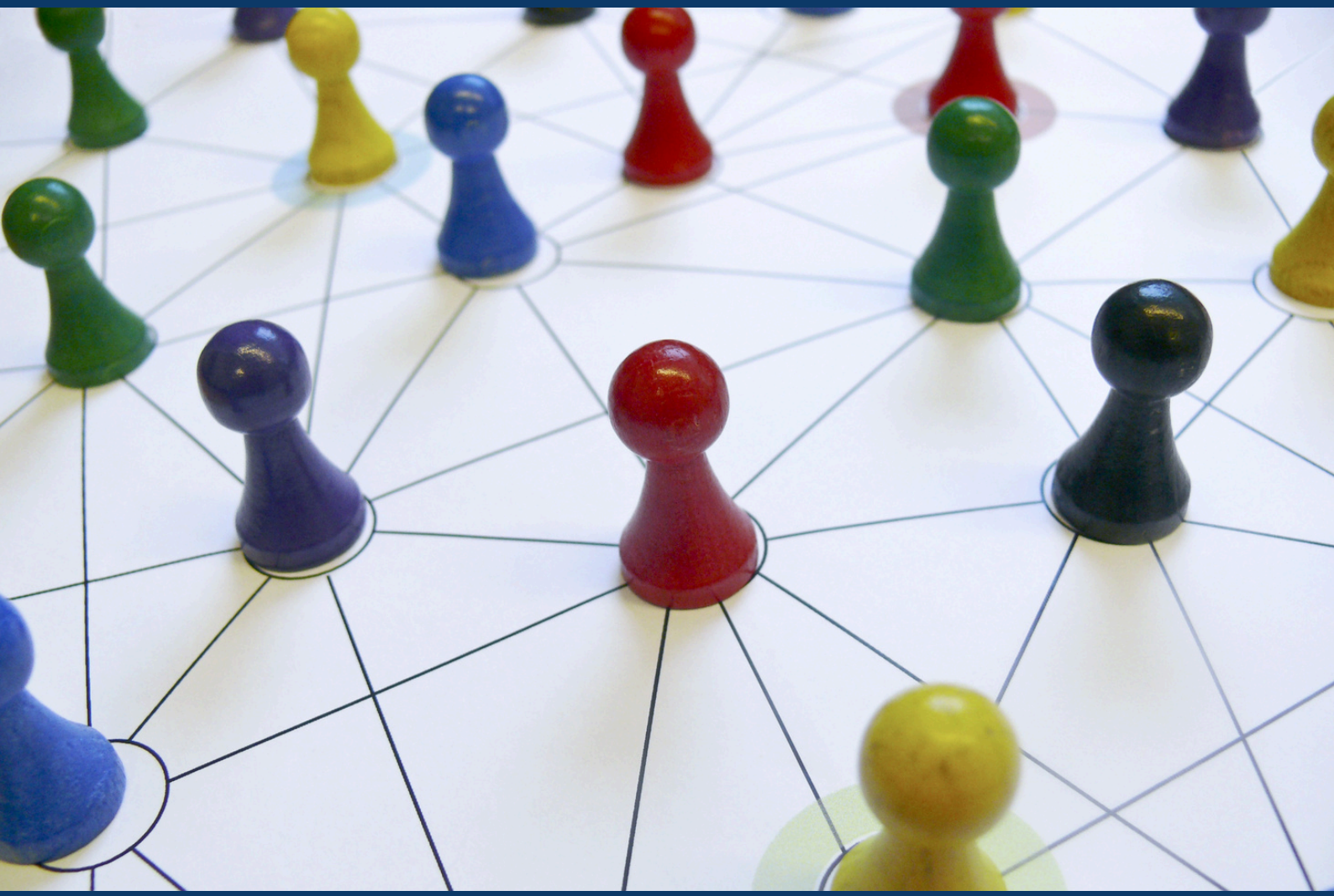
JEC JOINT ECONOMIC COMMITTEE

Opt-Out Obstacles:

Concerning Practices by Registered Data Brokers and the Multi-Billion-Dollar Cost of Breaches



Ranking Member Maggie Hassan | Minority Report

February 27, 2026

Opt-Out Obstacles: Concerning Practices by Registered Data Brokers and the Multi-Billion-Dollar Cost of Breaches

Executive Summary

In July 2025, Joint Economic Committee Ranking Member Maggie Hassan launched a major initiative to investigate financial scams and push for new ways to address this growing threat from both the public and private sectors. As one part of this effort, Ranking Member Hassan is examining how practices in the data broker industry can make Americans more vulnerable to scams. Data brokers – companies that typically collect and sell the personal information of individuals – often operate with little transparency. This lack of transparency makes it more difficult for individuals to secure their information online and, ultimately, protect themselves from the growing threat of scams. Data brokers, for example, can enable scams by making consumers' personal information available to bad actors, who can then use details like Social Security numbers, home addresses, or banking information to develop customized and convincing scams. In some cases, data brokers have allegedly sold this information directly to scammers; in others, cyber hacks of data brokers have exposed individuals' data to uncontrolled circulation online.[1]

In August 2025, Ranking Member Hassan issued investigative requests to several companies registered as data brokers: Comscore, Findem, IQVIA Digital (IQVIA), Telesign, and 6Sense Insights (6sense).[2] These requests followed a *WIRED* news report that these companies and others took steps to hide their opt-out pages – which allow individuals to request that their data be deleted or not sold – from search engine results.[3] In doing so, the companies made it more difficult for people to protect their information from scammers. To evaluate and address one facet of the role of data brokers in scams, Ranking Member Hassan pushed the companies to improve their data opt-out options and requested detailed information about these options.

Encouragingly, following Ranking Member Hassan's inquiries, most of the companies took action to improve individuals' access to opt-out options. This Joint Economic Committee – Minority report discusses findings from the investigation, including details on the companies' actions following the Ranking Member's requests, ongoing concerns regarding data broker practices, and the Committee's new calculation of the more than $20 billion cost to consumers from just four

recent data broker breaches. Conclusions from this report will continue to inform Ranking Member Hassan's ongoing investigations into scams.

Key Finding: Company Actions Following Ranking Member Hassan's Requests

Following Ranking Member Hassan's requests, Comscore, Telesign, 6sense, and IQVIA took actions to make their opt-out options more accessible to consumers and other parties. As discussed in detail in this report, these actions included removing "no index" code that had blocked opt-out pages from search engine results, adding opt-out links in more prominent locations, and publishing blog content explaining how people can exercise their privacy rights.

Notably, Findem did not respond to the Ranking Member's requests or written outreach from Committee staff and has not removed the "no index" code from its opt-out page – raising serious concerns about its responsiveness to opt-out requests and commitment to data privacy.

The Ranking Member also requested information from the five companies about their efforts, if any, to audit or assess the visibility of opt-out options or the success rates of opt-out requests (e.g., how often, how quickly, and why they are denied or granted). Only 6sense stated that it contracts with third-party auditors to conduct both of these assessments.

Key Finding: Estimated Cost of More than $20 Billion to U.S. Consumers from Recent Data Broker Breaches

Given the amount of personal information about consumers that data brokers hold, breaches of data broker companies can lead to massive amounts of personal data falling into the hands of scammers; this, in turn, results in major costs for American consumers. Through new calculations published for the first time in this report, the Joint Economic Committee – Minority estimates that identity theft stemming from just four large data broker breaches in recent years cost U.S. consumers more than $20 billion.

TERMS	DEFINITIONS
Data broker	Traditionally, companies that collect and sell individuals' information to third parties for purposes such as marketing, employment or tenant screening, and identity verification
Opt-out option	A common privacy choice that involves a mechanism (e.g., webform) for consumers and other parties to request that companies delete or not sell their personal information
"No index" code	Code placed on a webpage that instructs search engines not to show that page in search results
Dark patterns	Design choices (e.g., confusing user interfaces) that purposefully obscure privacy choices for consumers and other parties and make them difficult to access

Introduction

Data brokers are traditionally companies that sell personal information collected from commercial, government, and other public sources, typically without the knowledge of consumers or other parties.[4] For instance, data brokers can acquire this information when people visit websites, make purchases at particular businesses, interact on social media accounts, record workouts on health fitness apps, or donate to certain causes.[5] These and other typical online actions reveal information about people's interests and behaviors, from spending habits and dating preferences to health concerns and political leanings.[6] Some data brokers collect dates of birth, addresses, names, and even Social Security numbers.[7] Scammers can combine this sensitive information with personal insights to perform personalized and devastating scams.[8]

Whether through data brokers directly selling personal information to scammers or scammers obtaining this information through data breaches, bad actors can use information from data brokers to perpetrate identity theft and scams.[9] In one example, scammers reportedly used a woman's Social Security number – exposed by a data broker breach – to steal her identity.[10] The scammers proceeded to open fraudulent bank accounts, write bad checks, and introduce various inaccuracies to her credit report, including incorrect addresses and a designation as the criminals' "known associate."[11] The scammers' activities made it difficult for the woman to secure a mortgage and led the woman to experience stress-related fertility issues – events that she said stole "not only someone's credit card information, but [her] chance to be a mother."[12] In another example, ahead of the November 2025 elections, *Fox News* reported that scammers were targeting retirees by using personal information obtained from data brokers and public voter registration databases.[13] Information such as names, addresses, and contact information helped scammers craft fake polling updates, donation requests, and ballot-related phishing messages.[14]

As detailed in this report, it can be very difficult for individuals to protect themselves by getting their personal information removed from data brokers' databases. The Federal Trade Commission (FTC) has described "a fundamental lack of transparency" in the data broker industry, in part because of how data brokers present opt-out options (e.g., a webform) to consumers.[15] These options allow consumers and other parties to request that companies delete or not sell their data.[16] According to FTC, data broker opt-out options are "largely invisible and incomplete," making it difficult for consumers to understand or exercise them.[17]

State and Federal Oversight of Data Brokers

With varying success, the federal government and state governments have at times worked to strengthen oversight of the data broker industry. In 2019, the Government Accountability Office reported that FTC enforcement actions – including those brought under narrowly-tailored laws – reflect the absence of a "comprehensive federal privacy statute with specific internet privacy standards for the private sector" and stated that much of the data industry is outside consistent federal oversight.[18] The Consumer Financial Protection Bureau attempted to regulate data

brokers with a new rule under the Fair Credit Reporting Act that would have limited their ability to sell Americans' sensitive information, but the Trump Administration rescinded this rulemaking in May 2025.[19]

Nearly 20 states have enacted comprehensive data privacy laws.[20] These laws generally require companies to provide individuals with the right to access, delete, or opt-out of the sale of their data.[21] New Hampshire, for example, requires that businesses, including data brokers, provide "a clear and conspicuous link" to their opt-out options.[22] The New Hampshire law also states that these businesses cannot obtain consumer consent through "dark patterns" – user interfaces "designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice."[23] Recent legislation – in Texas, for example – also requires companies to establish multiple "secure and reliable methods" for consumers to exercise their privacy rights.[24]

Ranking Member Hassan's Investigation

In the absence of federal policy and with patchwork state laws, many data brokers have implemented practices limiting the ability of individuals to safeguard their personal data – which in turn, can expose them to scams.[25] In August 2025, *WIRED* reported that many data brokers were using a "no index" code – instructing search engines like Google to exclude a webpage from search results –– on webpages that provided opt-out options for consumers to request that the companies delete or not sell their data.[26] This code, *WIRED* noted, created a barrier for consumers seeking to exercise their data privacy rights.[27]

Ranking Member Hassan issued investigative requests to five companies registered as data brokers that the *WIRED* report had identified: Comscore, Findem, IQVIA Digital (IQVIA), Telesign, and 6Sense Insights (6sense).[28] Several of these companies described ways that their business models differ from the practices of traditional data brokers due to the information they collect or the services they provide.[29]

The requests from Ranking Member Hassan urged these companies to improve the accessibility of their opt-out options for individuals, explain how these options appeared on their websites, and clarify why certain opt-out or privacy pages did not appear in search results.[30] The Ranking Member also requested that the companies provide the results of any audits or assessments that they had conducted on the visibility of their opt-out options and the success rates of opt-out requests.[31] Following these requests, Comscore, IQVIA, Telesign, and 6sense took steps to improve opt-out options and submitted written responses in August and September 2025. IQVIA, Telesign, and 6sense then provided the Committee with additional information in January 2026.[32] Findem did not respond to the Ranking Member's initial request or repeated written follow-up from Committee staff, raising concerns about its responsiveness to opt-out requests and commitment to data privacy.

Data Brokers Have Enabled Fraud and Scams, Costing Americans Billions of Dollars

The information that data brokers typically collect and sell can enable scam activity. The Consumer Financial Protection Bureau has noted, for example, that the "data broker industry…is used to facilitate a range of financial scams" by giving scammers information they can use to target victims.[33] In addition, according to an FTC report, "storing data about consumers indefinitely may create security risks," in part because the data can attract bad actors and enable them to "predict passwords, answers to challenge questions, or other authentication credentials."[34] Despite these risks, companies have implemented "lax data security practices" that "may impose enormous financial and human costs," according to FTC.[35]

In some cases, data brokers have sold personal information directly to scammers. In 2021, for example, several data brokers agreed to pay nearly $200 million to resolve federal charges that they had knowingly sold data on vulnerable consumers, including elderly Americans, to scammers.[36] As noted in testimony to the House Committee on Energy and Commerce, bad actors often do not need to "hack many U.S. databases when so much data can be legally purchased from U.S. data brokers, which appear to do very little customer vetting."[37]

In other cases, scammers have taken advantage of preventable security failures. In 2017, for example, a data breach at Equifax – a large credit reporting agency that also serves as a data broker – exposed the personal information of 147 million people after hackers exploited a software vulnerability known to the company.[38] More recently, in 2023, data broker National Public Data experienced one of the largest data breaches in U.S. history, hitting an estimated 270 million Americans – or nearly 8 in every 10 Americans – and exposing sensitive data including Social Security numbers, dates of birth, names, and addresses.[39] The data broker recently faced a class action lawsuit alleging that it had failed to implement security measures like multi-factor authentication and data encryption that could have better protected this information.[40]

Data taken from breaches can easily be used for fraud and scams. A 2016 Javelin Research survey found that 31.7 percent of individuals who were notified that they were victims of a breach had experienced fraud the same year.[41] Following the Equifax breach, for instance, a Minnesota woman reported that criminals had opened fraudulent accounts and issued credit cards in her name. [42] The criminals then forged a fake Social Security card using the woman's stolen Social Security number and tricked a credit bureau into canceling a freeze that she had requested.[43] FTC continues to help people recover from identity theft associated with the Equifax breach.[44]

NEW: Committee Estimates U.S. Consumers Have Lost More than $20 Billion Stemming from Just Four Major Data Broker Breaches

The Joint Economic Committee (JEC) – Minority analyzed large data breaches that occurred within the last 10 years for which there is public information on the number of U.S. residents who were impacted in each breach. While other data brokers also faced breaches during this period, reports on those breaches did not specify the number of impacted consumers who were U.S. residents, and the Committee did not use these examples as part of its calculations. For instance, in 2019, People Data Labs experienced a breach that exposed records for 622 million individuals; however, reports did not specify how many of these victims were U.S. residents.[45] In contrast, the reporting on the four selected breaches provided the number of impacted U.S. residents.

Based on these parameters, the JEC – Minority analyzed these four major data breaches: the Equifax data breach that occurred in 2017, in which 147 million U.S. residents reportedly had data exposed;[46] the 2018 Exactis breach, in which 230 million U.S. residents reportedly had data exposed;[47] the 2023 National Public breach, in which about 270 million U.S. residents reportedly had data exposed;[48] and finally the 2025 TransUnion breach, in which 4.4 million U.S. residents reportedly had data exposed.[49]

The JEC – Minority then sought to estimate the total number of people who were likely to experience a financial loss because of identity theft following each breach, as well as the total financial loss from this theft. The Committee calculations posited that just over 30 percent of breach victims experienced identity theft in 2017, which we assume based on the Javelin Research finding above.[50] The Committee then applied a reduction factor to this share for a more conservative estimate based on experts' findings. To do so, the Committee imposed a 10 percent drop each year in the share of breach victims who experienced identity theft. To determine the number of identity theft victims who will experience financial loss, the Committee then applied the U.S. estimates from the U.S. Bureau of Justice Statistics regarding the proportion of people in the country who experience a financial loss because of identity theft (between 58 percent and 69 percent depending on the year).[51] To gauge a total estimated loss from each breach, staff then multiplied the reported number of U.S. residents impacted by each of the data breaches by the Bureau of Justice Statistics' median expected loss from identity theft of $200. [52]

Summing the final estimates across all four breaches, the JEC – Minority finds a total nominal loss of *$20.9 billion for U.S. consumers impacted by these four breaches alone*.

Notably, consumers with data exposed in a breach may try to recover losses through a class action lawsuit against the companies that experienced the breach. These cases make clear that the total financial losses that victims of identity theft experience are likely far greater than the median of $200 lost to identity theft, reported above. Following the 2017 Equifax breach, for example, the company agreed to pay up to $425 million to compensate affected consumers.[53]

The settlement provided claimants a maximum of $20,000 for damages, which can include unauthorized charges to an individual's account, additional expenses from freezing credit reports, fees paid to an attorney or professional accountant, and other fees.[54]

Following Ranking Member Hassan's Requests, Most Companies Took Action to Improve the Accessibility of Their Opt-Out Options

Most Companies Removed "No Index" Code and Took Other Actions that Made Their Opt-Out Options More Visible

Following Ranking Member Hassan's August 2025 requests, most companies took steps to improve opt-out options. Ranking Member Hassan welcomes these efforts and encourages sustained commitments from the companies. A summary of these actions appears below.

Company "No Index" Codes and Impact on Privacy Controls

Company	"No Index" Code	Intentional[55]	Impacted Page	Code Status Following Hassan Request
Comscore	Yes	No	"Data Subject Rights" links to opt-out form	Removed
Telesign	Yes	No	"Privacy Request" contains opt-out form	Removed
6sense	Yes	Yes	"Privacy Policy" links to opt-out form[56]	Removed
IQVIA	Yes	Yes	"Your Privacy Choices" contains opt-out form	Removed[57]
Findem[58]	Yes	Unknown	"Do not sell or share my personal information" contains opt-out form	Not Removed

Upon receiving the Ranking Member's letter, Comscore conducted a review of its website for "no index" code. [59] In its response to the Committee, Comscore confirmed that its "Data Subject Rights" page previously contained "no index" code.[60] Among other uses, this page provides links to separate forms through which a consumer can submit opt-out requests.[61] Comscore attributed the origin of the "no index" code to an earlier version of the page that the company created in 2003.[62] The company could not determine why former personnel had placed the code on this page, although it suggested that the code was not intended to prevent consumer access

to opt-out options.[63] The company reported to the Committee that it has removed the "no index" code from the "Data Subject Rights" page and additional privacy pages identified in the website review.[64]

Telesign also removed the "no index" code and improved access to its opt-out options.[65] To begin, Telesign confirmed that the opt-out request form – as hosted on its "Privacy Request" page – did not appear in search results at the time of the *WIRED* report.[66] According to the company, it uses a third-party search engine optimization tool that restricts the search engine visibility of its pages by default.[67] Telesign, however, stated that it was unaware of this setting until the publication of the *WIRED* report, after which the company immediately enabled search engine visibility on relevant pages.[68] Encouragingly, following Ranking Member Hassan's requests, Telesign also added a link to the "Privacy Request" page to its website footer, making it accessible on each page of the company's website.[69]

Of note, though, Telesign stated to the Committee that its opt-out options had always been "readily available and transparent," but this assertion is questionable.[70] The company argued, for example, that consumers have previously been able to find the opt-out option on a third-party website maintained by Telesign's vendor (OneTrust), that the third-party website was titled "Telesign Privacy Rights Form," and that it appeared in search results.[71] In this case, however, consumers would need to look beyond Telesign's official website and rely on an opt-out form on a third-party website. Telesign also cited multiple links on its website to the opt-out form, including in its Privacy Notice, Job Applicant Privacy Notice, Data Privacy Framework Notice, and Cookie Notice.[72] Committee staff found, however, that many of these links were located on pages where consumers might not expect to find privacy options or privacy notice pages with more than 9,000 words.[73]

6sense, by contrast, disputed the *WIRED* report and stated that its "Privacy Center" page – where people can exercise their opt-out rights – was indexed and available in search results at the time of publication.[74] The company acknowledged, however, that its "Privacy Policy" page, which contains a link to the opt-out form, had previously contained "no index" code and that it removed this code following the *WIRED* report.[75] 6sense told the Committee that the code had been intended to limit spam that the company receives.[76] Following Ranking Member Hassan's requests, the company also published a blog to its website to provide "helpful, relevant content about exercising opt-out rights."[77]

IQVIA informed the Committee that in September 2025, the company replaced its previous "Your Privacy Choices" opt-out page with a new page hosted by an outside vendor, OneTrust, pursuant to a contract between IQVIA and OneTrust in June 2025.[78] IQVIA stated that it did not provide instructions to OneTrust regarding the indexing of the page, but the company did, however, confirm that – unlike the earlier version – the new page does not include "no index" code.[79] In an earlier response to the Committee, IQVIA had stated that it had no current plans to remove the "no index" code from the earlier version of the opt-out page, in part because it said

that the code improved the opt-out process for parties and the company, including by minimizing spam.[80] The company also contended that the previous page had appeared in Google search results and that *WIRED* was incorrect in assuming that no index code would hide the page.[81] The example the company provided to support this point, however, appeared to resemble text that would appear in a Google Search AI Overview and not traditional search results.[82]

Separately, IQVIA also stated that individuals "may opt-out through various forums," including a Google search AI Overview.[83] Committee staff found that this feature generally provides links to relevant content in response to user queries, but its outputs can vary over time and are not guaranteed to include specific pages.[84] For example, a Committee staff Google search of "IQVIA privacy opt-out form" produced an AI Overview output different from the apparent example cited in the company's response and did not provide a direct link to the earlier version of IQVIA's "Your Privacy Choices" opt-out page at the time it was live.[85]

Findem Continues to Restrict Opt-Out Option Accessibility and Failed to Respond to Oversight

Findem did not respond to the Ranking Member's request. The company's failure to respond to the Committee's oversight raises serious, broad questions about its responsiveness to opt-out requests and commitment to data privacy. Importantly, Findem has not removed the "no index" code from its "Do not sell or share my personal information" opt-out page, which is still not visible in search results.[86] Findem's mandatory disclosures in 2024 also show that the company did not process 80 percent of privacy requests from consumers and other parties due to "insufficient data."[87] This result, alongside Findem's lack of response to the Committee's investigation and ongoing use of "no index" code, raises serious concerns.

Only 6sense Stated that it Audits Both the Visibility and Success Rates Associated with Opt-Out Options

In response to Ranking Member Hassan's requests, four companies submitted information about how they manage their privacy practices. Encouragingly, 6sense referenced formal audits or assessments of the visibility and success rates associated with its opt-out options. Specifically, the company informed the Committee that, before *WIRED*'s reporting, the company had contracted with a privacy compliance firm to audit its compliance with the California Consumer Privacy Act and had received results in December 2025.[88] According to 6sense, this audit reviewed "controls covering the visibility of opt-out options" on the company's website and validated its compliance with opt-out obligations and other requirements under the California law.[89] Records of the audit indicate that this review involved verifying that 6sense's website footer contained a link to the opt-out page, for example.[90] 6sense also stated that the company conducts annual internal reviews of privacy controls, including pages with information on privacy practices and opt-out methods.[91]

In addition, 6sense provided examples of audits and assessments regarding the success rates of opt-out requests. The company, for example, stated that third-party data security auditors provide independent evaluation of its handling of opt-out requests, including through requesting documentation of successful requests for a randomly selected sample of individuals.[92] As part of this process, the company produces "evidence to the auditors providing justification for any [privacy] requests reported as being denied" (or unsuccessful).[93] 6sense informed the Committee that aggregate information on its website shows that "well below 1% of [California-related deletion] requests received by 6sense are denied or otherwise unsuccessful."[94]

Most companies, however, stated that they do not conduct audits or assessments evaluating the visibility of their opt-out options and/or the success rates of opt-out requests. Relatedly, Comscore and Telesign acknowledged that they only discovered the "no index" code on their pages following the *WIRED* reporting.[95]

Comscore stated that the company has "complied with all data subject requests received within timelines prescribed by law."[96] At the same time, Comscore acknowledged that it "does not conduct formal audits or assessments" of the kind described above.[97] Similarly, IQVIA stated that the company "monitors its systems and processes" but "does not conduct the types of audits or other assessments referenced" in the Ranking Member's requests.[98] IQVIA did, however, provide information on its efforts to support the choices of health care professionals regarding their data preferences, including for individuals who do not want to be contacted for promotional services by pharmaceutical sales or receive related materials by mail.[99] Telesign likewise noted that it "has not historically audited whether its privacy request page is visible" in search results.[100] The company also did not indicate that the company or third parties have conducted audits of the success of opt-out rates.[101] Telesign did, however, state that its privacy team individually processes each opt-out request.[102] According to the company, Telesign had "processed" all opt-out requests in 2025 as of August 26, 2025.[103]

Conclusion

Following Ranking Member Hassan's requests, most companies took action to make their opt-out and other privacy pages more visible for individuals, including by removing "no index" code, adding opt-out links in more prominent locations, and publishing blog content that explains how consumers can exercise their privacy rights. Ranking Member Hassan welcomes these actions as supporting greater protection for consumers against scams and other harms.

Notably, Findem failed to engage with the Committee's oversight entirely, and mandatory disclosures from the company in 2024 show that it did not process 80 percent of privacy requests from individuals. Also of concern is the fact that most of the companies that responded to the Ranking Member's requests stated that they do not conduct audits evaluating the visibility

and/or success rates associated with their opt-out options. Only 6sense provided information on assessments or audits related to both metrics.

The Committee's findings underscore the need for clear, easy access to opt-out options and more rigorous oversight within the data broker industry. Especially given the Committee's calculation that U.S. residents have lost more than $20 billion in recent data breaches, additional action is needed to protect Americans from scams connected to data brokers. At a minimum, opt-out options should be easy to locate and use. Data brokers could also improve privacy outcomes by auditing the success rates of opt-out requests, including how frequently they are approved or denied and why. As the volume of information that data brokers collect on individuals continues to grow – and as U.S. losses to scams escalate – data brokers, the Administration, and Congress can all play a key role in addressing scam risks stemming from data broker practices.

---

[1] House Committee on Energy and Commerce, Testimony Submitted for the Record of Justin Sherman, Senior Fellow and Research Lead, Data Brokerage Project, Duke University Sanford School of Public Policy, *Hearing on Who Is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy*, 118th Cong. (Apr. 19, 2023) (www.congress.gov/118/meeting/house/115788/witnesses/HMTG-118-IF02-Bio-ShermanJ-20230419.pdf) (H. Hrg. 118-26).

[2] As explained in more detail below, several of these companies describe their business models as distinct from the practices of traditional data brokers due to the information that they collect or the services that they provide.

[3] *Data Brokers Are Hiding Their Opt-Out Pages from Google Search*, WIRED (Aug. 12, 2025) (www.wired.com/story/data-brokers-hiding-opt-out-pages-google-search). Committee staff selected these five companies, in part, because they reportedly had not responded to requests for comment from *WIRED*.

[4] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014) (www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf).

[5] Consumer Financial Protection Bureau, *Protecting Americans from Harmful Data Broker Practices* (Dec. 13, 2024) (3170-AB27) (www.federalregister.gov/documents/2024/12/13/2024-28690/protecting-americans-from-harmful-data-broker-practices-regulation-v); Consumer Reports, *Your Exercise Bike Knows a Lot About You—and It Doesn't Keep Every Secret* (Jan. 21, 2025) (www.consumerreports.org/health/health-privacy/exercise-machine-privacy-a3907557984/); Open Secrets, *The Third-Party Brokers Who Make Millions Selling Your Data to Political Groups* (Apr.

21, 2022) (www.opensecrets.org/news/2022/04/the-third-party-brokers-who-make-millions-selling-your-data-to-political-groups/).

[6] Consumer Financial Protection Bureau, *Fact Sheet: The CFPB's Proposed Rule to Rein in Sprawling Data Broker Industry* (Dec. 2024) (files.consumerfinance.gov/f/documents/cfpb_fcra-nprm-fact-sheet_2024-12.pdf).

[7] *Id.*

[8] *Id.*

[9] *Id.*; *My Wallet Was Stolen at a Bar. Then My Identity Theft Nightmare Began*, Los Angeles Times (Oct. 26, 2022) (www.latimes.com/business/technology/story/2022-10-26/identity-theft-nightmare).

[10] *My Wallet Was Stolen at a Bar. Then My Identity Theft Nightmare Began*, Los Angeles Times (Oct. 26, 2022) (www.latimes.com/business/technology/story/2022-10-26/identity-theft-nightmare).

[11] *Id.*

[12] *Id.*

[13] *Scammers Target Retirees with Election Tricks and Fake Polling Updates Ahead of Nov 4 Vote*, Fox News (Oct. 22, 2025) (www.foxnews.com/tech/scammers-target-retirees-election-tricks-fake-polling-updates-ahead-nov-4-vote).

[14] *Id.*

[15] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014) (www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf).

[16] *Data Brokers Are Hiding Their Opt-Out Pages from Google Search*, WIRED (Aug. 12, 2025) (www.wired.com/story/data-brokers-hiding-opt-out-pages-google-search/).

[17] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014) (www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf).

[18] Government Accountability Office, Testimony Before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, Statement of Alicia Puente Cackley, Director Financial Markets and Community Investment, *Consumer Privacy: Changes to Legal Framework Needed to Address Gaps* (GAO-19-621T) (June 11, 2019) (www.gao.gov/assets/gao-19-621t.pdf).

[19] *Top US Consumer Watchdog Has a Plan to Fight Predatory Data Brokers*, WIRED (Dec. 3, 2024) (www.wired.com/story/cfpb-fcra-data-broker-oversight/); *CFPB Quietly Kills Rule to Shield Americans from Data Brokers*, WIRED (May 15, 2025) (www.wired.com/story/cfpb-quietly-kills-rule-to-shield-americans-from-data-brokers/).

[20] International Association of Privacy Professionals, *US State Privacy Legislation Tracker: Comprehensive Consumer Privacy Bills* (Nov. 24, 2025) (iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf).

[21] *Id.*

[22] N.H. Rev. Stat. Ann. § 507-H (2024).

[23] *Id.*

[24] Tex. Bus. & Com. Code Ann. § 541.055 (West 2024).

[25] *Data Brokers Are Hiding Their Opt-Out Pages from Google Search*, WIRED (Aug. 12, 2025) (www.wired.com/story/data-brokers-hiding-opt-out-pages-google-search/); Consumer Financial Protection Bureau, *Fact Sheet: The CFPB's Proposed Rule to Rein in Sprawling Data Broker Industry* (Dec. 2024) (files.consumerfinance.gov/f/documents/cfpb_fcra-nprm-fact-sheet_2024-12.pdf).

[26] *Id.*

[27] *Id.*

[28] *E.g.*, Letter from Ranking Member Hassan to Comscore (Aug. 13, 2025). Committee staff selected these five companies, in part, because they reportedly had not responded to requests for comment from *WIRED*.

[29] The companies are registered in the California Privacy Protection Agency Data Broker Registry under the Delete Act. *See* Delete Act, 2023 Cal. Stat. ch. 709 (S.B. 362). Regarding their business models, Comscore told the Committee that it "focuses on online audience measurement" for "leading American companies, news organizations, and government agencies." Letter from Comscore to Ranking Member Hassan (Sept. 3, 2025). In connection with this work, the company collects data on the online behavior of individuals who participate in research panels, as well as data from third-party sources. Comscore, Privacy Policy (www.comscore.com/About/Privacy-Policy) (accessed Jan. 29, 2026). IQVIA stated that its subsidiary IQVIA Digital "is only a data broker relating to healthcare professionals and not for other types of 'consumers.'" Email from IQVIA to JEC Staff (Jan. 27, 2026). Telesign stated that it "does not 'sell' personal information like traditional data brokers" but instead delivers certain information on potential customers to merchants to help them protect their businesses from fraud. Email from Telesign to JEC Staff (Jan. 30, 2026). 6sense stated that its "customers are businesses interested in selling to other businesses" and that the "B2B contact information" the company provides "is the same as would be found on a standard business card." Letter from 6Sense Insights to Ranking Member Hassan (Sept. 2, 2025). According to its website, Findem "aggregates data from 100,000+ websites" and "ingests millions of human data points" to build profiles for job candidates that give recruiters and organizations the "ability to find and manage talent." Findem, What Are Findem's Core Features? (findem.zendesk.com/hc/en-us/articles/22822918401303-What-are-Findem-s-core-features) (accessed Jan. 29, 2026).

[30] *E.g.*, Letter from Ranking Member Hassan to Comscore (Aug. 13, 2025).

[31] *Id.*

[32] Letter from Comscore to Ranking Member Hassan (Sept. 3, 2025); Letter from IQVIA to Ranking Member Hassan (Sept. 5, 2025); Letter from Proximus Global to Ranking Member Hassan (Aug. 26, 2025) (responding on behalf of Telesign); Letter from 6Sense Insights to Ranking Member Hassan (Sept. 2, 2025); Email from IQVIA to JEC Staff (Jan. 27, 2026); Email from IQVIA to JEC Staff (Jan. 28, 2026); Letter from Telesign to JEC Staff (Jan. 28, 2026); Letter from 6Sense Insights to JEC Staff (Jan. 29, 2026).

[33] Consumer Financial Protection Bureau, *Protecting Americans from Harmful Data Broker Practices* (Dec. 13, 2024) (3170-AB27). (www.federalregister.gov/documents/2024/12/13/2024-28690/protecting-americans-from-harmful-data-broker-practices-regulation-v).

[34] Federal Trade Commission, *Data Brokers: A Call for Transparency and Accountability* (May 2014) (www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf).

[35] Federal Trade Commission, *Trade Regulation Rule on Commercial Surveillance and Data Security* (3084-AB69) (www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security).

[36] U.S. Department of Justice: *Justice Department Recognizes World Elder Abuse Awareness Day; Files Cases Against Marketing Company and Executives Who Knowingly Facilitated Elder Fraud* (June 15, 2021);

[37] House Committee on Energy and Commerce, Testimony Submitted for the Record of Justin Sherman, Senior Fellow and Research Lead, Data Brokerage Project, Duke University Sanford School of Public Policy, *Hearing on Who Is Selling Your Data: A Critical Examination of the Role of Data Brokers in the Digital Economy*, 118th Cong. (Apr. 19, 2023) (www.congress.gov/118/meeting/house/115788/witnesses/HMTG-118-IF02-Bio-ShermanJ-20230419.pdf) (H. Hrg. 118-26).

[38] Final Order and Judgment, *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, No. 1:17-md-2800-TWT (N.D. Ga. Jan. 13, 2020); Government Accountability Office, *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach* (GAO-18-559) (Aug. 2018) (www.gao.gov/assets/gao-18-559.pdf).

[39] *Huge Data Breach Involving Social Security Numbers Could Impact Millions of Americans*, News 5 Cleveland (Sept. 9, 2024) (www.news5cleveland.com/news/local-news/huge-data-breach-involving-social-security-numbers-could-impact-millions-of-americans).

[40] Class Action Complaint, *Hofman v. Jerico Pictures, Inc. d/b/a National Public Data*, No. 0:24-cv-61383 (S.D Fla. Aug 1, 2024).

[41] Misty Vasquez, *The Financial Crimes Management of Account Takeover Fraud*, University of Texas (2017) (repositories.lib.utexas.edu/server/api/core/bitstreams/05cec0bf-59b1-4368-a51b-2225e95dd527/content).

[42] *KARE 11 Investigations: Identity Theft Nightmare*, KARE 11 (Oct. 1, 2019) (www.kare11.com/article/news/investigations/kare-11-investigates-identity-theft-nightmare/89-36b012c8-d201-49ac-8a8e-4bca83403579).

[43] *Id.*

[44] Federal Trade Commission, *Equifax Data Breach* Settlement (Nov. 2024) (www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement).

[45] *People Data Labs Data Breach: What & How It Happened?*, Twingate (blog) (June 28, 2024) (www.twingate.com/blog/tips/People%20Data%20Labs-data-breach).

[46] Final Order and Judgment, *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, No. 1:17-md-2800-TWT (N.D. Ga. Jan. 13, 2020).

[47] *Florida Class Action Claims Exactis Breach Affects 230 Million Americans*, Law.com (June 29, 2018) (www.law.com/dailybusinessreview/2018/06/29/florida-class-action-claims-exactis-breach-affects-230-million-americans/?slreturn=20260113161903).

[48] *Huge Data Breach Involving Social Security Numbers Could Impact Millions of Americans*, ABC News 5 Cleveland (Sept. 9, 2024) (www.news5cleveland.com/news/local-news/huge-data-breach-involving-social-security-numbers-could-impact-millions-of-americans).

[49] *TransUnion Data Breach Impacts More than 4.4 Million Americans – Here's How to Spot Identity Theft*, CNBC Select (Nov. 26, 2025) (www.cnbc.com/select/transunion-data-breach-impacts-over-4-million/).

[50] Misty Vasquez, *The Financial Crimes Management of Account Takeover Fraud*, University of Texas (2017) (repositories.lib.utexas.edu/server/api/core/bitstreams/05cec0bf-59b1-4368-a51b-2225e95dd527/content).

[51] See, e.g., U.S. Bureau of Justice Statistics, Victims of Identity Theft, 2021 (NCJ 306474) (Oct. 2023).

[52] *Id.*

[53] Federal Trade Commission, *Equifax Data Breach* Settlement (Nov. 2024) (www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement).

[54] Nebraska Attorney General, *Equifax Data Breach Settlement FAQs* (July 24, 2019) (ago.nebraska.gov/sites/default/files/doc/7-24-19%20Equifax%20FAQs%20-%20Post%20Approval.pdf).

[55] All respondents that intentionally placed the code stated that it was intended, in part, to minimize spam that the companies receive. Letter from 6Sense Insights to Ranking Member Hassan (Sept. 2, 2025); Letter from IQVIA to Ranking Member Hassan (Sept. 5, 2025).

[56] As noted below, 6sense stated to the Committee that the company's "opt-out form is contained in its Privacy Center, and the Privacy Center was indexed before any reporting was published or outreach by the Committee." Letter from 6Sense Insights to JEC Staff (Jan. 29, 2026).

The company acknowledged, however, that its "Privacy Policy" page, which contains a link to the opt-out form, had previously contained "no index" code and that it removed this code following the *WIRED* report. Letter from 6Sense Insights to Ranking Member Hassan (Sept. 2, 2025).

[57] IQVIA informed the Committee that a previous version of the "Your Privacy Choices" page included "no index" code. According to IQVIA, the company replaced this version of the page in September 2025 with a page hosted by an outside vendor, OneTrust, pursuant to a contract between IQVIA and OneTrust in June 2025. IQVIA stated that it did not provide OneTrust with instructions about the indexing of the page but did confirm that the page did not include "no index" code. Email from IQVIA to JEC Staff (Jan. 27, 2026); Email from IQVIA to JEC Staff (Jan. 28, 2026).

[58] Committee staff reviewed Findem's opt-out page and found that it still contained "no index" code. Screenshot on file with Committee.

[59] Letter from Comscore to Ranking Member Hassan (Sept. 3, 2025).

[60] *Id.*

[61] Comscore, Data Subject Rights (www.comscore.com/About/Privacy/Data-Subject-Rights) (accessed Nov. 5, 2025).

[62] Letter from Comscore to Ranking Member Hassan (Sept. 3, 2025).

[63] *Id.*

[64] *Id.*

[65] Letter from Proximus Global, to Ranking Member Hassan (Aug. 26, 2025) (responding on behalf of Telesign).

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *Id.*

[71] *Id.*; Letter from Telesign to JEC Staff (Jan. 28, 2026).

[72] Letter from Proximus Global to Ranking Member Hassan (Aug. 26, 2025) (responding on behalf of Telesign).

[73] *Id.*; See, e.g., Telesign, Privacy Notice (www.telesign.com/privacy-notice) (accessed Jan. 13, 2026); Telesign, Login - TelePortal (teleportal-la6.telesign.com/auth/login/) (accessed Jan. 13, 2026).

[74] Letter from 6Sense Insights to Ranking Member Hassan (Sept. 2, 2025).

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] Email from IQVIA to JEC Staff (Jan. 28, 2026).

[79] *Id.*; Email from IQVIA to JEC Staff (Jan. 27, 2026).

[80] Letter from IQVIA to Ranking Member Hassan (Sept. 5, 2025).

[81] Email from IQVIA to JEC Staff (Jan. 27, 2026)

[82] Letter from IQVIA to Ranking Member Hassan (Sept. 5, 2025).

[83] *Id.*; Email from IQVIA to JEC Staff (Jan. 28, 2026).

[84] Screenshot of Google AI overviews from staff searches of "IQVIA opt-out" on file with Committee.

[85] Screenshot of Google AI overview from a staff search of "IQVIA privacy opt-out form" on file with Committee.

[86] Screenshot of Findem's "Do not sell or share my personal information" opt-out page with "no index" code on file with Committee; Screenshot of staff Google search of "Findem opt-out" that did not provide a search result to the opt-out page on file with Committee.

[87] Findem, Platform Privacy Policy (www.findem.ai/privacy-policy-platform) (accessed Nov. 5, 2025).

[88] Letter from 6Sense Insights to JEC Staff (Jan. 29, 2026).

[89] *Id.*

[90] *Id.*

[91] *Id.*

[92] *Id.*

[93] Letter from 6Sense Insights to Ranking Member Hassan (Sept. 2, 2025); Letter from 6Sense Insights to JEC Staff (Jan. 29, 2026).

[94] Letter from 6Sense Insights to JEC Staff (Jan. 29, 2026).

[95] Letter from Comscore to Ranking Member Hassan (Sept. 3, 2025); Letter from Proximus Global to Ranking Member Hassan (Aug. 26, 2025) (responding on behalf of Telesign).

[96] Letter from Comscore to Ranking Member Hassan (Sept. 3, 2025).

[97] *Id.*

[98] Letter from IQVIA to Ranking Member Hassan (Sept. 5, 2025).

[99] *Id.*

[100] Letter from Proximus Global to Ranking Member Hassan (Aug. 26, 2025) (responding on behalf of Telesign).

[101] Email from Telesign to JEC Staff (Jan. 5, 2026).

[102] *Id.*

[103] Letter from Proximus Global to Ranking Member Hassan (Aug. 26, 2025) (responding on behalf of Telesign).