Negotiating privacy:

Bipartisan agreement on US privacy rights in the 117th Congress

By IAPP Senior Westin Research Fellow Müge Fazlioglu, CIPP/E, CIPP/US

WHITEPAPER

CONTENTS

Negotiating privacy:

Bipartisan agreement on US privacy rights in the 117th Congress

By IAPP Senior Westin Research Fellow Müge Fazlioglu, CIPP/E, CIPP/US

EXECUTIVE SUMMARY

For many years, the subject of U.S. privacy legislation has been one of interest for boards, companies, law and policymakers, industry groups, privacy advocates, academics, and many other stakeholders. Numerous proposals and drafts of federal legislation have circulated and as many events, symposia and hearings on Capitol Hill have been held. Yet, despite efforts over multiple sessions, members of Congress have still not reached legislative agreement on what privacy rights should be enshrined at the federal level.

Research scope

This white paper examines the progress made in Congress toward bipartisan agreement on privacy rights over the current legislative session, analyzing the 18 bipartisan federal privacy bills (see Appendix) introduced in the 117th Congress.

As a complement to the IAPP "U.S. Federal Privacy Legislation Tracker," which includes privacy-related bills within the current Congress, the focus in this analysis is limited to bills that have received support from both Democrats and Republicans. The aim is to understand why certain pieces of privacy legislation have broader support among lawmakers and how they differ from proposals that have received support from only one party.

The analysis divides the proposed legislation into several groups:

1. Those that focus on collection, use and sale of consumer data.
2. Those that relate to health (including COVID-19 and "vaccine passports"), financial or educational/children's data.
3. Those that concern the Federal Trade Commission and its privacy enforcement mandate and authority.
4. Those that impose obligations or restrictions upon the collection and/or use of data by government entities or law enforcement agencies.

> ***Most privacy bills with bipartisan support focus on only a single privacy right or issue.***

Key findings

The results of this analysis reveal that all but one of the consumer privacy bills with bipartisan support focus on just a single privacy right or issue. These include data portability as per the Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021, dark patterns as per the Deceptive Experiences To Online Users Reduction Act and the right to delete as per the Data Elimination and Limiting Extensive Tracking and Exchange Act.

None of the omnibus or comprehensive consumer privacy bills have received bipartisan support. These bills contain provisions on multiple privacy rights or obligations — to access, correction, deletion, data security, privacy officers, etc. — and include bills such as the Consumer Data Privacy and Security Act of 2021, the SAFE DATA Act, the Consumer Online Privacy Rights Act, the Information Transparency & Personal Data Control Act and the Online Privacy Act of 2021.

TAKEN TOGETHER, THESE FINDINGS INDICATE:

- Congress has had the most success in forging consensus around narrow privacy rights and issues.
- As privacy-related bills are expanded to encompass multiple individual rights and more business obligations, they are less likely to draw support from the other side of the political aisle.
- Ultimately, multiple and significant partisan gaps still remain over the shape and scope of a "comprehensive" federal consumer privacy law.
- None of the federal privacy bills that contain either a private right of action or a state law preemption provision have received bipartisan support.

WHY BIPARTISANSHIP MATTERS

Bipartisanship is not rooted in idealism or feel-good notions. It is the essential, if hidden, core of the negotiations that enables Congress to get things done.

Bipartisanship has been the keystone of the work done in Congress to enact new laws, and is one of the strongest predictors of future success for proposed legislation. For instance, a study of laws enacted by Congress between 1973 and 2016 found the passage of most, including landmark enactments, was defined by "substantial bipartisan support." Despite, or perhaps in spite of, increasing ideological polarization in Congress, majority parties have rarely been able to advance their legislative agenda without support from the minority party. Indeed, passage of laws in line with the majority party's priorities usually requires support from a substantial portion of the minority party in either the House or the Senate or endorsement from the minority party leadership.

Other studies have shown how bipartisanship waxes and wanes over time, different ways to measure it, and the factors that influence it. Although bipartisan coalitions are costly to build, bipartisanship plays a pivotal role in U.S. politics across foreign and domestic policy domains and will likely be an important factor in the enactment of privacy rights at the federal level.

> ***Bipartisanship plays a pivotal role in U.S. politics across foreign and domestic policy domains and will likely be an important factor in the enactment of privacy rights at the federal level.***

Turning to the specific pieces of privacy-related legislation in Congress that count both Democrats and Republicans among their sponsors and cosponsors, the following sections examine bills by the type of data or entity that they regulate. Starting with bills related to consumer data, the analysis also covers bills concerning health (including COVID-19 and "vaccine passport"), financial, and children's data, the FTC, and restrictions and obligations on governmental entities.

CONSUMER PRIVACY

This first and largest group of privacy-related bills introduced in Congress concern consumer privacy rights. In general, these bills enact privacy rights for consumers or impose obligations on businesses with respect to the collection, processing and handling of consumers' personal data. Several of these bills have been reintroduced from a previous session of Congress. While some are nearly identical to their predecessors, others have been revised significantly. In addition, many of these bills are entirely new.

As of the date of this writing, 16 federal privacy bills deal strictly with protections for consumer data. Of these, six have secured bipartisan support. Within each chamber, the bipartisan consumer data privacy bills with the greatest number of cosponsors are:

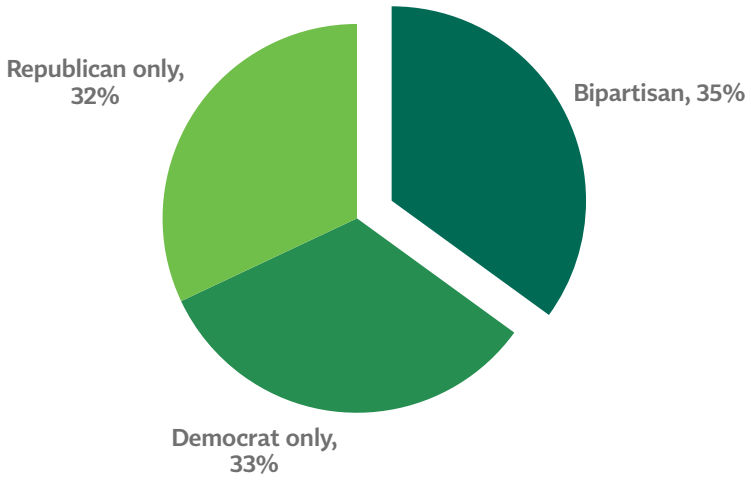
- ACCESS Act of 2021 (28 cosponsors in the House of Representatives).
- Filter Bubble Transparency Act (eight cosponsors in the Senate).

The remaining consumer data privacy bills with bipartisan support have only secured between one and three cosponsors.

ACCESS Act of 2021

The Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021 grants U.S. consumers and businesses a right to data portability. Specifically, the bill requires large online platforms to "facilitate consumers and businesses switching from one platform to another." The bill is not only underpinned by the principle of data portability, but also of interoperability, and establishes some requirements around data minimization. The bill grants the FTC and the Department of Justice the authority to decide which platforms would be subject to these

PRIVACY BILL SPONSORSHIP BY PARTY



requirements and would also require a platform to petition the FTC before changing its interoperability interface. The FTC would also be required to establish a technical committee to assist platforms with the law's implementation and be granted the authority to recover civil penalties and provide injunctive relief.

During the mark-up of the bill, House Judiciary Committee Chairman Jerrold Nadler, D-N.Y., called it an "important bipartisan measure" that "strikes the right balance to encourage competition, give consumers more choices, and protect user privacy."

> ***16 federal privacy bills deal strictly with protections for consumer data. Of these, six have secured bipartisan support.***

Filter Bubble Transparency Act

The Filter Bubble Transparency Act, introduced in both the House and Senate, requires that certain platforms notify users if their personal data is used to select the content they see using an "opaque algorithm." Platforms must also provide users with a version of their service that uses an "input-transparent" algorithm and allows them to see unmanipulated content. The bill has elicited support from both sides of the political aisle, but, notably, for different reasons. For Democrats, the problems the bill addresses not only relate to privacy, but also concern the addictiveness of content personalized by algorithms, as well as its potential to promote extremism via platform models that seek to maximize user engagement. Meanwhile, for Republicans, the bill takes aim at a perceived lack of transparency around speech and censorship-related decisions by large platforms.

Social Media Privacy Protection and Consumer Rights Act of 2021

This bill grants users of social media and other online platforms several rights related to transparency, consent and access. Its first main provision stipulates that online platforms provide users the option to essentially opt out of data collection, and platforms may "deny certain services or completely deny access to the user" if the user's opting out "creates inoperability in the online platform."

Second, disclosures to users under the transparency obligations of the bill must be made in a form that is "easily accessible," "of reasonable length" and use language that is "clear, concise, and well organized, and follows other best practices appropriate to the subject and intended audience."

Third, covered entities must also establish a privacy or security program and publish a description that details how the entity uses personal data, addresses privacy risks, and provides access to employees and contractors to the personal data of users.

In addition, the bill imposes certain disclosure and consent requirements on entities that introduce new products that would override a user's privacy preferences or make changes to their privacy or security program. Lastly, users are entitled to a copy of the personal data that the operator processes, free of charge and in an accessible format.

DETOUR Act

The Deceptive Experiences to Online Users Reduction Act, introduced in both the Senate and House, prohibits large online operators from manipulating or misleading consumers

into providing personal information or giving consent. It also aims to promote consumer welfare with respect to the behavioral research conducted by such entities. In particular, the bill prohibits the following practices:

1. The design, modification or manipulation of a user interface "with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or user data."
2. The subdivision or segmenting of online consumers into groups for the purposes of a behavioral or psychological experiment, except when their informed consent is obtained.
3. The design, modification or manipulation of a user interface that is directed at a child "with the purpose or substantial effect of causing, increasing, or encouraging compulsive usage."

The conduct prohibited in (3) specifically includes video-play functions that are initiated "without the consent of a user."

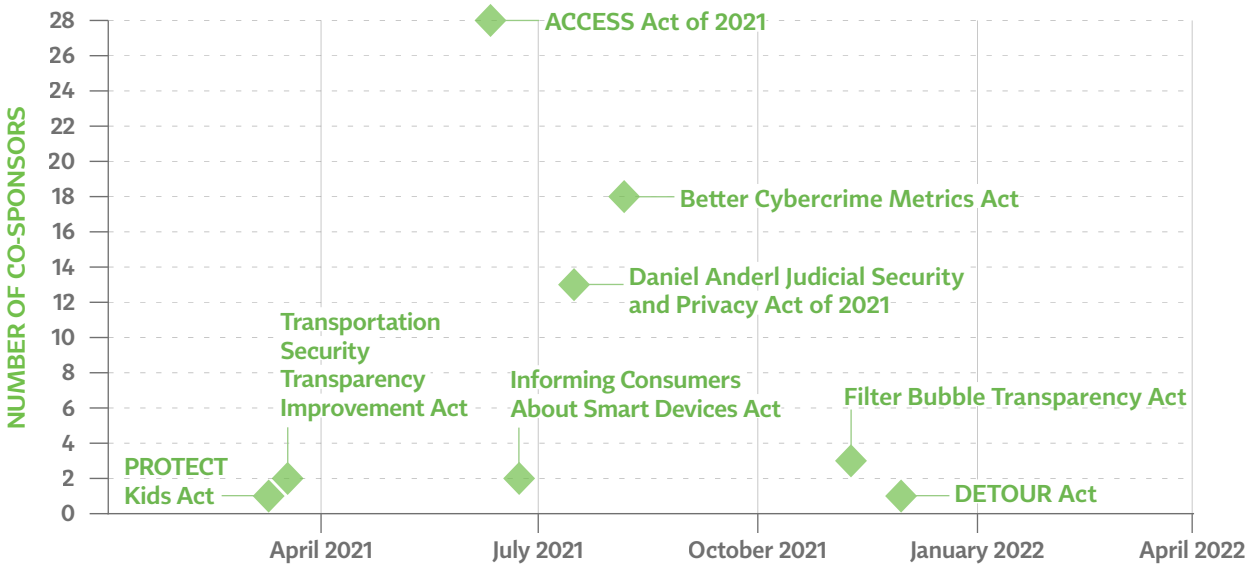
DELETE Act

While versions of the Data Elimination and Limiting Extensive Tracking and Exchange Act have been introduced in both the House and the Senate, only the Senate version of the bill has received bipartisan support.

In the broadest sense, this bill establishes a centralized system allowing individuals to request deletion of their personal data "simultaneously" across data brokers. It has been described as both "pro-consumer and pro-competition."

The first provision of the bill requires data brokers to annually register with the FTC, similar to S.2290, and provide certain information, such as their methods for allowing users to opt out of their collection of use of personal data; limitations on their data collection, use or sale; and a list of the types of information they collect and the sources from which they collect that information. This data broker registration information would be made publicly available and provided in

ALL BIPARTISAN PRIVACY BILLS IN THE HOUSE OF REPRESENTATIVES



a downloadable format by the FTC, barring certain exceptions.

The main provision of the bill creates a centralized data deletion system. Essentially, this system would allow "an individual, through a single submission, to request that every data broker who is registered…[to] delete any personal information related to such individual." The bill places an emphasis on the creation of a centralized system that would allow individuals to make "a single deletion request" through a website operated by the FTC that would automatically delete an individual's data across registered data brokers.

Moreover, the DELETE Act would establish a "Do Not Track" list, which would include individuals who submit a deletion request through the centralized system, from which registered data brokers "may not collect or retain more personal information than is necessary to identify an individual" who is included on the list.

Informing Consumers about Smart Devices Act

Outside of definitions and details on how it would be enforced by the FTC, the only substantial provision of this bill is a single sentence imposing transparency requirements on the makers of smart devices: "Each manufacturer of a covered device shall disclose whether the covered device manufactured by the manufacturer contains a camera or microphone as a component of the covered device." Importantly, the bill excludes mobile phones, laptops or other devices consumers would reasonably expect to include a camera or microphone.

HEALTH, FINANCIAL AND CHILDREN'S PRIVACY

Nine privacy-related bills introduced in the 117th Congress involve the regulation of health information, genetic information, consumer software, devices and applications that collect, process and store health information, COVID-19 emergency health data or the use of "vaccine passports." Of these nine bills, three of them have bipartisan support.

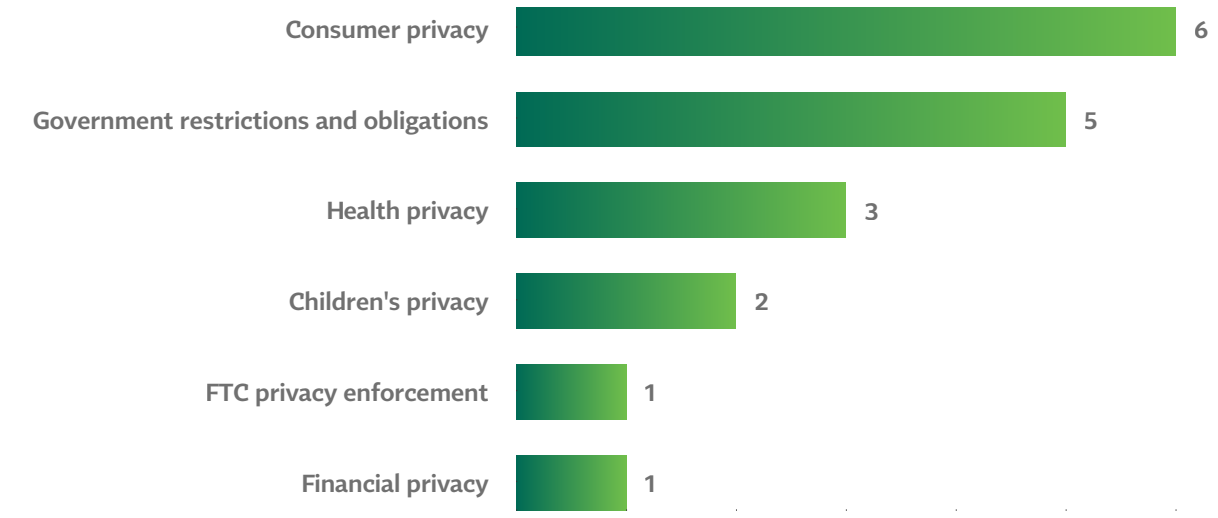
Five privacy bills related strictly to financial data have been introduced, and only one has secured bipartisan sponsorship, with the remaining four supported only by Republicans.

Meanwhile, within the domain of educational and children's privacy, two of the five bills introduced in the 117th Congress have received support from a member of both parties.

Protecting Personal Health Data Act

With the goal of alleviating a gap left by the Health Insurance Portability and Accountability Act, the Protecting Personal Health Data Act requires promulgation of regulations by the Department of Health and Human Services "to help strengthen privacy and security protections for consumers' personal health data that is collected, processed, analyzed, or used by consumer devices, services, applications, and software." This would be done by the Secretary of Health and Human Services in consultation with HHS's National Coordinator for Health Information Technology, the FTC and other relevant stakeholders and federal agency heads as deemed appropriate. This group would also be charged with establishing a National Task Force on Health Data Protection to study various issues of relevance to the bill,

BIPARTISAN PRIVACY BILLS BY FOCUS



including deidentification methodologies, encryption standards and transfer protocols, and cybersecurity risks with respect to and privacy concerns related to consumer and employee health data.

The Protecting Personal Health Data Act is rooted in a report issued in July 2016 by HHS entitled, "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA." The report notes the proliferation of "wearable fitness trackers, social media sites where individuals share health information through specific social networks, and other technologies" that enable the sharing and collection of health data, little to none of which Congress had envisioned when it enacted HIPAA in 1996.

SMARTWATCH Data Act

The Stop Marketing and Revealing the Wearables and Trackers Consumer Health Data Act prohibits the transfer, sale, sharing or provision of access to consumer health information or "other individually identifiable consumer health information" that is collected from a "personal consumer device."

The bill is limited in the scope of application, however, only entities that would provide such information to another entity whose "primary business function … is collecting or analyzing consumer information for profit" or if the purpose of such a transfer, sale, sharing or provision of access is "to otherwise add value to the entity" collecting the consumer health information.

The bill also contains numerous exceptions. One is for consumer health information that is "aggregated or anonymized," to which the prohibition would not apply. The other primary exceptions to the prohibitions include consent, or in cases where the information is being provided to a health plan, health care clearinghouse, health care provider, government organization or agency to comply with other applicable laws, or to academic, medical, research institutions or other nonprofit organizations acting in the public interest. Entities may also transfer such consumer health information to an entity's "affiliates or other trusted businesses or persons" if the information is part of its "external processing procedures" and is based on "compliance with privacy protections and other appropriate confidentiality and security measures."

Additional rules and exceptions would apply to transfers of such consumer health information to foreign entities, and the requirements of the law would be enforced by the Secretary of Health and Human Services.

Health Data Use and Privacy Commission Act

This bill establishes the Commission for the Comprehensive Study of Health Data Use and Privacy Protection to study issues relating to protection of individual privacy and the appropriate balance to be achieved between protecting individual privacy and allowing and advancing appropriate uses of personal health information.

While not establishing new rules for privacy per se, through its establishment of a commission to study health data and privacy issues, the law focuses on the same kinds of issues addressed by S.24 and S.500.

The duties of the commission would include studying the monitoring, collection and distribution of personal health information

by different levels of government, currently existing relevant statutes and regulations, as well as legislation pending before Congress and state legislatures, private-sector recommendations, frameworks and proposals, and self-regulatory efforts undertaken or proposed by the private sector to respond to privacy issues.

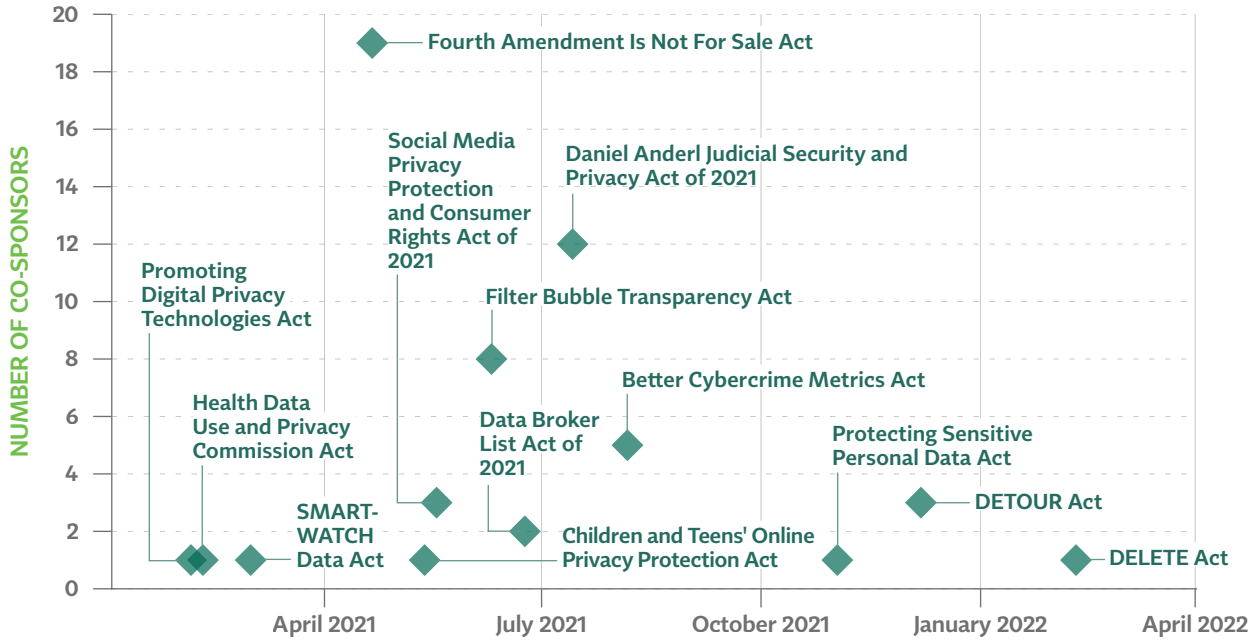
The commission is also charged with examining differences between U.S. and international rules for protecting the privacy of health information, the need for consistency in deidentification standards for health data, technologies used for treatment, payment and health care operations, and employer practices and policies regarding employee health information privacy.

Additional tasks for the committee include "an examination of efficacy, recommendations, and advantages and disadvantages of different enforcement mechanisms," including private rights of action and spanning the enforcement of privacy laws and rules by the FTC, HHS Office for Civil Rights, Civil Rights Division of the Department of Justice, and state agencies and attorney generals.

Lastly, the commission would examine the issues of consent and providing consumers notices of privacy practices, including "whether such practices are effective in informing consumers of their rights and responsibilities," as well as statutory and regulatory employee training requirements, including an assessment of best practices.

The commission would be composed of 17 members appointed by the comptroller general, which are to reflect the views of "health providers, ancillary health care workers, health care purchasers, health plans, health technology developers, researchers, consumers, public health experts, civil liberties experts, genomics experts, educators, the consumer electronics industry, and relevant (federal) agencies."

ALL BIPARTISAN PRIVACY BILLS IN THE SENATE



COVID-19 and 'vaccine passport' bills

Although none of the bills related to COVID-19 data or "vaccine passport" have secured bipartisan support, they are included here as important counterexamples of privacy-related bills that have received support from only one political party. The absence of bipartisanship in this particular privacy domain is, perhaps, more of an indicator of the political division around the pandemic rather than around privacy per se.

Within this category, the focus of bills has also shifted as the pandemic has worn on. The bills introduced early in 2021, sponsored by Democrats alone, concerned COVID-19 emergency health data and technology for contact tracing. The Public Health Emergency Privacy Act restricts use and disclosure of COVID-19 emergency health data, including by websites and mobile apps, while the Secure Data and Privacy for Contact Tracing Act of 2021 creates grants for state, tribal and territorial public health agencies to develop technology for contact tracing in COVID-19 that meet privacy, security and other standards.

Other bills introduced in mid- to late 2021, sponsored only by Republicans, dealt with the issue of "vaccine passports" and employer-mandated vaccine requirements. The No Vaccine Passports Act, No Vaccine Passports for Americans Act, and Passport Act each prohibit federal agencies from issuing "vaccine passports" or passes to certify COVID-19 vaccination status or from publishing or sharing COVID-19 records or "similar health information" of U.S. citizens, or prohibit the use of federal funds to support a system requiring citizens to provide documentation of their vaccination status "in order to travel, attend an event, or conduct other activities."

The latest such bill to be introduced, the Employee Privacy Act, amends the Fair Labor Standards Act to prohibit employers from inquiring about the vaccination status of their employees or prospective employees.

> ***Five privacy bills related strictly to financial data have been introduced, and only one has secured bipartisan sponsorship, with the remaining four supported only by Republicans.***

Protecting Sensitive Personal Data Act

The Protecting Sensitive Personal Data Act is a narrow bill that requires declarations be made for foreign investments in U.S. businesses that maintain "sensitive personal information" by expanding the Department of the Treasury's Committee on Foreign Investment's oversight regarding such declarations. A statement accompanying release of the bill singled out concern for "harmful actors in China and elsewhere" as one of the reasons that strengthened oversight authority for CFIUS was needed.

Children and Teens' Online Privacy Protection Act

This bill amends the Children's Online Privacy Protection Act of 1998 by extending privacy protections to children aged 12 to 16, including the provision of notice and consent, that were previously only applicable to children 12 and under, as well as establishing greater online privacy protection in general for children and minors.

Specifically, the bill prohibits operators of websites, online services or apps, and mobile apps directed at children from collecting their personal information without providing notice and obtaining consent. Covered entities must also provide parents and minors with certain information upon request, such as a description of the specific types of personal information it has collected from the child, as well as provide "the opportunity at any time to delete personal information collected from the child." Furthermore, they may not condition access to their games, services, websites, or applications on the provision of personal information above what "is reasonably required to participate." Lastly, they must "establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children and minors."

> ***Within the domain of educational and children's privacy, two of the five bills introduced in the 117th Congress have received support from a member of both parties.***

The bill contains several other notable provisions. These include a prohibition on targeted marketing directed at children or minors without their consent, the right to challenge the accuracy of and erase or correct inaccurate personal information, and an obligation for covered entities to make users aware of mechanisms for the erasure or elimination of personal information. In addition, the bill requires internet-connected devices targeted to children and minors to meet certain cybersecurity standards and requires manufacturers to display an "easy-to-understand privacy dashboard," that details whether, what and how personal information of a child or minor is collected, transmitted, retained, used and protected by the manufacturer.

PROTECT Kids Act

The Preventing Real Online Threats Endangering Children Today Kids Act also amends COPPA, expanding its scope by raising the age for parental consent from children under 13 to under 16, adding precise geolocation and biometric information to the list of protected personal information, and extending protections to include services provided through mobile apps. The bill also requires covered entities, which include operators of websites, online services and mobile apps, to delete a child's personal information upon the verified request of a parent. Covered entities may also not terminate services to children whose parents refuse to permit further collection or use of that child's information. Lastly, the bill contains a provision that requires the FTC to conduct a study on "on the appropriateness of the existing actual knowledge standard," found in section 1303(a)(1) of COPPA, which prevents operators from collecting personal information without when it has "actual knowledge" that it is collecting such information from a child, as well as "what effects changing such standard will have on children's online privacy."

FTC PRIVACY AUTHORITY AND ENFORCEMENT

Several bills introduced deal directly with the enforcement powers, budget, staff and structure of the FTC. What sets these bills apart from others is that their main provisions impose a new requirement upon or direct the FTC to carry out some specific task or internal reorganization with respect to consumer privacy. Of the six bills in this category, only one has garnered bipartisan support, with the rest being supported only by Democrats.

Data Broker List Act of 2021

The only bipartisan bill related to the FTC's authority and enforcement powers is the Data Broker List Act of 2021. Although the primary purpose of the bill is to impose requirements on data brokers regarding collection and use of personal information, it also contains a provision that would require these data brokers to register annually with the FTC (similar to the DELETE Act).

The remaining five bills that centrally deal with the FTC's scope of privacy enforcement and authority are sponsored or cosponsored only by Democrats. The most impactful of these perhaps is the Data Protection Act of 2021, which would restructure the FTC by first establishing a new independent federal data protection agency to regulate the processing and use of personal data. The bill would then transfer the functions of the FTC "under a federal privacy law to prescribe rules, issue guidelines, or conduct a study or issue a report mandated under such law" to the new agency at a certain "transfer date." It would also give the new agency power to enforce rules prescribed under the FTC Act "with respect to the collection, disclosure, processing and misuse of personal data," although it would not modify, limit or otherwise affect the authority of the FTC with respect to large data collectors other than the previously defined transfer of rulemaking activities under a federal privacy law.

GOVERNMENT RESTRICTIONS AND OBLIGATIONS

The final group of bipartisan bills included in this study impose some limitation or obligation on government entities. These range from bills that mandate grants to support privacy-enhancing technologies, limit the types of data law enforcement and intelligence agencies can collect, focus on the use of "sensitive security information" in the aviation industry, improve the government classification and collection of data regarding cybercrime, to one that protects the privacy and safety of federal judges and their families.

Promoting Digital Privacy Technologies Act

One of the narrowest privacy-related bills in scope, the bill directs the National Science Foundation to support research grants for PETs. While the House version has only secured Democratic sponsors, the Senate version of this bill has attracted sponsors from both parties.

Fourth Amendment is Not for Sale Act

Similar to the previously mentioned bill, only the Senate version of the Fourth Amendment is Not for Sale Act has received bipartisan support. Sponsored by Sen. Ron Wyden, D-Ore., this bill prevents law enforcement and intelligence agencies from "obtaining subscriber or customer records in exchange for anything of value." In the Senate, it was referred to the Judiciary Committee. The Senate version of this bill has also drawn the greatest number of co-sponsors of Senate privacy-related bills, with 19 co-sponsors. The House version is available here.

Daniel Anderl Judicial Security and Privacy Act of 2021

With its origins set in a tragedy, this bill introduced in the Senate and House aims to "improve the safety and security of the (federal) judiciary." Daniel Anderl was the 20-year-old son of District Court Judge Esther Salas. He died from a gunshot wound inflicted by an assailant who came to the family's home and authorities believed was targeting Judge Salas. In line with Salas' call for more privacy for federal judges in the aftermath of her son's death, lawmakers in the House and Senate introduced the Daniel Anderl Judicial Security and Privacy Act of 2021.

Noting that threats against federal judges increased nearly fivefold between 2015 and 2019, the bill prohibits government agencies from publicly posting or displaying certain covered information, which includes but is not limited to a federal judge's home address, telephone number, email address, name or address of a school or daycare attended by an immediate family member, or name and address of an employer of an immediate family member. The bill also prohibits data

brokers from selling, licensing, trading or purchasing such covered information of federal judges and their immediate family members. Furthermore, the bill contains provisions that provide grants to states and local governments to prevent such disclosures, as well as security training and education for federal judges and their immediate family, including "best practices for using social media and other forms of online engagement and for maintaining online privacy." Lastly, the bill enables the establishment and administration of a vulnerability management program in the judicial branch.

Better Cybercrime Metrics Act

This bill, signed into law by President Joe Biden on May 5, 2022, contains several provisions that would improve classification and collection of data regarding cybercrime. First, it authorizes the National Academy of Sciences to develop a taxonomy to categorize different types of "cybercrime and cyber-enabled crime" and report its findings to Congress. Second, it requires the attorney general to establish a category in the National Incident-Based Report System for cybercrime and cyber-related crime based on the taxonomy. Third, the bill requires coordination between the directors of the Bureau of Justice Statistics and Bureau of the Census to include questions related to cybercrime victimization in the National Crime Victimization Survey.

Transportation Security Transparency Improvement Act

This bill addresses policies of the Transportation Security Administration related to the definition of "Sensitive Security Information." The goal of the legislation is to bring greater understanding and clarity to how TSA designates SSI, improve its training of personnel regarding SSI and increase its outreach to external stakeholders who come into contact with SSI.

CONCLUSION

The primary purpose of this analysis was to identify areas of overlap between Democrats and Republicans in terms of the types of legislation at the federal level related to privacy that they support. It can help point the way forward for a better way of thinking about the lawmaking process, particularly around privacy issues.

This analysis provides a starting point for individuals, organizations and groups who want to advocate for change in the nation's federal privacy laws. These efforts should begin by examining bipartisan bills in detail. Even limiting the discussion to bipartisan bills, however, leaves significant room for discussion since the proposals are so wide-ranging. From data deletion, data portability and interoperability to freedom from dark patterns, deception and algorithmic manipulation, lawmakers in Congress have shown bipartisan support for a substantial number of privacy rights. These bills, if passed, would have noticeable impacts on the digital economy and serve as a much-needed step on the way to filling in the gaps in protections for consumer privacy at the federal level.

From data deletion, data portability and interoperability to freedom from dark patterns, deception and algorithmic manipulation, lawmakers in Congress have shown bipartisan support for a substantial number of privacy rights.

Furthermore, this study revealed an important finding about the two most contentious issues in the federal privacy law debate: preemption and private right of action. Namely, none of the bills that contain either provision have received bipartisan support. In line with suggestions that weaker versions or "gradations" of these concepts would be politically feasible, an analysis of existing sectoral federal privacy laws has demonstrated that Congress has already taken "a wide range of paths...with respect to preemption in previous privacy laws." Yet, until a version of preemption or private right of action emerge that can secure bipartisan support, it is unlikely that bills that include either provision in their current forms have a realistic chance of passing.

This analysis has identified the privacy-related federal bills that have the greatest chances of success in that they are supported by both Democrats and Republicans. Bipartisan support should be used to identify proposals that have the most realistic chances of passing. In this way, the focus on bipartisanship is a rational exercise in pragmatism. Certainly, many valuable partisan proposals for privacy legislation exist, but they will produce nothing more than wishful thinking if they cannot secure at least some degree of support from the other party. Although the analysis does not ultimately assume that only bills with bipartisan support may ultimately pass, it elevates bipartisanship, which has long been neglected in the federal privacy debate, to its rightful place in this discussion given its importance in the law and policymaking process.

APPENDIX

Table 1. Privacy-related federal bills with bipartisan support, from most cosponsors to least

BILL TITLE	NUMBER	CO-SPONSORS
Augmenting Compatibility and Competition by Enabling Service Switching Act of 2021	H.R.3849	28
Fourth Amendment is Not for Sale Act	S.1265	19
Better Cybercrime Metrics Act	H.R.4977; S.2629	House: 18 Senate: 5
Daniel Anderl Judicial Security and Privacy Act of 2021	H.R.4436; S.2340	House: 13 Senate: 12
Filter Bubble Transparency Act	S.2024; H.R.5921	Senate: 8 House: 3
Deceptive Experiences to Online Users Reduction Act	S.3330; H.R.6083	Senate: 3 House: 1
Social Media Privacy Protection and Consumer Rights Act of 2021	S.1667	3
Protecting Personal Health Data Act	S.24	2
Data Broker List Act of 2021	S.2290	2
Transportation Security Transparency Improvement Act	H.R.1871	2
Informing Consumers about Smart Devices Act	H.R.3898; H.R.4081	1; 1
Data Elimination and Limiting Extensive Tracking and Exchange Act	S.3627	1
Stop Marketing and Revealing the Wearables and Trackers Consumer Health Data Act	S.500	1
Health Data Use and Privacy Commission Act	S.3620	1
Protecting Sensitive Personal Data Act	S.3130	1
Children and Teens' Online Privacy Protection Act	S.1628	1
Preventing Real Online Threats Endangering Children Today Kids Act	H.R.1781	1
Promoting Digital Privacy Technologies Act	S.224	1

CONTACT

Mark Thompson
Director of Research and Insights, IAPP
mthompson@iapp.org

Müge Fazlioglu
Senior Westin Research Fellow, IAPP
muge@iapp.org

IAPP Research and Insight
research@iapp.org

Follow IAPP on Social Media

Published May 31, 2022.

The IAPP disclaims all warranties, expressed or implied, with respect to the contents of this presentation, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.
© 2022 International Association of Privacy Professionals. All rights reserved.