i2Coalition US Tech Policy Handbook 2022

The US Tech Policy Handbook was created for the i2Coalition's 10th anniversary Washington, D.C., fly-in in June 2022. It includes a comprehensive briefing on our discussion areas and positions, along with extensive background on the following issues:

#1: INTERMEDIARY LIABILITY - DMCA SEC. 512 & TECHNICAL MEASURES

#2: INTERMEDIARY LIABILITY - SECTION 230 & CONTENT MODERATION

#3 FEDERAL CONSUMER DATA PRIVACY & SECURITY

#4: DNS - WHOIS PRIVACY

#5: TRADE: US-EU TRANSATLANTIC DATA PRIVACY FRAMEWORK

#6: INTERNET GOVERNANCE

#7: FBI INFORMAL DISCUSSION & I2C SPECIAL LAW ENFORCEMENT PROJECT

#8: BROADBAND AND HIGH-SPEED INTERNET ACCESS

The US Tech Policy Handbook is organized into two sections: **I. Key Messages on Policy Issues**, and **II. Background on Policy Issues**. The "Key Messages" section covers each issue briefly, and we'd like you to read it and think about how those points impact your businesses. The "Background" section is optional reading and provides more detail for those who would like to take a deeper dive.

I. KEY MESSAGES ON POLICY ISSUES

#1: INTERMEDIARY LIABILITY - DMCA SEC. 512 & TECHNICAL MEASURES

- **The DMCA's Vital Role in Growing the Digital Economy.** The Digital Millennium Copyright Act (DMCA), enacted in 1998, is one of the cornerstones of the multi-trillion dollar digital economy. Its safe harbor provisions have allowed i2Coalition members to build the essential, globally-architected technology infrastructure that makes the Internet work, free from crippling litigation threats. The careful balance Congress struck in the DMCA has also benefited content creators who have found numerous new distribution paths and revenue streams.

- **The DMCA Has Supported Technology Diversity & Evolution.** A chief strength of the DMCA and its safe harbors has been its ability to accommodate new technologies far beyond what Congress envisioned in 1998. Congress wanted these provisions to be forward-looking and adaptable to new technologies. Courts have followed Congress' intent by finding that a broad array of online service providers (OSPs) are protected by the safe harbors. The DMCA's framework has stimulated investment and growth in the Internet. The diversity of our i2Coalition membership is a great example of that success.

- **The Existing DMCA Framework Still Benefits the Entire Internet Ecosystem.** The DMCA framework continues to serve the entire Internet ecosystem well and should largely be left intact with little to no modification. We do not believe that it is necessary to amend Section 512(i) regarding standard technical measures (STMs) or to require the Copyright Office to conduct an STM rulemaking. A balanced framework for collaborative efforts and voluntary standards development already exists.
    - Section 512(i) was included in the DMCA to encourage open and voluntary standards-setting, not technical mandates.
    - Targeting "sub-industries" for technical measures is ill-advised and inconsistent with Section 512's language and principles. The Copyright Office should not propose any changes, including legislation, that turn the DMCA's voluntary standards-setting process into one leading to technical mandates.

- **Abuse Mitigation is a Key Tool.** Copyright abuse differs from some other kinds of abuse online, where "you know it when you see it." It is far more nuanced and complex. Because of the ecosystem's diversity, efforts come through individual risk assessment and mitigation.
    - There is no centralized database of copyrighted material one can check upon. Even if one existed, there is no surefire way to determine that the user doesn't have a valid license for that copyrighted material or that it is not fair use. It has been one of the most challenging problems to address proactively, which is why quick, effective reactive mitigation has always served as a primary focus of OSP attention.
    - More often than not, the biggest impediment to efficient resolution of copyright infringement abuse queries is a lack of standardization in abuse reporting, which results in insufficient information being conveyed to take action. A significant portion of abuse complaints that reach help desks are inactionable. Education needs to be directed toward rightsholders on how to file thorough, complete, valid, and actionable complaints.

#2: INTERMEDIARY LIABILITY - SECTION 230 & CONTENT MODERATION

- **Understanding the Scope of Section 230.** Section 230 of the Communications Decency Act is a cornerstone of Internet intermediary liability law. It does not just apply to "Big Tech" social media platforms and was written well before those platforms even existed. By its express statutory terms, Section 230 provides liability protections to Internet businesses of all sizes as well as non-profit organizations, including libraries, schools, colleges, and universities, and even individuals when they host and moderate user-generated content.
    - Unlike the "Big Tech" social media platforms, multitudes of organizations of our kind existed when Section 230 was written and enacted into law in 1996. The underlying reasons for applying Section 230 liability protections to Internet infrastructure providers in 1996 are even more critical today.
    - Section 230 is essential to the companies that operate the infrastructure on which speakers depend. While social media platforms dominate the headlines, everything online depends on the Internet's infrastructure, including the services provided by Internet infrastructure providers, from hosting companies, data centers, domain registrars, and registries, to cloud infrastructure providers, managed services providers, and related services.
    - Internet infrastructure providers play a critical role in promoting open and robust Internet speech by not only providing the infrastructure on which much of the Internet depends but also by providing services that minimize barriers to entry for anyone with a message, no matter their viewpoint. Internet infrastructure providers also drive economic growth by providing small businesses with greater reach and flexibility to innovate.
- **Dangers of Overbroad Section 230 Reform Legislation.** As the current (117th) Congress continued a vigorous, charged debate about reforming Section 230, with numerous bills introduced, the i2Coalition became increasingly alarmed that Congress could pass uninformed, blanket legislation inflicting significant, damaging economic and societal impacts on the online operations of all our diverse coalition membership.
    - Legitimate issues about political bias, disinformation, and misinformation carried through the largest social media platforms have a significant place in this national conversation. But Congressional debates must take care not to drown out other vital concerns about economic disruption and litigation risks that proposed Section 230 revisions raise for the multitudes of other entities that are expressly covered by and rely on its liability protections.
    - Congress must ask whether revising Section 230 is the soundest approach to addressing a specific policy matter that may involve only a handful of large commercial players. Uninformed and overbroad changes to Section 230 present a host of dangers to the entire Internet ecosystem, including but not limited to higher operating costs, legal uncertainty, litigation risks, reduced innovation, and slower economic growth and recovery.
    - The U.S. economy has continued to struggle in the recovery from the current pandemic. Small businesses of all kinds, non-profit organizations, libraries, schools, and institutions of higher learning cannot withstand the additional economic uncertainty and burdens caused by well-intentioned but ill-advised changes to Section 230.

#3: FEDERAL CONSUMER DATA PRIVACY & SECURITY

- **Support for a Comprehensive, National Legislative Approach.** Privacy is an increasingly important consumer expectation online. If companies value the trust and safety of their users, they need to meet those growing expectations. The i2Coalition works closely with policymakers to

educate about and maximize understanding of the business and user impacts of privacy and data collection legislation and regulation affecting the technology sector in the U.S. and globally. A comprehensive, national approach establishing a baseline of federal consumer data privacy and security can be a foundation for consumer trust. To that end, the i2Coalition appreciates the recently renewed efforts in Congress toward achieving that goal in federal legislation, and recognizes the value of uniformity in this space to avoid a patchwork of state laws.

- **The Role of Strong Encryption**. The i2Coalition believes enhanced privacy policies go hand in hand with the ability to deploy strong encryption, unencumbered by backdoors, to ensure security. We combine and leverage privacy and encryption tools to keep people safe online.

#4: DNS - WHOIS PRIVACY

- **Balancing Global Privacy and Data Access.** The i2Coalition has been closely engaged with ICANN, NTIA, and other stakeholders on the development of a sound, workable global access model for domain name registration data that meets the requirements of the GDPR, federal and state laws, and the needs of law enforcement agencies.
    - Holders of registration data (referred to as “contracted parties,” a reference to the contracts that registries and registrars have with ICANN) engage with law enforcement agencies (including the FBI, FTC, FDA, and Europol) to facilitate lawful access to domain name registration information for legitimate purposes, as defined in the GDPR.
    - Law enforcement agencies today have the ability to request redacted domain name registration data - which they do - and contracted parties are responding to those requests on a regular, ongoing basis. Several large domain registries and registrars also separately worked with law enforcement agencies to develop a dedicated mechanism by which law enforcement agencies could gain access to their domain name registration information. This mechanism is in place and used by law enforcement.
    - The change in public WHOIS access was prompted by Europe’s GDPR, under which some registrant information — name, organization, address, phone number, and email — is deemed personal data that cannot be published publicly. Since then, privacy laws in many countries and several states, including California, have mirrored those restrictions.
    - Registries and registrars regularly meet with law enforcement agencies as part of the ICANN Governmental Advisory Committee’s (GAC’s) Public Safety Working Group (PSWG) to develop and discuss the best methods for requesting redacted domain name registration data so that responses are timely. PSWG representatives include law enforcement personnel from the FBI, FTC, FDA, and Europol.
    - Today, some WHOIS data continues to be available publicly, but those personal data elements are no longer published for public use. WHOIS data has not “gone dark,” but shifted to a gated access method accessible only to those who have an established legal purpose. This change has prompted some to call for the passage of U.S. legislation to force a return to the public publishing of all WHOIS data.

- **Federal Legislation is Not Required.** i2Coalition opposes the calls for WHOIS legislation, as it would do far more harm than good to both the U.S. digital economy and the public good. Further, those that legitimately need access to personal information, like law enforcement and researchers, still have the ability to access it, so there is no urgency to address this problem legislatively.
    - The ICANN EPDP created baseline practices for registries and registrars with regard to the publication of personal data, providing predictability to those parties with lawful rights

to access the data. The ICANN process has provided the opportunity to consider the bigger picture and find the intersection between privacy and harm reduction.
    - The i2Coalition endorses systems that make the process for authorized access as streamlined and as predictable as possible so that those who rely on this data and have a qualifying need to use it can do so while maintaining the privacy protections that the EU put in place. Congress should let the multistakeholder process work. No legislation is needed at this time.

#5: TRADE - US & EU TRANSATLANTIC DATA PRIVACY FRAMEWORK

- We applaud the announcement of the new US-EU Transatlantic Data Privacy Framework which will provide new safeguards to ensure that US intelligence activities are limited to what is necessary and proportionate to protect national security, and also will create a new redress system to address the complaints of EU citizens.

- This framework will help i2Coalition members and multitudes of other companies doing business with the EU. We congratulate the U.S. and EU negotiators for reaching this milestone and look forward to the ongoing implementation.

#6: INTERNET GOVERNANCE

- The i2Coalition strongly supports the multistakeholder model (MSM) of Internet governance and appreciates the U.S.. government's continuing leadership in promoting the MSM globally. The MSM continues to be the proper way to develop global policy for globally-architected, open Internet infrastructure.

- The MSM has come under threat as authoritarian regimes seek to wall off their citizens from the global Internet. We support and commend the U.S. government's efforts in supporting the American candidate for ITU Secretary-General (Doreen Bogdan-Martin) who is the right leader for promoting continued open Internet policies and the MSM for Internet governance.

#7: FBI INFORMAL DISCUSSION & I2C SPECIAL LAW ENFORCEMENT PROJECT

- **Mutual Benefits of Informal Consultation.** Thank you for joining us at our fly-in. We believe opportunities like this for our members to have policy discussions with FBI leadership are highly useful and mutually beneficial. This helps our members to better understand how the FBI engages in important tech policy discussions, and if and how it may choose to consult with the industry directly.
- **i2Coalition Members Special Law Enforcement Project.** The i2 Coalition is in the early stages of developing a special project to enhance how our members collaborate and interface with law enforcement. Our membership includes companies that operate some of the largest help desks in the world, and they sometimes run into problems not having an active relationship with the FBI when an agent reaches out to engage. One of the goals of our project is to change this dynamic so that our members have ready guidance to know what to do to properly and timely handle these requests.
- **Discussion Topic-Access to Domain Registration Data.** There are many other areas we could cover today, but one interesting discussion could emerge around domain registration data, and whether the FBI has the access it needs to this data from Internet infrastructure providers in our space.

#8: BROADBAND AND HIGH-SPEED INTERNET ACCESS

- **Broadband is a National Priority.** The i2Coalition commends and supports the U.S. government's work to close the digital divide and deploy high-speed Internet access to underserved and unserved communities. This is an economic and social priority, made more urgent in light of our experiences during the COVID-19 pandemic when so much of our civic life and economic activity were thrust online. As Internet infrastructure providers, we have learned firsthand that equitable Internet access and Internet resilience are more important than ever.
- **Bipartisan Investment in the Future.** We especially applaud the swift, bipartisan collaboration between the Administration and Congress that made the broadband grant programs a reality. This initiative will benefit the nation's citizens and our economy for many decades to come.

II. BACKGROUND ON POLICY ISSUES

#1: INTERMEDIARY LIABILITY - DMCA SEC. 512 & TECHNICAL MEASURES

Key discussion topics with our IP guest speakers will include:

- Whether Congress should "reform" the DMCA, and to what extent (DMCA text link), including proposed changes to the STMs provisions in Section 512(i) and the Tillis/Leahy SMART Copyright Act; and
- Whether even under the existing DMCA legal framework, the Copyright Office has authority and should conduct a rulemaking on standard technical measures (STMs) under Section 512(i).

Senate: Sen. Tillis' DMCA Reform Efforts. In 2020, Sen. Thom Tillis (R-NC) was re-elected to the Senate for a second term (ending in Jan. 2027) and is the Ranking Member of the Senate Judiciary Intellectual Property (IP) Subcommittee with jurisdiction over copyright, patent, and trademark law (Sen. Patrick Leahy (D-VT), who is retiring this year, chairs the IP Subcommittee). Tillis' Counsel Brad Watts leads the Senator's IP legislative work. During his first term and continuing to the present, Sen. Tillis has called for DMCA reform. In general, Sen. Tillis and his staff actively promote and support the interests of content creators regarding digital copyright and in other IP areas.

- In the prior (116th) Congress, as Chair of the IP Subcommittee, and following the Copyright Office release in May 2020 of a major report assessing Section 512 of the DMCA, Sen. Tillis released for public input a comprehensive draft DMCA reform bill. The tech community opposed most of this draft bill because its provisions were largely skewed in favor of content creators. ● In the current (117th) Congress, Sen. Tillis did not re-offer that draft comprehensive DMCA reform bill but instead directed his staff to work with stakeholders from the content and tech communities on reforming discrete parts of the DMCA. Sen. Tillis has most recently focused his efforts on two key areas: (1) amending Section 512(i) of the DMCA regarding STMs (service providers must accommodate and not interfere with STMs in order to maintain eligibility for 512 safe harbors); and (2) developing copyright legislation desired by the content community to authorize courts to issue orders to "service providers" requiring them to block "foreign rogue" piracy websites. These two activity areas are summarized below.
- **STMs: Tech Industry Opposition to Tillis/Leahy Introduction of the "SMART Copyright Act."** On March 17, 2022, Sen. Tillis and Sen. Leahy introduced the "Strengthening Measures to Advance Rights Technologies Copyright Act ("SMART" Copyright Act"). Numerous tech industry associations (including the i2Coalition) and civil society groups wrote a letter on March 29 to the

Senators and the Senate Judiciary and Rules Committee members voicing immediate, strong opposition to the SMART Act. Many other critiques of the bill were posted as well by tech public interest groups. The legislation would clearly break the DMCA's careful balance between innovation and copyright protection.
    - Its proposed amendments to the STM provisions in Sec. 512(i)) would lessen service provider and user clarity and certainty in present and future technical measures that are employed to maintain safe harbor status under the DMCA.
    - The bill's new proposed Sec. 514 would result in endless triennial litigation cycles overseen by the Copyright Office about a new, entirely separate category of "designated technical measures" (DTMs). The proposed Section 514 would give the Copyright Office authority far beyond its technical expertise to identify and mandate such DTMs, transforming it into an Internet regulator. The bill's direct and heavy-handed government involvement in the creation of technical measures for private industry conflicts with traditional U.S. standards policy and also creates grave risks to, among other things, cybersecurity, network performance, competition, collaboration, and innovation.
- **Proposed "Foreign Rogue" Website Blocking Legislation.** Sen. Tillis has directed his staff to work with stakeholders from the content and tech industries on separate, targeted legislation that would authorize courts to issue web blocking orders to service providers to shut down "foreign rogue" websites. The content community seeks this legislation and has described these websites as primarily designed or provided for the purpose of infringing copyright, with no commercially significant purpose or use other than copyright infringement, and intentionally marketed to promote copyright infringement. The i2Coalition does not believe this legislation is necessary or appropriate, but has been willing at meetings convened by Sen. Tillis' office over the past six months to discuss and critique the idea with Sen. Tillis' staff and representatives from the content community, along with our colleagues in the broader tech, library, and ISP communities.

Copyright Office: Section 512 Initiatives. The Copyright Office has initiated a Notice of Inquiry (NOI) on STMs and accepted public comments, and conducted stakeholder consultations on STMs and voluntary technical measures, as summarized below.

- **Standard Technical Measures (512(i)) NOI Proceeding**. In May 2020, as an outgrowth of several years of copyright hearings conducted by the House Judiciary Committee, the U.S. Copyright Office issued a major Report on Section 512 of Title 17, to assess the DMCA Section 512 "safe harbor" framework, which limits an online service provider's liability for infringement if the provider meets certain conditions. One of these conditions is that the online service provider "accommodates and does not interfere with standard technical measures" (STMs) to identify or protect copyrighted works. In the report, the Copyright Office stated its view that the identification of STMs may improve the overall functioning of the notice-and-takedown system. In September 2020, the Copyright Office held virtual stakeholder discussions covering the legal foundation of STMs, current technologies and their potential for adoption as STMs, and means of identifying or developing STMs going forward. In June 2021, Senators Thom Tillis and Patrick Leahy asked the Copyright Office to further explore the identification and implementation of STMs under section 512(i). In April 2022, the U.S. Copyright Office issued a Federal Register notice initiating an inquiry proceeding to gather public comments to advise Congress on the development and use of STMs for the protection of copyrighted works, as defined in section 512(i) of Title 17. The public comments were filed on May 27, 2022 (link to i2Coalition comments).

- **Voluntary Technical Measures Consultations.** Separate from but complementary to the STMs NOI, the Copyright Office began consultations on voluntarily deployed technical measures for identifying or protecting copyrighted works online, announced in the Federal Register on December 22, 2021, with the opening plenary session held on February 22, 2022. The Office released the following session schedule[1]:

  Session A: "Balance of rights and responsibilities"
  Date: Thursday, June 2, 11 am – 1 pm
  Topic: The past imbalances in rights and obligations between large and small stakeholders and among rightsholders, service providers, and users and how such imbalances have shaped current technical measures. This session sought to identify specific remedies for these imbalances going forward.

  Session B: "Variation among technical measures deployment: purposes & scalability" **Date:** Tuesday, June 7, 2 – 4 pm
  Topic: The differences between technical measures used to identify copyrighted works and technical measures used to protect copyrighted works with the goal of identifying how to ensure that future policies and practices acknowledge these differences. This session sought to also identify points of scalability to address the "one-size-doesn't-fit-all" issue discussed during the plenary.

  Session C: "Availability, affordability, & accessibility of technical measures"
  Date: Thursday, June 9, 11 am – 1 pm
  Topic: Issues relating to availability, affordability, and accessibility of technical measures, with the goal of identifying how cost and access can be equitably calibrated.

  Session D: "Error rate & human vs. technological review"
  Date: Thursday, June 16, 2 – 4 pm
  Topic: Issues regarding error rates and challenges of both human and technological review, with the goal of determining guidelines and practices that balance what is feasible given the capabilities and limitations of today's technologies with forming practices in which unacceptable errors can be avoided.

  Session E: "International Issues"
  Date: Tuesday, June 28, 2–4 pm
  Topic: International aspects of voluntary technical measures. This session will also consider the developments in Europe, specifically the implementation of the EU DSM, and elsewhere and how these developments may impact current and future policies in the United States regarding voluntary technical measures, with the goal of identifying points of potential harmony and dissonance with current policies, and points of best practice/lessons learned.

  Session F: "Mandatory standard technical measures vs. voluntary technical measures & the role of government"
  Date: Thursday, June 30, 11 am–1 pm
  Topic: The impact and efficiency of technical measures developed in mandatory or voluntary contexts, with the goal of finding a potential balance between mandatory and voluntary design processes and standards in the technical measures context, and how such balance

[1] The i2Coalition was invited to be on panel sessions A and F.

would operate in the digital ecosystem. This session sought to explore the role of government, particularly the U.S. Copyright Office, regarding mandatory and voluntary technical measures, with the goal of identifying potential areas for legislative support and short and long-term activities of various government agencies.

#2: INTERMEDIARY LIABILITY - SECTION 230 & CONTENT MODERATION

Section 230 Statutory Language.
The liability protections of Section 230(c) apply to a "provider or user of an *interactive computer service*," which in Section 230(f)(2) is defined as:

> any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions. 47 U.S.C. Section 230(f)(2).

Section 230 (full link here) also provides a specific subdefinition of the term "access software provider" in Section 230(f)(4):

> The term "access software provider" means a provider of software (including client or server software), or enabling tools that do any one or more of the following:
>
> (A) filter, screen, allow, or disallow content;
>
> (B) pick, choose, analyze, or digest content; or
>
> (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content. 47 U.S.C. Section 230(f)(4).

Federal Legislative Proposals on Section 230. Numerous Section 230 bills have been introduced in the 117th Congress but, to date, bipartisan consensus has not emerged to move legislation forward. The following is a link listing Section 230 bills introduced in the 117th Congress: See "Resources" Section, House & Senate Proposals. (Source: Disruptive Competition Project, CCIA)

Political Gridlock in Congress. Republicans and Democrats want to reform Section 230 largely for different reasons. Some Republicans allege that the largest social media platforms have moderated too much content and censored their political speech. Some Democrats believe that the platforms do not moderate enough to take down disinformation and misinformation. Despite the broad range of service providers and organizations expressly covered by Section 230, critics of the law have tended inaccurately to equate and reduce the statutory term "interactive computer service" to large social media platforms only. Early on in this debate, some policymakers critical of "Big Tech" simplistically argued that Section 230 needs to be repealed in its entirety under the mistaken belief that Section 230 only applies to social media providers. Those bills were followed by a variety of others that would set conditions and limits on the Section 230 liability protections. Some of the bills are expressly limited in their application to the largest platforms based on factors such as numbers of users and revenue metrics. Major themes have emerged in many of these bills, including: platform transparency and accountability; the creation of new, dedicated digital regulatory commissions to oversee digital platforms; removing 230 protections to allow lawsuits against providers for transmission of child sexual

abuse materials (CSAM); and fighting social media political bias against conservative voices.

i2Coalition Section 230 Advocacy Examples:

- **Senate: S. 3538, EARN IT Act (CSAM) & Tech Sector Opposition.** Both in the 116th and 117th Congresses, the i2Coalition joined with numerous other tech, public interest, and civil society groups in opposing a bill sponsored by Sens. Lindsey Graham (R-SC) and Richard Blumenthal (D-CT) which would create an exception to Section 230's liability protection to allow federal civil actions and state civil and criminal actions against service providers for transmission of child sexual abuse material (CSAM). Although the bill was approved by the Senate Judiciary Committee, it is highly controversial and has not moved forward for further consideration in the 117th Congress.
    - Our strong opposition pointed out numerous problems in the bill, including drafting concerns likely leading to overbroad moderation limiting free expression online, or to outright prohibitions on upload capabilities due to providers' liability concerns.
    - We also opposed the bill's provision disincentivizing the use of strong end-to-end encryption (E2E) because it would allow courts to consider the offering of E2E as evidence in support of claims that a provider was acting recklessly or negligently. The mere threat that use of encryption could be used as evidence against a service provider in a criminal prosecution would be a strong disincentive to using it. As infrastructure providers, we stand at the heart of the digital economy, and maximizing its safety depends on our ability to keep our technologies secure. Strong encryption unencumbered by backdoors is critical for not only national security and personal security of individuals, including children, but a continued competitive digital economy. Indeed, the Biden Administration has explicitly urged the private sector to use robust encryption as part of our national cybersecurity strategy.
    - We pointed out that further erosion of Section 230's protections that our industry relies upon will have damaging unintended consequences. Section 230 affirmatively facilitates positive partnerships among websites, service providers, advocacy groups, and law enforcement in combating child exploitation online. Its legal protections allow infrastructure providers to share signs of abuse, invest in new preventative technologies, and moderate content. Without Section 230, this level of cooperation will likely not be able to continue and would force criminals further underground.
    - Instead of considering ill-advised bills like EARN IT, we have consistently asked Congress to work with us as we continue to build more effective ways of combating child endangerment online. As an industry, we seek to continue to partner cooperatively with law enforcement, safety professionals, and organizations including the National Center for Missing & Exploited Children to end child endangerment online.

- **Senate: S. 797, Platform Accountability and Consumer Transparency (PACT) ACT & Exemption for Internet Infrastructure.** Senators Brian Schatz (D-HI) and John Thune (R-SD.) reintroduced the Platform Accountability and Consumer Transparency (PACT) Act in the 117th Congress. This bipartisan bill would amend Section 230 to make platforms' content moderation practices more transparent and hold those companies accountable for content that violates their own policies or is illegal.
    - After discussing with the sponsors' offices the implications of this bill for our members when it was first proposed in the prior Congress, the i2Coalition achieved inclusion of an exemption provision for "Internet Infrastructure Service." This move has led sponsors of other Section 230 bills to follow suit by including similar and appropriate Internet

infrastructure exemption provisions (e.g., H.R. 2154, Protecting Americans From Dangerous Algorithms Act).
    - This success demonstrates the value of our educational advocacy with Congress to ensure policymakers' understanding of our role in the Internet ecosystem and avoid overbreadth in the legislative process.

- **Continued Vigilance: i2Coalition Leading the "Coalition of the Otherwise Affected."** As detailed above, the i2Coalition has underscored the imperative that Congress understand the full scope of Section 230 and the importance of its legal shield for entities beyond the largest social media platforms. We will continue to lead an informal "coalition of the otherwise affected" in the 230 debate, working closely with our colleagues in the library and higher education communities to educate policymakers on that point. Below is additional background which we have emphasized in this debate on the importance of Section 230 to these other groups, made even more critical as our nation and economy continues to weather and recover from the COVID-19 pandemic.

    - Small & Medium Businesses. In the 1990s, innovative online commercial businesses sprouted and grew, notably Prodigy, the Internet Service Provider (ISP) involved in the case which Congress set to overturn when drafting Section 230. Today legions of companies covered by the statutory definition of an "interactive computer service"- *other than* the largest social media platforms-- together with their users depend on Section 230 liability protections in maintaining smooth, efficient, and safe online operations.
        - These companies include ISPs, web hosting companies, managed cloud providers, and DNS registries and registrars. Overwhelmingly they often serve the smallest of businesses in our local communities. During this pandemic, these providers have served as an economic lifeline for many of their customers forced to scramble to shift their businesses online where possible.
        - Internet infrastructure providers in particular rely on Section 230 protection because it offers crucial assurances that they will not be treated as the publishers or speakers of content made available by others. This protection has become foundational to the economic diversity and low barriers to entry that characterize today's Internet and is vital because of the nature of critical Internet infrastructure services such as website hosting and content distribution networks, which may create a superficial association between the infrastructure provider and third-party content. Section 230 has played a key role in protecting such companies against lawsuits relating to content posted by third parties that the infrastructure provider never reviewed and in no way endorsed.
        - The liability protections of Section 230 support competition by allowing entrepreneurs as well as small- and medium-sized businesses to engage in commerce online and offer choices beyond those of the largest companies without the threat of devastating legal fees pressuring them either to leave the market or not enter it at all. Policymakers should recognize that the monumental, sudden shifts to online commerce and remote work nationwide during COVID-19—moves that prevented the entire economy from grinding to a halt—were powered substantially by all of these other online players who depend on the existence of Section 230 liability protections.

- Educational Institutions. University networks counted as among the most vital pioneering infrastructure of the Internet in the 1980s and early 1990s. Now, more than twenty-five

years after Section 230's enactment into law and in reliance on it, multitudes of colleges and universities have built sophisticated networks managed with content moderation rules tailored to their unique academic communities. Perhaps most dramatically, the reach and operational practices, including content moderation, of the networks of many higher education institutions and public and private elementary and secondary schools made continued learning a possibility during the COVID-19 pandemic because they were protected from litigation threats over user-generated content.

- Libraries. Public libraries began launching online services in the early days of the Internet to make it accessible to the citizens in their communities, frequently giving their patrons who lacked their own Internet connection their very first glimpse of the World Wide Web. That crucial service to library patrons continues today, especially in the nation's most vulnerable, economically disadvantaged urban and rural areas lacking sufficient residential access to broadband. Among other online services, many libraries—including the Library of Congress, the National Archives, the New York Public Library, and major state university system libraries—host interactive computer services that provide user-generated content. During the COVID-19 pandemic crisis, it is no exaggeration to state that online libraries, including through their interactive offerings that welcome user-generated content, stepped up to help sustain and continuously bolster our communities.

#3: FEDERAL CONSUMER DATA PRIVACY & SECURITY

New Push for National Consumer Data Privacy & Security Legislation. On June 3, the Chair (Rep. Frank Pallone (D-NJ)) and Ranking Member (Rep. Cathy McMorris-Rodgers (R-WA)) of the House Energy & Commerce Committee and the Ranking Member of the Senate Commerce Committee (Sen. Roger Wicker (R-MS) released draft Bipartisan Federal Consumer Data and Security Legislation (also called the "3 Corners bill"; section-by-section summary here). Senate Commerce Committee Chair Maria Cantwell (D-WA) chose not to join that announcement. Sen. Cantwell believes that the draft 3 Corners bill falls short in protecting consumers and so far instead is pointing to a revision of her privacy bill from 2019 as the appropriate vehicle. Another key Democrat, Sen. Brian Schatz (D-HI), has similar concerns and has urged panel leaders to advance a proposal that imposes on companies a duty of care standard for online data to protect the personal data of users. Sen. Schatz has said that if his Senate Commerce Committee colleagues cannot include that duty of care, then they should not preempt states from adopting consumer-first online privacy reforms. Many Democrats support creating a duty of care standard for online data, but it is widely opposed by Republicans.

Preliminary Industry Analysis of the 3 Corners Bill. The International Association of Privacy Professionals (IAPP) has posted some preliminary assessment and analysis of the 3 Corners draft, whose text is still evolving. The bill's requirements are built around a broad range of concepts in its four titles–to provide a duty of loyalty, consumer data rights, corporate accountability, and enforcement.

Private Right of Action. On private right of action, the 3 Corners bill allows people to sue technology companies directly four years after the bill's enactment to allow businesses to get up to speed with the new requirements, and to give consumers time to understand the law. Senate Commerce Chair Cantwell took issue with a four-year delay on private rights of action. Chair Cantwell also continues to differ from her counterparts regarding how to prohibit companies from imposing pre-dispute mandatory arbitration on consumers, which is typically seen in terms of service agreements. Cantwell's bill would prohibit such mandatory arbitration in cases of "substantial" privacy harm, defined as harm to an individual worth $1,000 or more, or certain physical and mental harm. The effort is meant to give consumers the choice to

resolve disputes in a public court of law instead of through a paid arbiter, which some see as favorable to companies. The bipartisan 3 Corners bill only states companies would not be able to enforce pre-dispute arbitration agreements with respect to minors, a narrower definition. It would also allow private right of action for specific claims, including those alleging violations of kids' privacy.

Pre-emption. Although touted as breaking the logjam over the preemption and private rights of action disagreements which cratered earlier attempts to pass comprehensive consumer data privacy bills, the 3 Corners bill is drawing opposition from some industry groups, notably the U.S. Chamber of Commerce. The 3 Corners bill would preempt state consumer data privacy laws, with the exception of Illinois' biometric privacy protection act and a section of California's privacy law related to data breaches. But the Chamber is concerned that it would allow other adjacent categories of consumer protection laws to remain enforceable, like laws around cyberstalking or facial recognition. In a preliminary assessment the Chamber said that a national privacy law should be a true national standard but notes that the bill's preemption language carves out fifteen different state laws including those in California and Illinois, so the Chamber contends that it would effectively create a new national patchwork of privacy laws.

ACLU Concerns. Progressive interests have also weighed in with concerns. The ACLU sent a June 10 open letter to Congress in which it rejected the 3 Corners bill as being full of "problematic provisions" that will need time to fix, and also made the same argument against Senate Commerce Committee Chair Cantwell's rival privacy draft that is now circulating. The ACLU pointed to recent state laws passed quickly and with minimal input from privacy advocates, claiming those efforts allowed industry segments to successfully push harmful or effectively useless state privacy bills. The ACLU does not want Congress to make the same mistake.

Childrens' Online Privacy & Safety. The 3 Corners bill addresses children's online safety, including by stating that the definition of "sensitive covered data," which is subject to stronger protections, includes information of individuals under the age of 17. It bars companies from targeting advertising at children 17 and younger, and from transferring the data of kids aged 13 to 17 to third parties without their express affirmative consent. It would also establish a Youth Privacy and Marketing Division at the Federal Trade Commission to enforce its provisions.

House E&C Subcommittee Hearing. The House Energy & Commerce Subcommittee on Consumer Protection and Commerce scheduled a June 14 legislative hearing on the 3 Corners bill and hopes to hold a markup soon, as early as June 22. Without the support of Senate Commerce Committee Chair Cantwell (D-WA), and in recognition of the short remaining legislative calendar ahead of the November midterm elections, it may be difficult to pass a comprehensive federal consumer data privacy and security. If legislation does not pass this year, we can expect that the 3 Corners bill will be a starting point for drafting in the next Congress.

#4: DNS - WHOIS PRIVACY

ICANN 2022 Summary: GDPR and Registration Data Access. When GDPR was enacted, the ICANN Board adopted the Temporary Specification for gTLD Registration Data (Temporary Specification), establishing temporary requirements to allow ICANN and gTLD registry operators and registrars to comply with the GDPR while continuing to uphold existing ICANN contractual requirements and community-developed policies. It maintained a robust collection of registration data, but restricted access to registration data that might include personal information. In effect, most directory information contained in gTLD domain registration data is no longer publicly available. Parties seeking access to non-public gTLD registration data must request that access from the contracted parties (i.e., the holders of domain

registration data who have contracts with ICANN). Contracted parties are required to provide reasonable access to personal data in registration data based on a legitimate interest pursued by the third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the registered name holder or data subject, pursuant to GDPR Article 6(1)(f). Each contracted party conducts its own assessment to determine whether a request for access will be granted. This has fragmented a system that many rely upon for reasons as varied as law enforcement investigations, intellectual property, and security incident response, among others. The new registration data policy recommended by the community, following the Temporary Specification, confirmed the Temporary Specification approach. (Source: ICANN org Submission to the European Commission Call for Evidence on the EU Toolbox Against Counterfeiting 6 April 2022, Section 3.3.)

ICANN 2022 Summary: Addressing Accuracy of Registration Data. The EU's GDPR also affected ICANN org's ability to investigate inaccuracy of registration data and take steps to address it with gTLD registrars. Pre-GDPR, ICANN org investigated the accuracy of gTLD registration data both in response to external complaints and in the context of the WHOIS Accuracy Reporting System project, in which ICANN org proactively identified potential inaccuracies and addressed them with registrars. This project was paused upon the effective date of the GDPR, given that much of the registrant contact information is now redacted from public view and, thus, not accessible for analysis. gTLD registrars remain obligated to collect, retain, and validate and verify this contact data, but are no longer obliged to publish it. Instead of this proactive analytic approach, ICANN org's activities in the registration data accuracy context are solely in the compliance context. If there is a question or complaint concerning a particular registrar's compliance with registration data verification and validation requirements, ICANN org will take steps to ensure the registrar is complying with the obligations in the RAA, according to which they must take reasonable steps to maintain the accuracy of their registrants' contact information. (Source: ICANN org Submission to the European Commission Call for Evidence on the EU Toolbox Against Counterfeiting 6 April 2022, Section 3.3.)

#5: TRADE - US & EU TRANSATLANTIC DATA PRIVACY FRAMEWORK IAPP

Infographic: From Privacy Shield to Transatlantic Data Privacy Framework (April 2022)

New Transatlantic Data Privacy Framework. On March 25 the United States ("U.S.") and the European Commission ("EU Commission") announced an "agreement in principle" to develop a new Trans-Atlantic Data Privacy Framework ("Framework"). The Framework is intended to re-establish a legal mechanism for transfers of EU personal data to the U.S. after the Court of Justice of the European Union ("CJEU") invalidated the EU-U.S. Privacy Shield over concerns about the breadth of U.S. surveillance laws in its *Data Protection Commission v. Facebook Ireland and Maximillian Schrems* ("*Schrems II*") judgment on July 16, 2020. In a joint statement, President Joseph Biden and European Commission President Ursula von der Leyen emphasized the Framework's shared commitments to advance privacy, data protection, the rule of law, and security. They noted that the new Framework would enhance the previously invalidated Privacy Shield framework to help small and large companies compete in the digital economy and support the continued flow of data underpinning more than $1 trillion in cross-border commerce annually.

Following the invalidation of the EU-U.S. Privacy Shield in *Schrems II*, regulators commenced immediate negotiations on the new framework to enable companies to continue to transfer data to the U.S. After more than a year of negotiations between the U.S. and the EU, the U.S. committed to incorporating new safeguards to form a durable and reliable basis for the European Commission's future adequacy decision regarding protections afforded to EU personal data transferred into the U.S. The joint announcement focused on trying to address several concerns highlighted by the Court in *Schrems II* by committing to

several new data protection measures to be implemented by the U.S. intelligence community.

The Framework will build on the structure of the previously invalidated Privacy Shield framework and will focus on several key principles, including:

- The free and safe flow of data between the EU and participating U.S. companies. ● The enactment of rules and binding safeguards to limit access to data by U.S. intelligence authorities to only what is "necessary and proportionate" to advance defined national security objectives and without disproportionately impacting the protection of privacy and civil liberties. ● The creation of a two-tier redress system to investigate and resolve EU data subjects' complaints regarding access of data by U.S. intelligence authorities including the creation of a Data Protection Review Court that would consist of individuals chosen from outside the U.S. government who would have full authority to adjudicate claims and direct remedial measures as necessary. EU individuals will continue to have access to multiple avenues of recourse to resolve complaints regarding participating companies, including options for alternative dispute resolution and binding arbitration. ● The obligation for companies processing data transferred from the EU to meet high standards including requirements to adhere to, and self-certify their adherence to, the Privacy Shield Principles under the oversight of the U.S. Department of Commerce.
- The encouragement of U.S. intelligence agencies to adopt procedures to ensure effective oversight of new privacy and civil liberties standards.
- The development of specific monitoring and review mechanisms.

Forthcoming Biden Executive Order and DOJ Regulation. For now, many of the details are still unknown and the White House has indicated that additional information is forthcoming in an Executive Order and the adoption of legal documents to effectuate the new Framework in both the U.S. and the EU. Together, the U.S. government and the European Commission will continue working to formalize their commitment to form the Trans-Atlantic Data Privacy Framework.

Schrems Reaction. Max Schrems, the lead litigant in *Schrems II*, issued a statement through his nonprofit organization, noyb ("None of Your Business"). Schrems stated that the US and EU had made solely a political announcement and that until there was a final text to review, the Framework could be months away from implementation. Additionally, Schrems indicated that he would closely review the text when issued and was likely to challenge it if it is deemed not to be in line with EU law. Noyb speculated that this may lead to legal uncertainty for the time being. Schrems reportedly is prepared to challenge any final adequacy decision that would fail to provide the needed legal certainty.

Ongoing Use of Standard Contractual Clauses. Given the possibility of legal challenges to the new Transatlantic Data Privacy Framework, Standard Contractual Clauses (SCCs) are likely to remain an important mechanism for effectuating GDPR compliant transfers of data from the EU to the US. According to the General Data Protection Regulation (GDPR), contractual clauses ensuring appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries. This includes model contract clauses–the SCCs–that have been "pre-approved" by the European Commission. Inclusion of SCCs in international data transfer agreements enables controllers and processors to comply with their obligations under the GDPR.

- On May 25, 2022, the European Commission announced the release of a new guidance document relating to SCCs and international data transfers. The guidance is included in a series of questions and answers, which the European Commission is making available for general informational purposes to provide practical guidance on the use of SCCs and assist stakeholders in their compliance efforts under the GDPR.
- After the US-EU Privacy Shield was invalidated by the 2020 *Schrems II* decision, SCCs became

the primary mechanism for transferring data from the EU to the US in compliance with the GDPR.

#6: INTERNET GOVERNANCE

Biden Admin. Declaration on the Future of the Internet. On April 28, the Biden administration announced a new global partnership to set norms for the use of technology by nation-states: the Declaration for the Future of the Internet. The statement was signed by 61 nations and aims to establish a code of practice for how democratic countries should engage with the web, although it is non-binding and lays out no specific policy commitments or requirements. The Declaration's vision for the Internet is broad—aspiring to promote universal Internet access, protect human rights, ensure fair economic competition, design secure digital infrastructure, promote pluralism and freedom of expression, and guarantee a multi-stakeholder approach to Internet governance. It stands as an implicit criticism of Russia's and China's efforts to wall off their citizens from the global Internet.

ITU Secretary-General Election Impact. American candidate Doreen Bogdan-Martin is running against a Russian candidate Rashid Ismailov for the position of ITU Secretary-General. The new Secretary-General will replace China's Houlin Zhao, who has served in the position for eight years. The election will take place during a plenipotentiary conference in September. U.S. interests are working intensively in support of Bogdan-Martin's candidacy as it is not a given that she will prevail.

- There have been shifts in country support recently. For years, there were liberal governments favoring an open Internet approach on one side and authoritarian countries on the other. Swing states like India and Brazil have started voting with more closed-Internet policies. There is growing concern that some developing countries may be willing to side with the Russian candidate in the upcoming election. The Russian candidate Ismailov has support from China and reportedly there are many other countries that are sympathetic to Russia's agenda.
- The election is important for shaping two core things at the center of the Internet: (1) tech standards, and (2) processes and authorities for Internet governance. Multistakeholder tech standards supported by democratic nations have been valuable in efforts to bring Internet access and broadband connectivity to low-income countries. It also has been enormously helpful for national security to have consistent standards. The U.S. is concerned that Russia will seek to limit these benefits by pushing greater state control of the Internet and will attempt to change ITU standards in order for the ITU to take over and essentially eliminate the role of Internet governance organizations.

#7: FBI INFORMAL DISCUSSION & I2C SPECIAL LAW ENFORCEMENT PROJECT

Context. The i2Coalition has made it a priority to consult with law enforcement policy leaders at the FBI at several of its prior Washington fly-in meetings. These in-person, informal discussions build relationships and support mutual understanding of respective roles and functions when it comes to investigating and handling online abuses and potential crimes. With the relaunch of our in-person events, this session will inform the development of our special law enforcement project for members. It will also serve to reinforce with FBI leadership i2Coalition's core values of education advocacy around Internet infrastructure and our commitment to meaningful and appropriate collaboration.

#8: BROADBAND AND HIGH-SPEED INTERNET ACCESS

Biden Administration Broadband Goals. The Biden administration is actively pursuing the goal of connecting all Americans to affordable, reliable high-speed internet. The new Bipartisan Infrastructure

Law (also called the Infrastructure Investment and Jobs Act (IIJA) as passed by Congress) provides $65 billion in funding to help achieve that objective. These funds add to and support existing programs that expand Internet access and use.

Four agencies are leading this major effort: the National Telecommunications and Information Administration (NTIA), the Federal Communications Commission (FCC), the Department of the Treasury, and the U.S. Department of Agriculture (USDA).

The Programs support high-speed Internet planning (e.g., data collection, mapping, and feasibility studies), infrastructure for deployment, and adoption (ensuring access through mechanisms including subsidies, equipment, public access, digital literacy, skills training, workforce development, and telehealth). The goal of these programs is to achieve digital equity through improved access and intentional, inclusive planning that leads to effective, impactful outcomes.

NTIA: Internet for All Initiative. On May 13 the Department of Commerce and NTIA announced the "Internet for All" initiative, launching a new website and outlining details for three new funding programs to be administered by the NTIA as part of the Biden's administration's broadband program:

- Broadband Equity, Access, and Deployment (BEAD) Program ($42.5 billion)
- Enabling Middle Mile Broadband Infrastructure Program ($1 billion)
- State Digital Equity Act programs ($1.5 billion)

The Senate Commerce Committee Subcommittee on Communications, Media, and Broadband held an NTIA oversight hearing on June 9, 2022, at which NTIA Administrator Alan Davidson testified and reported on NTIA's progress to date in implementing the broadband programs for which it is responsible.

FCC Mapping. The development and release of accurate broadband mapping is a critical component in the national broadband deployment program. The FCC has indicated that sometime before year-end (late fall) it will release updated maps to be used for making funding decisions to improve broadband access.