Before the
**National Telecommunications and Information Administration**
Washington, D.C. 20230

| | | |
|---|---|---|
| In the Matter of | ) | |
| | ) | |
| Developing the Administration's Approach to Consumer Privacy | ) | Docket No. 180821780-8780-01 |
| | ) | |
| | ) | |
| *Notice and Request for Public Comments* | ) | RIN 0660-XC043 |

# Comments of the Motion Picture Association of America, Inc.

Nov. 9, 2018

Neil Fried
SVP & Senior Counsel
Motion Picture Association of America, Inc.
1301 K Street NW, Washington, D.C. 20005
(202) 378-9100

## Overview

The NTIA seeks comment on a federal approach for advancing privacy that also protects prosperity and innovation, and that is rooted in a set of user-centric outcomes and high-level goals.[1] Because ensuring continued access to WHOIS data will help accomplish the NTIA's user-centric outcomes and high-level goals, and will advance privacy while protecting prosperity and innovation, the NTIA should make ensuring such access an element of the federal approach.

WHOIS data—which contains contact information about domain name registrants—has been a cornerstone of online security and safety since before the dawn of the commercial internet.[2] Access to such information is critical to: 1) creating the transparency, accountability, and trust consumers need to be willing to share their data in the online environment; 2) protecting consumers from identity theft, misuse of data, and online lawlessness generally; and 3) maintaining the hospitable online environment necessary to promote the prosperity and innovation the NTIA seeks.

Unfortunately, the Internet Corporation for Assigned Names and Numbers has enacted a Temporary Specification[3]—under the stated goal of complying with the European Union's General Data Protection Regulation—that is unnecessarily resulting in restricted access to important WHOIS data well beyond what the GDPR mandates, and not just in Europe, but also in the United States and elsewhere.[4] This overbroad application of the GDPR is already hindering the ability of law enforcement agencies and others to investigate illict behavior—including sex trafficking, unlawful sale of opioids, cyber-attacks, identity theft, and theft of intellectual property.[5]

A chief, user-centric outcome of a federal privacy approach should be protecting consumers from illicit behavior online, which requires timely and meaningful access to WHOIS data. The MPAA therefore asks the NTIA to include as one of the elements of the federal privacy approach, continued efforts to ensure that certain basic WHOIS information remains publicly available, and that any information that the GDPR does require to be removed from public access still be available to third parties with legitimate interests through a reasonable, timely, and effective process. Such efforts should include Administration support for solutions through the multistakeholder process, for ICANN assumption of WHOIS under a unified access model, for WHOIS access requirements in trade agreements, and for federal legislation requiring registrars and registry operators to continue providing lawful access.

---

[1] Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01, *Notice and Request for Public Comments*, 83 Fed. Reg. 48600, 48600 (Sept. 26, 2018), https://www.gpo.gov/fdsys/pkg/FR-2018-09-26/pdf/2018-20941.pdf.

[2] *See History of WHOIS*, ICANN WHOIS, https://whois.icann.org/en/history-whois (last visited Nov. 7, 2018).

[3] ICANN, TEMPORARY SPECIFICATION FOR GTLD REGISTRATION DATA (May 25, 2018), https://www.icann.org/resources/pages/gtld-registration-data-specs-en.

[4] *See, e.g.,* ICANN, GOVERNMENTAL ADVISORY COMMITTEE, *Communiqué—San Juan, Puerto Rico* (Mar. 15, 2018) (stating that the GDPR applies only to the privacy of natural persons, not legal entities, and that it allows for access to data for legitimate purposes, regardless; cautioning against restricting access to registrant email addresses as a disproportionate response in light of the impact on law enforcement, cybersecurity and rights protection). https://gac.icann.org/advice/communiques/20180315_icann61%20gac%20communique_finall.pdf.

[5] *See, e.g.,* ANTI-PHISHING WORKING GROUP & MESSAGING, MALWARE AND MOBILE ANTI-ABUSE WORKING GROUP, ICANN GDPR AND WHOIS USERS SURVEY 4 (Oct. 2018), *available at* https://apwg.org/apwg-news-center/icann-whois-access/temporySpecSurvey and https://www.m3aawg.org/rel-WhoisSurvey2018-10.

## I. Continued WHOIS Access Will Advance the NTIA's Desired, User-Centric Outcomes and Ensure a Reasonably Informed User Who Is Empowered to Meaningfully Express Privacy Preferences

The request for comments states that dictating privacy practices, such as specific "notice and choice" requirements, can produce cumbersome privacy policies that few people read and that offer only binary options.[6] Consequently, the NTIA proposes instead to focus on outcomes.[7] To that end, the request for comments enumerates a number of desired outcomes aimed at producing "a reasonably informed user, empowered to meaningfully express privacy preferences" over data collection,[8] namely: 1) transparency, 2) user control; 3) minimization of data collection, 4) security of data; 5) opportunities for user access and correction; 6) risk management, to mitigate harmful use or exposure of the data; and 7) accountability.[9]

A federal approach to privacy that prioritizes continuing access to WHOIS data would help accomplish these outcomes. Users are not "reasonably informed" or "empowered to meaningfully express privacy preferences" if they cannot determine the entity behind a website—whether to verify its identity; to research its background; to find a contact for purposes of conveying information, preferences, questions, and concerns; or to seek redress for harms.

As the NTIA points out, "[t]rust is at the core of the United States' privacy policy formulation."[10] This trust is critically important online in light of the sheer magnitude of interactions consumers have with the "array of products and services" that they encounter in the digital environment, "many of which have become integral to their daily lives" and "depend on the collection, retention, and use of personal data."[11] Such trust requires transparency on the front end of online interactions, as well as accountability on the back end, and WHOIS access advances both of these NTIA-enumerated, user-centric outcomes.

Transparency on the front end is important so consumers providing personal information online to obtain goods or services have faith "that organizations will respect their interests, understand what is happening with their personal data, and [can] decide whether they are comfortable with this exchange."[12] It is much harder for users to trust organizations when deciding whether to turn over information if they can't determine with whom they are dealing. The lack of such transparency is a problem not only for individuals' beneficial use of the internet, but also for the success of online businesses, as evidenced by the NTIA data indicating that "at least one-third of online households have been deterred from certain forms of online activity, such as financial transactions, due to privacy and security concerns."[13] Continued access to WHOIS data will help consumers identify domain name registrants and web site operators when necessary, advancing the NTIA's user-centric outcome of transparency.

---

[6] *Notice and Request for Public Comments*, at 48601.
[7] *Id*.
[8] *Id.*
[9] *Id.*, at 48601-02.
[10] *Id.*, at 48600.
[11] *Id*
[12] *Id*
[13] *Id.*

Accountability is important on the back end, both as a deterrent to harmful behavior and so consumers know there are avenues for remedy should something go wrong. Consumers, businesses, public interest organizations, agencies, and law enforcement will have a much harder time advancing such accountability if they cannot find culprits who have misused information or engaged in other illicit online activity. Continued access to WHOIS data will advance the NTIA's user-centric outcome of accountability by making sure domain name registrants and web site operators know they can be approached, and by helping consumers, businesses, public interest organizations, agencies, and law enforcement do so.

Lastly, by helping users to approach domain name registrants and relevant administrative and technical representatives, continued access to WHOIS data will advance the NTIA's user-centric outcomes of enabling consumers to better control, minimize, secure, or correct collected data; and to mitigate harm from disclosure.

## II. Ensuring Continued Access to WHOIS Data Will Advance the NTIA's Goals of Harmonizing the Regulatory Landscape, Creating Legal Clarity While Preserving Innovation, Promoting Comprehensive Application, Following a Risk- and Outcome-Based Approach, Facilitating Interoperability, and Relying on FTC Enforcement

The request for comments also identifies a set of "high-level goals" intended to establish a "broad outline for the direction that Federal action should take."[14] Ensuring continued access to WHOIS data will advance the NTIA's goals of harmonizing the regulatory landscape, aiding legal clarity while maintaining the flexibility to innovate, promoting comprehensive application, following a risk- and outcome-based approach, and relying on FTC enforcement.[15]

Harmonization. Federal efforts to ensure continued access to WHOIS data will advance the NTIA's goal "to avoid duplicative and contradictory privacy-related obligations placed on organizations" and "ensure that the regulatory landscape for organizations that process personal data in the United States remains flexible, strong, predictable, and harmonized."[16]

With an overbroad interpretation of the GDPR gaining ground and renewed efforts by states to legislate on privacy,[17] access to WHOIS data may be hindered by duplicative and contradictory obligations. Moreover, reduced availability of WHOIS data will weaken efforts to contact domain name registrants whose domains are used—either with their knowledge or surreptitiously—for identity theft, misuse of personal data, and other unlawful behavior. Ensuring a continued baseline of WHOIS access obligations will help harmonize the requirements and maintain a strong defense against privacy-related and other harms.

---

[14] *Id.*, at 48602.

[15] *See id.*, at 48602-03.

[16] *Id.*, at 48602.

[17] *See, e.g.*, California Consumer Privacy Act of 2018, A.B. 375 (Cal. 2018), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375; Protections for Consumer Data Privacy Act, H.B. 18-1128 (Colo. 2018), https://leg.colorado.gov/sites/default/files/documents/2018A/bills/2018a_1128_enr.pdf.

The Administration should take an "all of the above" approach and endorse a variety of contemporaneous efforts to ensure continued WHOIS access, including through diplomatic channels, the ICANN multistakeholder process, trade agreements, and U.S. legislative action. For example, the MPAA urges the Administration to continue reiterating the importance of access to WHOIS data and the problems associated with ICANN's overbroad application of the GDPR.[18] In the category of multistakeholder efforts, the NTIA should urge ICANN and stakeholders to accelerate work on adopting a post-GDPR WHOIS-solution through the Expedited Policy Development Process on the Temporary Specification for gTLD Registration Data.[19] The NTIA should also continue to support efforts to provide access to non-public WHOIS data through an accreditation and access model, including the proposal from ICANN for a unified access model, or through other means that ICANN has suggested exploring, such as ICANN assuming legal responsibility for providing access as a sole controller.[20] On the trade side, the Administration should seek robust WHOIS access requirements in future trade agreements, perhaps expanding on language included in the U.S.-Mexico-Canada Agreement.[21]

---

[18]*See, e.g.*, Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 61 (Mar. 12, 2018) (stating that "the WHOIS service is an incredibly valuable tool for governments, businesses, intellectual property rights holders, and individual Internet users around the world," supporting "a solution that maintains the WHOIS service to the greatest extent possible in the face of data protection and privacy regulations such as the European General Data Protection Regulation," expressing a need to "maintain[] a WHOIS service that is quickly accessible for legitimate purposes," encouraging "revisions to [ICANN's interim] model to permit access to the most amount of registration data as possible," voicing "concern[] with the uncertainty around how access to WHOIS information for legitimate purposes will be maintained in the period between the date of GDPR enforcement, May 25, and the time in which the community is able to develop and agree to a formal accreditation process," calling for "[p]lans … to be put in place to ensure that the users behind the already defined legitimate purposes—such as law enforcement, intellectual property enforcement, and cybersecurity—are not stymied in their efforts to serve the public interest," and saying that "[t]he United States will not accept a situation in which WHOIS information is not available or is so difficult to gain access to that it becomes useless for the legitimate purposes that are critical to the ongoing stability and security of the Internet."), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61; Letter from David J. Redl, Assistant Secretary of Commerce for Communications and Information, to Cherine Chalaby, Chair, ICANN Board of Directors (Apr. 16, 2018) (requesting an investigation into GoDaddy's throttling of Port 43 access and masking of WHOIS information), https://www.ntia.doc.gov/files/ntia/publications/redl_to_icann_on_registrar_issues_april_2018_1.pdf. *See also* Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, IGF-USA (July 27, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-igf-usa-2018; Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 63 (Oct. 22, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-63.

[19]*See* Heather Forrest, Generic Names Supporting Organization Council Chair, *GNSO Council Launches EPDP on the Temporary Specification for gTLD Registration Data*, ICANN BLOG (July 19, 2018) (discussing launch of a "fast track" policy development process to be completed by May 25, 2019), https://www.icann.org/news/blog/gnso-council-launches-edpd-on-the-temporary-specification-for-gtld-registration-data.

[20]Göran Marby, ICANN President and CEO, *ICANN GDPR and Data Protection/Privacy Update*, ICANN (Sept. 24, 2018), https://www.icann.org/news/blog/icann-gdpr-and-data-protection-privacy-update.

[21]United States-Mexico-Canada Agreement, Art. 20.C.11(1)(b) (requiring each nation, in connection with the management of its country-code top-level domain, to provide online public access to a database of domain name registrant contact information, subject to each nation's law and, if applicable, relevant privacy and data protection policies), https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/20%20Intellectual%20Property.pdf.

In the meantime, the NTIA should support federal legislation requiring registrars and registry operators to continue providing lawful access to WHOIS data. Such access requirements could be included in stand-alone legislation or as part of a broader privacy bill. As NTIA and other domestic and foreign governmental entities continue to work with stakeholders and European officials, such legislation would set a baseline level of access; ensure that domain name providers, domain name registrants, businesses, and individuals are not subject to privacy laws with conflicting treatment of WHOIS data—at least with regard to conduct within the jurisdiction of the United States; and exercise the federal government's prerogatives regarding the application of WHOIS and privacy policy to activity with a U.S. nexus.

Legal Clarity and Flexibility to Innovate. The request for comments says that "[t]he ideal end state would ensure that organizations have clear rules that provide for legal clarity, while enabling flexibility that allows for novel business models and technologies, as well as the means to use a variety of methods to achieve consumer-privacy outcomes."[22] Establishing baseline WHOIS access through diplomatic channels, the multistakeholder process, trade agreements, and federal legislation will help achieve this end state.

First, setting such a baseline will provide legal clarity. With the dissolution[23] of the Affirmation of Commitments between ICANN and the Department of Commerce,[24] ICANN is no longer subject to a federal contractual obligation to ensure WHOIS data remains publicly accessible. And while ICANN's bylaws and policies do still include commitments to make WHOIS data accessible,[25] that, alone, has not prevented domain name registrars and registry operators from limiting WHOIS access in the face of litigation uncertainty stemming from the GDPR and ICANN's vague and overbroad Temporary Specification. For example, inconsistent implementation of ICANN's Temporary Specification and confusion among registrars and registries has impeded attempts to investigate and mitigate cyber-attacks, according to a joint

[22] *Notice and Request for Public Comments*, at 48602. *See also id.* (stating that the adopted approach should "enable innovation in the methods used to achieve [the] privacy goals" and "balance[] the needs of organizations to be agile in developing new products, services, and business models with the need to provide privacy protections to their customers.").

[23] *See* Letter from Lawrence E. Strickling, Assistant Secretary for Communication and Information, to Dr. Stephen D. Crocker, Chair, ICANN Board of Directors (Jan. 6, 2017), https://www.icann.org/en/system/files/correspondence/strickling-to-crocker-06jan17-en.pdf.

[24] Affirmation of Commitments Between the Department of Commerce and the Internet Corporation for Assigned Names and Numbers, ¶ 9.3.1 (Sept. 30, 2009) (committing "to maintain timely, unrestricted and public access to accurate and complete WHOIS information, including registrant, technical, billing, and administrative contact information"), https://www.ntia.doc.gov/node/524.

[25] *See* Bylaws for Internet Corporation for Assigned Names and Numbers, Art. 1, § 4.6(e)(i), (e)(ii) (as amended June 18, 2018) (stating that "subject to applicable laws, ICANN shall use commercially reasonable efforts to enforce its policies relating to registration directory services and shall work with Supporting Organizations and Advisory Committees to explore structural changes to improve accuracy and access to generic top-level domain registration data, as well as consider safeguards for protecting such data" and that ICANN "shall cause a periodic review to assess the effectiveness of the then current gTLD registry directory service and whether its implementation meets the legitimate needs of law enforcement, promoting consumer trust and safeguarding registrant data"), https://www.icann.org/resources/pages/governance/bylaws-en; Göran Marby, ICANN President and CEO, *Data Protection and Privacy Update—Plans for the New Year*, ICANN Blog (Dec. 21, 2017) (making "it a high priority to find a path forward to ensure compliance with the GDPR while maintaining WHOIS to the greatest extent possible"), https://www.icann.org/news/blog/data-protection-and-privacy-update-plans-for-the-new-year.

analysis of more than 300 survey responses by the Anti-Phishing Working Group and the Messaging, Malware, and Mobile Anti-Abuse Working Group.[26] Creating a clear, countervailing obligation for registrars and registry operators to provide access to WHOIS data will remove the uncertainty stemming from an overbroad application of the GDPR, and facilitate the legitimate WHOIS interests of third parties, law enforcement, and other entities. Indeed, the GDPR itself specifically allows for disclosure of data to the extent required by local law.[27]

Second, setting a baseline will help enable novel business models and technologies, as well as a variety of methods to achieve consumer-privacy outcomes. Because WHOIS data had long been publicly available prior to May 2018, requiring continued access does not create burdensome new privacy requirements on registrars, registry operators, or registrants and web-site operators that would limit their flexibility to innovate. Indeed, registrars and registry operators will continue to have flexibility in the ways that they make the WHOIS data available, so long as they work through the ICANN process and abide by their obligations. In fact, clarifying access obligations might reinvigorate stalled efforts within the ICANN community to create a next-generation WHOIS system.[28] Similarly, the mere requirement to provide a modicum of contact information will in no way chill the ability of domain name registrants and web site operators to provide innovative products and services. To the contrary, ensuring law enforcement, individuals, and businesses continue to have access to WHOIS data to find and hold accountable entities using web sites to engage in identity theft, misuse of data, and illicit activity generally will help preserve the hospitable environment necessary for individuals and businesses to engage in online commerce, prosper, and innovate. Moreover, the continued availability of WHOIS data may reduce the need for the creation of more onerous privacy requirements that could potentially chill innovation.

Comprehensive Application. The request for comments states that "[a]ny action addressing consumer privacy should apply to all private sector organizations that collect, store, use, or share personal data in activities that are not covered by sectoral laws."[29] Clarifying the WHOIS access obligations for all registrars and registry operators would be comprehensive, at least within the scope of the implementing tool. In the case of a multistakeholder process, that scope would be close to global. While a trade agreement approach or federal legislation would not have global reach, it would at least be consistent within the signatories' jurisdiction in the former case, and

[26] ANTI-PHISHING WORKING GROUP & MESSAGING, MALWARE AND MOBILE ANTI-ABUSE WORKING GROUP, ICANN GDPR AND WHOIS USERS SURVEY 4 (Oct. 2018), *available at* https://apwg.org/apwg-news-center/icann-whois-access/temporySpecSurvey and https://www.m3aawg.org/rel-WhoisSurvey2018-10.

[27] *See* General Data Protection Regulation, Ch. II, Art. 6, §§ 1(c), 3, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (allowing disclosure "for compliance with a legal obligation to which the controller is subject.").

[28] *See* MARIKA KONINGS, ICANN, GENERIC NAMES SUPPORTING ORGANIZATION COUNCIL, FINAL ISSUE REPORT ON A NEXT-GENERATION GTLD RDS TO REPLACE WHOIS 5 (Oct. 2015) (providing "specific recommendations to the questions that are the focus of the PDP, including principles for a next-generation RDS to replace WHOIS and a proposed system model"), https://whois.icann.org/sites/default/files/files/final-issue-report-next-generation-rds-07oct15-en.pdf; Policy Development Process: Next-Generation Registration Directory Service to Replace WHOIS (last visited Nov. 9, 2018) (noting that work on the next-generation WHOIS system was "indefinitely suspended" after ICANN 61 in March 2018 "in light of the uncertain status of GDPR-related work"), https://gnso.icann.org/sites/default/files/file/field-file-attach/policy-briefing-next-gen-rds-05jun18-en.pdf.

[29] *Notice and Request for Public Comments*, at 48602.

within the United States' jurisdiction in the later. Regardless, any of these approaches would be an improvement over the inconsistent status quo.

Risk- and Outcome-Based Approach. The request for comments states that "[i]nstead of creating a compliance model that creates cumbersome red tape—without necessarily achieving measurable privacy protections—the approach to privacy regulations should be based on risk modeling and focused on creating user-centric outcomes."[30] Clarifying WHOIS access requirements would simply restore obligations that registrars and registry operators have long operated under. Domain name registrants, too, have long been on notice they must provide certain information that will be publicly disclosed, and that such information may be used for matters of public safety, consumer protection, law enforcement, dispute resolution, and enforcement of rights.[31] Consequently, clarifying the requirement would not create cumbersome new red tape. Rather, it would re-establish on more solid footing a tool that, as discussed above, serves the user-focused, privacy-related outcomes of promoting online transparency; putting consumers in a better position to control, minimize, secure, and correct data collected about them, as well as to mitigate harm of disclosure; and helping hold accountable those who use web sites to engage in misuse of personal data and illicit activity generally. And it does so without adding to "long, legal, regulatory-focused privacy policies and check boxes."[32] In this way, requiring continued access to WHOIS data is "reasonable and appropriate to the context."[33] Only information used to contact a domain name registrant and relevant administrative and technical representatives is collected, disclosure only occurs upon a query to a WHOIS database, and the purpose is consumer protection, online security, and rights enforcement. Many privacy laws, if not most, include provisions allowing access to information for these types of purposes because of their importance.[34]

For much the same reasons, a risk analysis weighs in favor of restoring such an obligation. In the absence of the requirement, individuals and businesses would face an increased risk of privacy-related or other harms as a result of having a harder time finding domain name registrants and web site operators. By contrast, registrars, registry operators, registrants, and web site operators would see little increased risk from the requirement, as they have long been subject to such an obligation. In fact, registrars and registry operators would see a diminished privacy litigation risk as a result of a clear obligation to provide access that would provide a defense against any claims of a GDPR violation, and in the case of federal legislation pre-empt any contradictory state privacy law. The risk to registrants is also comparatively small, as they, too, have long operated with these types of obligations and the information they must provide is relatively mundane data used to contact them. Registrants of domain names used for commercial purposes

[30] *Id.*

[31] *See* Internet Corporation for Assigned Names and Numbers, History of WHOIS, https://whois.icann.org/en/history-whois (last accessed Oct. 26, 2018) (stating that "WHOIS traces its roots to 1982, when the Internet Engineering Task Force published a protocol for a directory service for ARPANET users. ... As the Internet grew, WHOIS began to serve the needs of different stakeholders such as domain name registrants, law enforcement agents, intellectual property and trademark owners, businesses and individual users.").

[32] *Notice and Request for Public Comments*, at 48601.

[33] *Id.*, at 48601.

[34] *See, e.g.*, Gramm-Leach-Bliley Act, Pub. L. No. 106-102, § 502(e)(3), 113 Stat. 1338, 1438-39 (1999) (allowing disclosure to prevent fraud or unauthorized transactions or for public safety), https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf.

can provide business contact data, rather than more personal data, and can be reasonably expected to share information in light of the commercial nature of their activity. Individuals, too, have existing techniques and tools to prevent abuse of the data by third parties.

Interoperability. The request for comments states that "the internet-enabled economy depends on personal information moving seamlessly across borders," but because "governments approach consumer privacy differently," there is a "need for mechanisms to bridge differences, while ensuring personal data remains protected."[35] The WHOIS system, by its nature, is designed to provide for the interoperable flow of domain name data. And, as discussed above, a clear obligation to continue to provide WHOIS access may reinvigorate ICANN processes to create a next-generation system, which could further advance interoperability. Moreover, while the hope is that efforts to ensure WHOIS data remains available globally will succeed, the WHOIS system might be designed to reflect different privacy regimes in different countries, if necessary.

FTC Enforcement. The request for comments states that "the FTC is the appropriate federal agency to enforce consumer privacy."[36] Legislation requiring registrars and registry operators to continue making WHOIS information available could make the FTC the enforcing agency.

## Conclusion

Continuing access to WHOIS data will advance the NTIA's objectives for a federal privacy approach. By aiding transparency and accountability, access to WHOIS information helps create reasonably informed users, empowered to meaningfully express privacy preferences over data collection, and helps them control, minimize, secure, correct, and mitigate harmful exposure of the data collected about them. Such continued access would also help harmonize the WHOIS regulatory landscape, aid legal clarity without reducing flexibility, be comprehensive, facilitate interoperability and data flows, and help promote innovation by creating a hospitable environment for online commerce and communications. It would be consistent with a risk- and outcome-based approach, as it would not create cumbersome new burdens, and the data collection is reasonable and appropriate to the objectives of combating identity theft, misuse of data, cyber-attacks, and illicit conduct generally. The WHOIS system is also capable of aiding interoperability to enable the flow of data. Lastly, federal legislation in this area could be crafted to rely on FTC enforcement.

The European Union should not be setting U.S. WHOIS and privacy policy. Moreover, with growing concerns over illicit behavior on the internet, now is the time to increase online transparency, accountability, and trust—not diminish it. The MPAA therefore asks that the federal privacy approach prioritize efforts to ensure that certain basic WHOIS information remains publicly available, and that any information that the GDPR does require to be removed from public access still be available to third parties with legitimate interests through a reasonable, timely, and effective process. Such efforts should include Administration support for solutions through the multistakeholder process, for ICANN assumption of WHOIS under a unified access model, for WHOIS access requirements in trade agreements, and for federal legislation requiring registrars and registry operators to continue providing lawful access.

[35] *Notice and Request for Public Comments*, at 48602.
[36] *Id.*