Before the
Federal Trade Commission
Washington, D.C. 20580

In the Matter of	)	
	)	
Competition and Consumer Protection in the 21st Century	)	Project Number P181201
	)	
	)	
Hearing #12: April 9-10, 2019 The FTC's Approach to Consumer Privacy	)	Docket ID: FTC-2018-0098

Comments of the Motion Picture Association of America, Inc.

Submitted April 8, 2019

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

Overview

As the FTC examines gaps in current legal and self-regulatory privacy frameworks, the MPAA asks the Commission to address diminished access to WHOIS information.[1] In particular, the MPAA requests that the FTC continue urging the Internet Corporation for Assigned Names and Numbers to expeditiously adopt and implement an access and accreditation model restoring the availability of WHOIS information to protect consumers and legitimate commerce, including to combat copyright infringement. The MPAA also asks the FTC to help ensure domain name providers diligently review and grant requests for such access until the model is implemented.

Absent reasonable and timely access to WHOIS information, which contains basic contact data for holders of internet domain names, the FTC and others will lose many of the benefits of a tool that the Commission has long described as fundamental to protecting consumer privacy and to rooting out unfair and deceptive trade practices. WHOIS information has been publicly available since the founding of the commercial internet and virtually all efforts to combat illegal conduct online—such as identity theft, theft of intellectual property, fraud, cyber-attacks, illicit sale of opioids, and human trafficking—begin with an examination of WHOIS information.

WHOIS access is now subject to certain privacy laws, such as the European Union's General Data Protection Regulation. Privacy laws typically include provisions that would allow the continued availability of WHOIS information, and the GDPR is no different. Misapplication of the GDPR, however, has led domain name providers to restrict WHOIS access, even when and where the GDPR does not apply. This is compromising efforts to protect consumers and legitimate commerce. For example, two-thirds of 55 global law enforcement agencies surveyed no longer find that the WHOIS system meets their investigative needs, according to a recent presentation by the FTC's international consumer protection counsel.

ICANN has been seeking to resolve the WHOIS issue for more than a year. Successful completion of ICANN's self-regulatory policy development process and implementation of an access and accreditation model could ensure that WHOIS information for domestic and foreign web sites remains available for legitimate purposes in the United States and around the world. Absent a greater sense of urgency, however, finishing that development and implementation may take another year or more and, even then, fall well short of solving the problem. Every day that domain name providers unnecessarily limit access to WHOIS information puts consumers and legitimate commerce at increased risk. With all that is happening on the internet, now is not the time for reduced online transparency and accountability. Privacy regimes should protect consumers, not criminals. Indeed, the GDPR itself dictates a balance between privacy protection and third-party access to information for legitimate purposes.

If ICANN fails to adopt and implement an access and accreditation model expeditiously, and domain name providers do not continue providing WHOIS access in the meantime, the need to protect U.S. citizens and legitimate commerce may give Congress no choice but to mandate that domain name providers with a significant U.S. nexus continue making WHOIS information available. In such a circumstance, the MPAA hopes the FTC and other agencies will support such a legislative effort. Establishing a 21st century framework to prevent threats to consumer privacy will do little good if the perpetrators cannot be found in the first place.

---

[1]The MPAA is the voice of the American film and television industry, and represents Walt Disney Studios, Netflix Studios, Paramount Pictures, Sony Pictures, Universal City Studios, and Warner Bros. Entertainment.

I. Background

In the supporting materials for its hearing on "The FTC's Approach to Consumer Privacy," the Commission observes that a lot has happened since the agency last engaged in a comprehensive evaluation of data privacy issues, pointing to significant changes in technologies and business models.[2] The Commission also notes that some jurisdictions have adopted new approaches to privacy, including the European Union's April 2016 passage of the GDPR, which became effective in May 2018.[3] Pointing to the daily online privacy controversies occupying headlines and public debate, the Commission comments that "questions abound" about "the adequacy of exiting legal and self-regulatory frameworks to protect consumers from [privacy] harms without unduly restraining legitimate business activity."[4]

Contributing to those questions is domain name providers' restriction of access to WHOIS information following ICANN's May 2018 adoption of a temporary specification under the stated goal of complying with the GDPR.[5] The denial of critical information needed for the FTC and others to investigate and combat illicit activity online is just the sort of "limitation[] to the FTC's authority to protect consumers' privacy" that the agency seeks comment on.[6]

WHOIS information has been publicly available since the beginning of the commercial internet, and domain name registrants have long been on notice that such information may be used for consumer protection, law enforcement, dispute resolution, and enforcement of rights—including IP rights.[7] WHOIS access forms the basis of online transparency, security, and accountability.[8] It is necessary to protect consumer privacy, ensure public safety, and promote lawful commerce.[9] As FTC Bureau of Consumer Protection Director Howard Beale explained in 2002 congressional testimony about the investigative and enforcement uses of WHOIS information:

---

[2] *See* FTC Hearing #12: The FTC's Approach to Consumer Privacy, *Hearings on Competition and Consumer Protection in the 21st Century*, at 2, https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019 (last visited April 8, 2019).

[3] *See id.*

[4] *See id.*

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

[6] *See FTC Hearing #12*, at 4.

[7] *See* ICANN, History of WHOIS (stating that "WHOIS traces its roots to 1982, when the Internet Engineering Task Force published a protocol for a directory service for ARPANET users. Initially, the directory simply listed the contact information that was requested of anyone transmitting data across the ARPANET. 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. But the protocol remained fundamentally based on those original IETF standards. This is the WHOIS protocol that ICANN organization inherited when it was established in 1998."), https://whois.icann.org/en/history-whois (last visited Apr. 8, 2019).

[8] *See* Letter from David J. Redl, Assistant Secretary of Commerce for Communications and Information, to Cherine Chalaby, Chair, ICANN Board of Directors (April 4, 2019) (stating that "WHOIS information is a critical tool that helps keep people accountable for what they do and put online").

[9] *See id.* (stating that "[l]aw enforcement uses WHOIS to shut down criminal enterprises and malicious web sites. Cybersecurity researchers use it to track bad actors. And it is the first line in the defense of intellectual property protection").

> There is real danger that the benefits of the Internet may not be fully realized if consumers identify the Internet with fraud operators. We need to act quickly to stop fraud, both to protect consumers and to protect consumer confidence in e-commerce.[10]

Individuals and businesses rely on WHOIS information to verify that the online entities they communicate and transact with are who they say they are.[11] The knowledge that such information is available either before or after a problem arises is important in building trust in the internet ecosystem, even among users who do not anticipate searching the WHOIS information. This makes it essential to promoting legitimate commerce and competition online.

Law enforcement agencies and others rely on WHOIS to combat illegal conduct online, such as identity theft, theft of intellectual property, fraud, spread of malware, cyberattacks, illicit sale of opioids, and human trafficking.[12] Indeed, the FTC has long emphasized that "[i]n all of [the agency's] investigations against Internet companies, one of the first tools FTC investigators use to find wrongdoers is the Whois database [because the Commission] cannot easily sue fraudsters if [it] cannot find them."[13] A recent DOJ cyber report similarly states that "[t]he first step in online reconnaissance often involves use of the Internet Corporation for Assigned Names and Numbers' WHOIS database."[14]

Unfortunately, the temporary specification ICANN adopted is resulting in unnecessarily restricted access to important WHOIS information well beyond what the GDPR mandates, not just in Europe, but also in the United States and elsewhere.[15] The GDPR does not apply at all to non-personal information;[16] and even in the case of personal information, the regulation calls for a balancing between limiting access to protect privacy and disclosing information for legitimate interests[17] such as public safety, law enforcement and investigation, enforcement of rights or a

---

[10]*See e.g., Accuracy and Integrity of the "WHOIS" Database: Hearing Before the Subcomm. on Courts, the Internet, & Intellectual Property of the H. Comm. on the Judiciary*, 107th Cong. (May 22, 2002), Statement of Howard Beales, Director, FTC Bureau of Consumer Protection, at 2, https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-whois-datebase/whois.pdf.

[11]*Cf.* Jon Leibowitz, Commissioner, FTC, Prepared Statement of the Federal Trade Commission Before the Internet Corporation for Assigned Names and Numbers Meeting Concerning Whois Databases 7 (June 26, 2006) (stating that "[w]here a website does not contain contact information, consumers can go to the Whois databases and find out who is operating the website. This can help consumers resolve problems with online merchants directly, without the intervention of law enforcement authorities").

[12]*See, e.g.*, Letter to the U.S. Congress from 32 Organizations, March 14, 2019 (stating "that recent policy changes have effectively blocked access to this critical data set" and that "WHOIS data is critical to law enforcement, consumer protection agencies, child advocacy groups, anti-human trafficking organizations, cybersecurity investigators, intellectual property rightsholders, journalists, academics and others"), https://secureandtransparent.org/wp-content/uploads/2019/03/WHOIS-Cyber-Support-Letter-3-14-19.pdf.

[13]*Accuracy and Integrity of the "WHOIS" Database*, Statement of Howard Beales, at 3-4.

[14]DOJ, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 35 (July 2018), https://www.justice.gov/ag/page/file/1076696/download.

[15]*See, e.g., Letter to the U.S. Congress from 32 Organizations*.

[16]*See* GDPR, art. 1 (describing the subject matter and objectives of the regulation as relating to the processing and protection of personal data), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

[17]*See id.*, recital (4) (stating that "[t]he processing of personal data should be designed to serve mankind. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society

contract, fulfillment of a legal obligation, cybersecurity, and preventing fraud.[18] Moreover, the GDPR does not apply to American registrars and registries with respect to domain name registrations by U.S. registrants, or where domain name registrants and registrars are located outside the European Economic Area.[19] Furthermore, it applies only to information about "natural persons," and so imposes no obligation to obfuscate information about domain name registrants that are companies, businesses, or other legal entities, irrespective of the nationality or principal place of business of such entities.[20]

The FTC states in its request for comment that "the current approach [to privacy] needs to be examined in light of potential gaps in the Commission's existing authority, as well as new risks, new opportunities, and new knowledge."[21] According to the Commission, "[r]elevant questions include whether current approaches sufficiently protect consumer privacy; whether certain approaches may have unintentionally hindered innovation, growth, or competition, to the detriment of consumers and the economy; whether other approaches might better serve consumers and competition; and, if so, what those approaches should be."[22]

---

and be balanced against other fundamental rights, in accordance with the principle of proportionality"). *See also Joint Statement of the Governmental Advisory Committee and the At-Large Advisory Committee on the Expedited Policy Development Process at the ICANN64 Community Forum in Kobe, Japan* (Mar. 13, 2019) (stating that the GDPR "protects the privacy of natural persons *and allows for the processing of and access to data for legitimate purposes*") (emphasis added), https://atlarge.icann.org/advice_statements/13255.

[18]*See* GDPR, arts. 2(2)(d), 5(1)(b), 6, 23. *See also* ICANN, GOVERNMENTAL ADVISORY COMMITTEE, *Communiqué—San Juan, Puerto Rico* (Mar. 15, 2018) (stating that the GDPR allows for access to information for legitimate purposes), https://gac.icann.org/advice/communiques/20180315_icann61%20gac%20communique_finall.pdf.

[19]*See* GDPR, arts. 2(2)(a), 3.

[20]*See id.*, art. 1 (describing the subject matter and objectives of the regulation as relating to the protection of natural persons). *See also GAC San Juan Communiqué* (stating that the GDPR applies only to the privacy of natural persons, not legal entities); *Joint Statement of the Governmental Advisory Committee and the At-Large Advisory Committee* (stating that "[t]he GDPR only applies to personal data of natural persons and therefore does not regulate the processing of the data of legal persons"). *Cf. Accuracy and Integrity of the "WHOIS" Database: Hearing Before the Subcomm. on Courts, the Internet, & Intellectual Property of the H. Comm. on the Judiciary*, 107th Cong. (May 22, 2002), Statement of Howard Beales, Director, FTC Bureau of Consumer Protection, at 7 (stating that "[f]or commercial websites, [the FTC] believes the balance weighs in favor of public disclosure of basic registrant contact information. Once a company decides to sell products on the Internet, it should be accountable to the public so that the public can determine who the company is and where it operates from"), https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-whois-datebase/whois.pdf; Jon Leibowitz, Commissioner, FTC, Prepared Statement of the Federal Trade Commission Before the Internet Corporation for Assigned Names and Numbers Meeting Concerning Whois Databases 9 (June 26, 2006) (stating that the FTC "has always recognized that non-commercial registrants may require some privacy protection from *public* access to their contact information, without compromising appropriate real-time access by law enforcement agencies" and that "[r]estricting public access to Whois data for commercial websites and depriving the public of the ability to find information about such websites would contravene well-settled international principles"), https://www.ftc.gov/system/files/documents/public_statements/417701/p035302whoisdatabases.pdf.

[21]*See* FTC Hearing #12: The FTC's Approach to Consumer Privacy, *Hearings on Competition and Consumer Protection in the 21st Century*, at 2, https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019 (last visited Apr. 8, 2019).

[22]*See id.*

Diminished WHOIS access represents a gap in the Commission's authority, creating a new risk that the FTC (and others) will have difficulty obtaining information needed to investigate and combat unlawful conduct online. This indicates that current approaches do not sufficiently protect consumer privacy or promote lawful commerce, and that the GDPR is unintentionally hindering both. The result is a chill on innovation, growth, and competition to the detriment of consumers and the economy. The issue warrants FTC attention in its review of consumer privacy, especially in light of the agency's apparent concern over its available resources. Indeed, the Commission has dedicated two panels at the April 9-10 hearing to the question: "Is the FTC's Current Toolkit Adequate?"[23] Without access to WHOIS information, that toolkit is lacking.

The FTC asks whether "privacy protections [should] depend on the sensitivity of the data."[24] The answer is, of course, "yes." The information at issue here is basic contact data that domain name registrants have been providing since the dawn of the commercial internet. They have known it would be publicly available, and so have had little expectation of privacy over it. When balanced against the need to curb threats to the privacy of others (such as from spyware and phishing),[25] as well as to combat fraud, defend against cyber-threats, and fight other illicit conduct online, the analysis weighs in favor of disclosure. Additionally, making WHOIS information available to help find culprits can reduce the need for anticipatory regulation, whether aimed at particular individuals and entities gathering data, or the social networks whose facilities and services they use. This is particularly worth mentioning in light of the FTC's query about "the tradeoffs between *ex ante* regulatory and *ex post* enforcement approaches to privacy protection."[26]

II. The Need for ICANN to Restore WHOIS Access, and the Appropriateness of Legislation Should Such Efforts Fail

Because of the importance of WHOIS access, the MPAA asks the Commission—as a member of ICANN's Governmental Advisory Committee—to continue urging ICANN to expeditiously adopt and implement an access and accreditation model restoring the availability of WHOIS information to protect consumers and legitimate commerce, including to combat copyright infringement. The MPAA also asks the FTC to help ensure that domain name providers diligently review and grant requests for such access in the meantime, as is required by the "reasonable access" requirement in ICANN's temporary specification.[27] Domain name providers'

[23] *Id.* (providing a link to the agenda, which includes two April 10 panels on the FTC's "toolkit").

[24] *See id.*, at 3.

[25] *See, e.g.*, Jon Leibowitz, Commissioner, FTC, Prepared Statement of the Federal Trade Commission Before the Internet Corporation for Assigned Names and Numbers Meeting Concerning Whois Databases 4-5, 10 (June 26, 2006) (noting that the FTC relies on WHOIS information to combat spyware and phishing, and stating that "the existing availability of Whois databases can actually help enforcement agencies find out who is violating privacy laws and, consequently, help prevent the misuse of consumers' personal information"), https://www.ftc.gov/system/files/documents/public_statements/417701/p035302whoisdatabases.pdf.

[26] *See* FTC Hearing #12: The FTC's Approach to Consumer Privacy, *Hearings on Competition and Consumer Protection in the 21st Century*, at 3, https://www.ftc.gov/news-events/events-calendar/ftc-hearing-competition-consumer-protection-21st-century-february-2019 (last visited Apr. 8, 2019).

[27] *See* ICANN, TEMPORARY SPECIFICATION FOR GTLD REGISTRATION DATA appx. A, § 4.1 (May 25, 2018) (stating that a "Registrar and Registry Operator MUST provide reasonable access to Personal Data in Registration Data to third parties on the basis of a legitimate interests pursued by the third party, except where such

failure to do so is contrary to the GDPR's provisions allowing disclosure of even sensitive personal information for legitimate purposes.[28] Legitimate purposes for disclosure include law enforcement, combating cyber-crime, curbing fraud and threats to consumer privacy, and protecting intellectual property.[29] If ICANN does not expeditiously adopt and implement an access and accreditation model that recognizes such legitimate interests, or if domain name providers do not provide reasonable access for such purposes in the meantime, the U.S. Congress may have no choice but to mandate that domain name providers provide such access if they are doing business in the United States, registering domain names for people or businesses in the United States, or registering domain names used to market or sell goods or services to people in the United States.

FTC Consumer Protection Bureau Chief Howard Beales testified before Congress in 2002 that "it is hard to overstate the importance of accurate Whois data to [the agency's] Internet investigations,"[30] a sentiment the agency has continued to echo through the years.[31] Beales explained that:

> Because fraudulent website operators can defraud consumers quickly and disappear quickly, [the FTC needs] to move just as quickly to find them and stop them. The Whois database—when it is accurate—can help law enforcers quickly identify wrongdoers and their location, halt their conduct, and preserve money to return to defrauded consumers.[32]

The FTC uses WHOIS information, for example, to identify where a perpetrator is located, to serve process, to get investigative leads, and to conduct "surfs" of the internet for potentially false or deceptive advertising for a targeted product or service.[33] The importance of WHOIS access to the FTC led then-FTC Commissioner Jon Leibowitz to tell ICANN in 2006 that "Whois databases should be kept open, transparent, and accessible so that agencies like the FTC can

---

interests are overridden by the interests or fundamental rights and freedoms of the Registered Name Holder or data subject pursuant to Article 6(1)(f) GDPR"), https://www.icann.org/resources/pages/gtld-registration-data-specs-en.

[28] *See* GDPR, art. 6(1)(f).

[29] *See* ICANN, GOVERNMENTAL ADVISORY COMMITTEE, *Communiqué—San Juan, Puerto Rico* (Mar. 15, 2018), https://gac.icann.org/advice/communiques/20180315_icann61%20gac%20communique_finall.pdf; Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 61 (Mar. 12, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61.

[30] *Accuracy and Integrity of the "WHOIS" Database: Hearing Before the Subcomm. on Courts, the Internet, & Intellectual Property of the H. Comm. on the Judiciary*, 107th Cong. (2002), Statement of Howard Beales, Director, FTC Bureau of Consumer Protection, at 3-4, https://www.ftc.gov/sites/default/files/documents/public_statements/prepared-statement-federal-trade-commission-whois-datebase/whois.pdf.

[31] *See, e.g.*, Jon Leibowitz, Commissioner, FTC, Prepared Statement of the Federal Trade Commission Before the Internet Corporation for Assigned Names and Numbers Meeting Concerning Whois Databases 4 (June 26, 2006) https://www.ftc.gov/system/files/documents/public_statements/417701/p035302whoisdatabases.pdf.

[32] *Accuracy and Integrity of the "WHOIS" Database*, Statement of Howard Beales, Director, FTC Bureau of Consumer Protection, at 2.

[33] MANEESHA MITHAL, FTC CONSUMER PROTECTION BUREAU, ICANN PRESENTATION ENTITLED "HOW THE FTC USES WHOIS DATA," at 4-7 (June 2003), https://www.icann.org/en/system/files/files/mithal-whois-workshop-24jun03-en.pdf.

continue to protect consumers, and consumers can continue to protect themselves."[34]

Misapplication of the GDPR, which has resulted in inappropriate and unnecessary restriction of WHOIS access, is already harming consumer protection, public safety, and cybersecurity, as government entities, the private sector, and public interest groups have been warning for more than a year.[35] Indeed, the DOJ has expressed concern that "the GDPR may be interpreted to impede the ability of law enforcement authorities to obtain data critical for their authorized criminal and civil law enforcement activities."[36] The U.S. Commerce Department has also been outspoken about the value of WHOIS information to governments, businesses, intellectual property owners, and individual internet users across the globe, and has conveyed the concern of the United States about the lack of certainty around access to WHOIS information for legitimate purposes.[37]

Unfortunately, these fears have been realized. For example, according to an analysis by two cybersecurity working groups of more than 300 survey responses, misapplication of the GDPR is impeding attempts to investigate cyber-attacks by resulting in delayed or denied access to WHOIS information, and less useful information even when access is granted.[38] A survey of 55 global law enforcement agencies by ICANN's Public Safety Working Group reveals that 98 percent found the WHOIS system aided their investigative needs before ICANN's temporary specification took effect, as compared to 33 percent after, according to a presentation by the FTC's own counsel for international consumer protection.[39] An analysis by internet security expert Dave Piscitello indicates that the inability to access WHOIS data is harming the ability of commercial, public, and government IT administrators to identify cyber-attackers and block them from their networks.[40] And brand protection firm MarkMonitor has documented how restricted WHOIS access is hindering IP protection efforts.[41]

---

[34]Jon Leibowitz, Commissioner, FTC, Prepared Statement of the Federal Trade Commission Before the Internet Corporation for Assigned Names and Numbers Meeting Concerning Whois Databases 12 (June 26, 2006), https://www.ftc.gov/system/files/documents/public_statements/417701/p035302whoisdatabases.pdf.

[35]*See e.g.*, ICANN, GOVERNMENTAL ADVISORY COMMITTEE, *Communiqué—San Juan, Puerto Rico* (Mar. 15, 2018), https://gac.icann.org/advice/communiques/20180315_icann61%20gac%20communique_finall.pdf; Letter from more than 50 national and international organizations, trade associations, companies and non-profit entities to Article 29 Working Party, European Commission (March 5, 2018), https://www.icann.org/en/system/files/files/gdpr-comments-sheckler-et-al-article-29-wp-whois-05mar18- en.pdf.

[36]DOJ, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 115 (July 2, 2018), https://www.justice.gov/ag/page/file/1076696/download.

[37]*See, e.g.*, Remarks of David J. Redl, Assistant Secretary of Commerce for Communications and Information, ICANN 61 (Mar. 12, 2018), https://www.ntia.doc.gov/speechtestimony/2018/remarks-assistant-secretary-redl-icann-61.

[38]ANTI-PHISHING WORKING GROUP AND MESSAGING, MALWARE AND MOBILE ANTI-ABUSE WORKING GROUP, ICANN GDPR AND WHOIS USERS SURVEY (Oct. 18, 2018), http://docs.apwg.org/reports/ICANN_GDPR_WHOIS_Users_Survey_20181018.pdf.

[39]Laureen Kapin, FTC Counsel for International Consumer Protection & Co-Chair, ICANN Public Safety Working Group, ICANN63 GAC Plenary Meeting 8 (Oct. 23, 2018), https://gac.icann.org/presentations/icann63%20pswg.pdf.

[40]*See* Dave Piscitello, Blog, *Facts & Figures: Whois Policy Changes Impair Blocklisting Defenses*, THE SECURITY SKEPTIC (March 8, 2019), https://securityskeptic.typepad.com.

[41]*See* Statton Hammock, *GDPR and WHOIS: Adverse Impacts on Brand Protection*, Mark Monitor Blog (Oct. 22, 2018), https://www.markmonitor.com/mmblog/gdpr-and-whois-adverse-impacts-on-brand-

ICANN's temporary WHOIS specification will expire in May 2019. In anticipation of that expiration, ICANN launched an "expedited policy development process" to examine whether to adopt the temporary specification as a consensus policy, either "as is" or with modifications. Troublingly, the Expedited Policy Development Process team released a final report February 20, 2019, on a proposal that would compound matters by:

- perpetuating the misapplication of the GDPR to legal persons;
- continuing to reach beyond the jurisdiction of the GDPR; and
- allowing for further redaction or complete removal of important WHOIS data fields, including organization, technical contact, and administrative contact.[42]

Perhaps of most concern, the report fails to explicitly articulate that consumer protection, domain name abuse, IP protection, and investigation of cybercrime are legitimate purposes for collection of and access to WHOIS information, choosing instead to defer those issues to a "Phase 2" for future discussion under an unspecified timeline.[43] In evaluating the proposal, the Governmental Advisory Committee stated that the recommendation:

> risks creating a new registration directory service that does not collect, publish, nor allow for lawful disclosure of sufficient information and provide adequate procedures necessary for promoting 1) the security and stability of the [domain name system], 2) user confidence in the Internet, and 3) quick and efficient mitigation of malicious conduct.[44]

An ICANN subgroup nonetheless voted March 4 to adopt the report and revised policy and to send it to the ICANN Board for consideration.[45] This prompted the Governmental Advisory Committee to issue another statement emphasizing:

> the necessity of finding a swift solution to ensuring timely access to non-public registration data for legitimate third party purposes that complies with the requirements of the GDPR and other data protection and privacy laws, in view of the significant negative impact of the changes in WHOIS accessibility on users with legitimate purposes. The GAC has

---

protection?cid=gdprblog030919; Brian King, *GDPR, WHOIS and impacts to brand protection: Nine months later*, MarkMonitor Blog (March 10, 2019), https://www.markmonitor.com/mmblog/gdpr-whois-and-impacts-to-brand-protection-nine-months-later.

[42] *See* ICANN, GENERIC NAMES SUPPORTING ORGANIZATION, FINAL REPORT OF THE TEMPORARY SPECIFICATION FOR GTLD REGISTRATION DATA EXPEDITED POLICY DEVELOPMENT PROCESS (Feb. 20, 2019), https://gnso.icann.org/sites/default/files/file/field-file-attach/epdp-gtld-registration-data-specs-final-20feb19-en.pdf.

[43] *See id.*

[44] ICANN, GOVERNMENTAL ADVISORY COMMITTEE, GOVERNMENTAL ADVISORY COMMITTEE INPUT ON THE DRAFT FINAL REPORT OF THE EXPEDITED POLICY DEVELOPMENT PROCESS (EPDP) ON GTLD REGISTRATION DATA 1 (Feb. 20, 2019), https://mm.icann.org/pipermail/gnso-epdp-team/attachments/20190220/54940282/epdp-draftfinal-report-revisedgac-Input-20feb19-final-0001.pdf.

[45] ICANN, *GNSO Council Adopts EPDP Final Report on the Temporary Specification for gTLD Registration Data* (March 4, 2019), https://www.icann.org/news/announcement-2019-03-04-en.

previously noted that such legitimate purposes include civil, administrative and criminal law enforcement, cybersecurity, consumer protection and IP rights protection.[46]

The law enforcement, cybersecurity, intellectual property, and public safety communities have been warning about the problem with restricting WHOIS access for more than a year now, yet ICANN appears poised to advance a policy that does not yet create a clear, consistent, and timely means for accessing WHOIS information for legitimate purposes. Every day that passes without a delineated process in place for reliable access to WHOIS information decreases the ability to prevent or remedy unlawful behavior online, and increases the risks to consumers and legitimate commerce. A deadline for concluding Phase 2 work and a practical yet expeditious timeline are both necessary to effectively move the process forward.[47]

In that vein, the U.S. Commerce Department sent ICANN a letter April 4 stating that "[n]ow is the time to deliberately and *swiftly* create a system that allows for third parties with legitimate interests, like law enforcement, IP rights holders, and cybersecurity researchers to access non-public data critical to fulfilling their missions."[48] The letter added that the U.S. government is expecting ICANN to "achieve substantial progress, if not completion, in advance of ICANN's meeting in Montreal in November," and observed that "[w]ithout clear and meaningful progress, alternative solutions such as calls for domestic legislation will only intensify and be considered."[49]

In addition to providing exceptions for compliance with a legal obligation or to protect vital or public interests, the GDPR allows for disclosure in accordance with the local law of E.U. member states.[50] The United States is no less entitled than any European nation to such self-determination, especially since it is not a European Union member bound by the GDPR in the first place. Should ICANN fail to expeditiously restore reasonable and timely WHOIS access for the legitimate purposes of the law enforcement, consumer protection, intellectual property, cybersecurity, and public safety communities, the U.S. Congress may have no choice but to legislate to ensure that the FTC and others can continue to protect consumers and promote legitimate commerce.

---

[46]ICANN, GOVERNMENTAL ADVISORY COMMITTEE, *Communiqué—Kobe, Japan*, at 9-10 (Mar. 14, 2019), https://gac.icann.org/contentMigrated/icann64-kobe-communique.

[47]See *Joint Statement of the Governmental Advisory Committee and the At-Large Advisory Committee on the Expedited Policy Development Process at the ICANN64 Community Forum in Kobe, Japan* (Mar. 13, 2019) (stating that "a model for disclosure is equally as important to address expeditiously as the Phase 1 activity. We urge the EPDP to develop practical yet expeditious timelines, including a deadline in which to conclude the Phase 2 work").

[48]*See* Letter from David J. Redl, Assistant Secretary of Commerce for Communications and Information, to Cherine Chalaby, Chair, ICANN Board of Directors (April 4, 2019). Such prodding is additionally warranted in light of calls from some ICANN stakeholders to slow the process down. *See* ICANN TRANSCRIPTION, SPECIAL GENERIC NAMES SUPPORTING ORGANIZATION COUNCIL MEETING at 27, 28, 30-31 (March 4, 2019) (reflecting comments such as "Many of our current representatives are happy to continue in Phase 2 but only if the tempo is reduced significantly"; "I honestly would like to ask if there is any earthly reason why we are taking the same pace as Phase 1. … I understand that that was warranted by the tight deadline [for Phase 1] and expiry date of the temporary specification. … So I believe there is no reason to go to toil, tears and sweat in the second phase. I think that this should be slowed down"; "We certainly can't work at the same pace as the EPDP did and there's no need to do that here as well; we don't have the, you know, deadline staring us down"), https://gnso.icann.org/sites/default/files/file/field-file-attach/transcript-special-council-04mar19-en.pdf.

[49]*See Letter from David J. Redl to Cherine Chalaby.*

[50]*See* GDPR, art. 6(1)-(3).

Conclusion

Reduced access to WHOIS information—resulting from a misapplication of the GDPR—is hindering the ability of the FTC and others to combat threats to consumer privacy, to protect public safety, and to promote legitimate commerce. Although ICANN is seeking a comprehensive, self-regulatory solution to this problem, there is reasonable concern that such a solution will not arrive expeditiously, as well as a risk that—if and when it does arrive—it will not sufficiently resolve the matter. In the meantime, domain name providers are not providing reasonable access to WHOIS data for legitimate purposes, as required by ICANN's temporary specification.

The MPAA therefore asks the FTC to continue prodding ICANN to quickly implement an access and accreditation model that restores reasonable and timely WHOIS access for the legitimate purposes of the law enforcement, consumer protection, intellectual property, cybersecurity, and public safety communities, and to press domain name providers to grant reasonable and timely access in the interim. In the event ICANN and domain name providers fail to do so, the U.S. Congress is well within its prerogatives to pass legislation preserving access to WHOIS information to protect its citizens and promote legitimate commerce. Because of the importance of continued access to WHOIS information to the FTC and others, the MPAA asks the FTC and other agencies to support legislative efforts if such circumstances come to pass.