Comments to ICANN on
The GNSO's Initial Privacy & Proxy Services
Accreditation Issues Working Group Report

by Center for Democracy & Technology,
New America's Open Technology Institute,
and Public Knowledge

I. Intro/Background

The Center for Democracy & Technology, New America's Open Technology Institute, and Public Knowledge respectfully submit these comments to the Internet Corporation for Assigned Names and Numbers (ICANN) in response to the Initial Report from the Generic Names Supporting Organization's (GNSO) Policy Development Process Working Group on issues relating to the accreditation of privacy and proxy service providers.[1]

The Center for Democracy & Technology (CDT) is a nonprofit public interest advocacy organization that works to advance human rights online, and is committed to finding forward-looking and technically sound solutions to the most pressing challenges facing users of electronic communications technologies. With expertise in law, technology, and policy, CDT promotes policies that protect and respect users' fundamental rights to privacy and freedom of expression, and enhance their ability to use communications technologies in empowering ways.

New America is a nonprofit, nonpartisan public policy institute based in Washington DC that invests in new thinkers and new ideas to address the next generation of challenges facing the United States and the global community. The

[1] *Initial Report on the Privacy & Proxy Services Accreditation Issues Policy Development Process*, Submitted to ICANN's Generic Names Support Organization's Council on May 5, 2015, https://gnso.icann.org/en/issues/raa/ppsai-initial-05may15-en.pdf [hereinafter Initial Report].

Open Technology Institute is a program within New America that promotes affordable, universal access to open and unrestricted communications networks through technology development, applied learning, and policy reform.

Public Knowledge is a nonprofit public interest organization promoting freedom of expression, an open Internet, and access to affordable communications tools and creative works. Public Knowledge works to shape policy on behalf of the public interest at the intersection of intellectual property, telecommunications, and Internet law.

All three of our organizations work on human rights issues and support the preservation of anonymous and pseudonymous speech online. We submit these comments and associated recommendations in support of anonymous and pseudonymous speech exercised by domain registrants using privacy and/or proxy services.

A. Freedom of Expression Recognizes a Key Role for Anonymous and Pseudonymous Speech

Anonymous and pseudonymous expression are well-established as a central part of the right to freedom of expression. Privacy and freedom of expression have been intertwined for centuries, and at the intersection of those two rights lies the right to speak anonymously. The international human rights framework surrounding privacy and freedom of expression recognizes the important role of anonymous speech. Further, there is global recognition that the right to speak anonymously extends to the Internet.

Anonymous and pseudonymous speech have long traditions among thought leaders the world over. In the United States, the right to speak anonymously can be traced to the years leading up to the nation's founding. Today we recognize that Alexander Hamilton, James Madison, and John Jay are the authors of the foundational *Federalist Papers*; however, at the time of publication in the late 1780s, the authors published under the pen name

"Publius."[2] Anonymous and pseudonymous speech have long traditions elsewhere as well. For example, Jane Austen, Fanny Burney, Daniel Defoe, Alexander Pope, William Shakespeare, Jonathan Swift all published anonymously or under pseudonyms.[3]

Anonymity and pseudonymity allow speakers to speak when they might otherwise be unable to for fear of reprisal, antagonism, or threats to their safety or status. As a recent report from David Kaye, the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, explains, "[i]ndividuals and civil society are subjected to interference and attack by State and non-State actors, against which encryption and anonymity may provide protection."[4] In the United States, the Supreme Court recognizes that anonymous speech "may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible."[5] Even when the threat of retaliation is non-existent, anonymity allows a speaker to judged by his or message rather than his or her identity.[6] Similarly, anonymity and pseudonymity can empower a speaker to test out new ideas and new opinions without having

---

[2] Gregory E. Maggs, *A Concise Guide to the Federalist Papers As A Source of the Original Meaning of the United States Constitution*, 87 B.U. L. REV. 801, 811 (2007).
[3] *See, e.g.*, Robert Folkenflik, *Anonymous was a Writer*, THE LOS ANGELES TIMES (December 27, 2011) (highlighting a litany of famous authors, including Jane Austen, Fanny Burney, Daniel Defoe, Alexander Pope, William Shakespeare, Jonathan Swift, who published anonymously or under a pen name) http://articles.latimes.com/2011/dec/27/opinion/la-oe-1227-folkenflik-anonymous-20111227.
[4] David Kaye (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report on Encryption, Anonymity, and the Human Rights Framework*: *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. H.R.C. Doc. A/HRC/29/32 (May 22, 2015) at 7.
[5] *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-42 (1995) (explaining that anonymity allows a speaker "to ensure that readers will not prejudge her message simply because they do not like its proponent.")
[6] *McIntyre* at 342.

to face the threat of "de facto exclusion" from political, social, and cultural spheres.[7]

Privacy, freedom of expression, and freedom of opinion are recognized as fundamental human rights.[8] Indeed, the right to privacy and the right to freedom of expression depend on one another. As Frank LaRue, the previous Special Rapporteur on Free Expression and Opinion, explained in a 2013 report, "an infringement upon [privacy or free expression] can be both the cause and consequence of an infringement upon the other."[9] The right to speak anonymously and pseudonymously has been similarly established.[10] Anonymity offers the rare balance, advancing both privacy and free expression interests without privileging one over the other.[11]

In recent years, there has been global recognition that the right to speak anonymously extends to the Internet—what Special Rapporteur David Kaye refers to as "the central global public forum."[12] Crucially, Kaye's May 2015 report to the United Nations Human Rights Council stated that the "[p]rohibition of anonymity online interferes with the right to freedom of expression."[13] Individual states and their judiciaries, including the United States, Canada, the European Court of Human Rights, and the Republic of Korea, have all articulated a basic right to protect personal information, including identity,

---

[7] Frank La Rue (Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/17/27 (Apr. 17, 2013).
[8] *See, e.g.*, Kaye, *supra* note 4 at 9; Human Rights Council Res. 2012/20, U.N. Doc. A/HRC/20/L.13 (June 29, 2012); Global Network Initiative, *Principles on Freedom of Expression and Privacy* (n.d.).
[9] La Rue, *supra* note 7 at 13.
[10] *See, e.g.*, Kaye, *supra* note 4 at 7.
[11] Daniel Solove, *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet* 191 (2008).
[12] Kaye, *supra* note 4 at 5.
[13] Kaye, *supra* note 4 at 17.

online.[14] Further, there is public support for that right: a 2013 survey by the World Economic Forum found that more than three-quarters of those surveyed felt that "[p]eople should be able to say what they feel about their government on the Internet" and more than 60% felt that "[t]here are times when people should be able to be anonymous on the Internet" (the latter often being a prerequisite for the former).[15]

Despite strong condemnations against the prohibition of anonymous speech, some have argued against protecting online anonymity, contending that law enforcement or other interests outweigh those of the speaker. Whatever the interest in unmasking an anonymous speaker, free speech interests demand the preservation of opportunities for anonymous speech. As the U.S. Supreme Court recognized, although the right to remain anonymous "may be abused when it shields fraudulent conduct . . . our society accords greater weight to the value of free speech than to the dangers of its misuse."[16]

B. Registrant Contact Information Is and Will Be Abused

---

[14] Kaye, *supra* note 4 at 16; Charter of Fundamental Rights of the European Union 2000/C, 2000 O.J. (364) 10; *see also* World Econ. F., *The Internet Trust Bubble: Global Values, Beliefs and Practices* (2013) (finding overwhelming public support for the notion that "[a]ccess to the Internet should be a fundamental right for all people"); *Am. Civil Liberties Union v. Johnson*, 4 F. Supp. 2d 1029, (D.N.M. 1998) (holding that a state statute requiring website operators to restrict access to indecent materials through use of a credit card, debit account, or adult access code violated the First Amendment, because such a requirement "prevents people from communicating and accessing information anonymously."); *Doe v. 2TheMart.com*, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) (holding that "the right to speak anonymously extends to speech via the Internet."); *Sinclair v. TubeSockTedD*, 596 F. Supp. 2d 128, 132 (D.D.C. 2009) (explaining that, "[g]enerally speaking, the First Amendment protects the right to speak anonymously. Such rights to speak anonymously apply, moreover, to speech on the Internet.").

[15] World Econ. F., *supra* note 14.

[16] *McIntyre* at 357 (citing *Abrams v. United States*, 250 U.S. 616, 630–31 (1919) (Holmes, J., dissenting)).

There are a number of reasons why registrants may want to keep their contact information private given that the information is currently and will continue to be abused. Registrants may need to shield their personal contact information because publication of that information could subject them to harassment because of their viewpoints or unpopular speech. Others require privacy to protect themselves from the threat of attack by those who would do them harm. Still others simply need the reassurance of privacy to assert an identity online that is at odds with their offline identity. In addition, even for registrants who have "nothing to hide," publication of contact information raises legitimate locational privacy concerns.[17]

Some registrants face on- and offline harassment because of their viewpoints. For example, scouring the Internet for one's contact information and publishing it to facilitate widespread harassment—a practice known as "doxing"—is a relatively common form of online retaliation for unpopular speech.[18] Doxing has been used to harass women speaking out against sexism in video game culture.[19] And doxers sometimes use WHOIS lookup of domains to

---

[17] Some scholars have disputed the notion that having "nothing to hide" is a legitimate argument against privacy protections. *See, e.g.,* Daniel Solove, *Why Privacy Matters Even if You Have Nothing to Hide*, Chronicle of Higher Education (May 15, 2011), https://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/.

[18] *See* Emily Bazelon, *The Online Avengers*, NY Times (Jan. 15, 2014), http://www.nytimes.com/2014/01/19/magazine/the-online-avengers.html.

[19] *See, e.g.*, Adi Robertson, *Trolls Drive Anita Sarkeesian Out of Her Home to Prove Misogyny Doesn't Exist*, The Verge (Aug. 27, 2014) http://www.theverge.com/2014/8/27/6075179/anita-sarkeesian-says-she-was-driven-out-of-house-by-threats ("She's published a page of extremely violent sexual threats from the person who apparently drove her to call the police; in it, the user mentions the location of her apartment and threatens to kill her parents, who the user names and claims to be able to find."); Alex Hern, *Felicia Day's Public Details Put Online After She Described Gamergate Fears*, The Guardian (Oct. 23, 2014), http://www.theguardian.com/technology/2014/oct/23/felicia-days-public-details-online-gamergate ("The publication of [actor Felicia] Day's details is being seen as further strengthening the criticism that Gamergate's partcipants are pursuing an

find contact information. As a self-described "hobbyist hacker" explained in a blog post on "the art of doxing":

> If the person you are trying to dox happens to have a website you could try to do a WHOIS lookup on the domain name by using a service such as who.is or any other website out there that provide [sic] you with a WHOIS lookup feature (there are a lot of them).
>
> A WHOIS lookup will return various information about the domain owner like their name, email, phone number and address.[20]

Indeed, the founder of the Online Abuse Prevention Initiative, Randi Harper, was harassed by someone who called law enforcement to her home based on information obtained from the WHOIS record for her domain.[21]

Moreover, harassment extends beyond mere annoyance; some registrants may be contending with stalkers or other attackers who threaten their physical safety or even their very lives. For example, an online resource for victims of sexual violence, stalking, and intimate partner violence explains, "For anyone recovering from sexual violence, stalking or intimate partner violence, the ability to control their privacy and personal information is essential to rebuilding their sense of security. The Internet does not make that easy, especially when abusive partners are technologically savvy."[22]

---

anti-woman agenda, which has seen female game developers and journalists harassed and threatened, while male critics have been almost untouched.");
[20] EvilN0w, The Art of Doxing, http://hack.wtf/doxing/ (last visited July 7, 2015).
[21] Online Abuse Prevention Initiative, Letter to ICANN (July 2015), http://onlineabuseprevention.org/letter-to-icann-july-2015/.
[22] National Cyber Security Alliance, StaySafeOnline.org, *Privacy & Domestic Violence*, https://www.staysafeonline.org/data-privacy-day/privacy-and-domestic-violence/ (last visited July 7, 2015).

II. Recommendations

Consistent with the importance of anonymous and pseudonymous speech, as well as the numerous possibilities for harmful abuse of registrants' contact information, we make the following recommendations for consideration by the Working Group.

A. All Internet Users Must be Able to Use Privacy/Proxy Providers

Given the importance of anonymity and privacy to free speech and free expression, all registrants should have the benefit of these rights made possible by privacy/proxy services. However, registrants' rights can only be safeguarded if those services are able to prevent disclosure of data except in exceptional circumstances.

B. There Should be a High Threshold for Revealing Customer Data

Requests that providers "reveal" data of individuals and organizations will come from a variety of parties, including intellectual property owners and private computer security investigators around the world. Privacy/proxy service providers will face significant pressure to turn over this customer data to those who allege infringement or other violations of law or policy.

Mere allegation of infringement or illegality is insufficient cause for a provider to disclose a customer's data to a third party; it is frequently trivially easy for a party abusing the system to allege frivolous or nonexistent civil claims to justify a demand for personal information. Registrants should have the ability and opportunity to respond to the allegations and to the dangers to which they, their families, and their organizations might be subjected, and to obtain counsel on these matters.

Revealing a customer's registration data—which often must include sensitive personal details such as a physical address, email address, and phone number—should only occur when there has been a substantial showing of

likelihood of abuse and only after due process (see the next item below). What we seek to avoid is an Internet where privacy and anonymity concerns related to registrant contact information chill the decision to obtain a domain name and participate online.

C. Any Rules Governing "Revealing" Personal Data Must Follow Fair Procedures for Privacy/Proxy Customers

In addition, prior to a provider publishing a customer's private or proxied data in the globally and publicly available WHOIS database, customers must be allowed to provide information regarding whether such publication could endanger the safety of individuals or organizations whose physical location might otherwise be unknown. Customers should be entitled to a fair review process before their data is disclosed or published.

Further, within a short period after adoption and implementation of the final rules, ICANN should implement a mandatory review process to survey customers to understand the impact of disclosures made pursuant to the requirements ICANN has imposed. In addition, ICANN should seek to assess on a continuing basis whether these rules create a chilling effect on online speech.

D. Privacy/Proxy Providers Should Not Be Compelled to Assess or Monitor Registrants' Use of Domain Names

The proposed obligation on privacy/proxy service providers to refuse service to "commercial" actors resembles other attempts to impose on intermediaries the duty to deny service or act as enforcement agents.[23]

[23] For example, some parties have urged ICANN to construe the 2013 RAA to impose greater obligations on registrars to police copyright infringement occurring on their registrants' domains. Letter from Victoria Sheckler, Senior Vice President, Recording Industry of America, et. al., to Steve Crocker, Chairman and Fadi Chehada, CEO, ICANN, March 5, 2015, *available at* https://www.icann.org/en/system/files/correspondence/riaa-to-icann-05mar15-en.pdf. The same interests have persuaded one state in the U.S. to

Intermediaries, including privacy/proxy services, should not be required to assess the nature of content provided by third parties—including whether it is commercial or whether it may infringe another's copyright. In many cases, particularly in copyright and trademark, whether protected content is present and whether the underlying right is infringed are distinct inquiries. For very good reasons, including that it requires intermediaries to assume an inappropriate role in balancing users' competing rights, we generally do not require intermediaries to adjudicate that distinction.

The obligation to deny services to "commercial" websites would impose upon intermediaries a similar duty to monitor and assess the content and conduct of others. A provider may decide that a registrant is engaged in "noncommercial" activity at the time of their registration, but the nature of a registrant's use of a domain can change or evolve over time. In such a circumstance, what was an approved use of privacy/proxy services initially may become prohibited without any notice to the service provider. Creating such an obligation to monitor registrants' activity is ill-advised and inconsistent with the way that services providers on the Internet interact with one another.

E. A Privacy/Proxy Framework that Draws a Distinction Between "Commercial" and "Non-Commercial" Registrants Would Be Inappropriate and Inadministrable

We strongly support the continued availability of privacy/proxy services for non-commercial organizations, commercial organizations, and individuals and agree with the conclusion in the WG report that "P/P services should remain available to registrants irrespective of their status as commercial or non-commercial organizations or as individuals."[24]

---

prohibit certain websites from operating anonymously if they make certain content commercially available to citizens of that state. *See* Fla. Stat. § 501.155, "True Origins of Digital Goods Act" (2015).

[24] Initial Report at 7.

Some actors seek to limit access to privacy/proxy services for certain types of registrants engaged in "commercial services" and/or "financial transactions" online. However, this restriction would be problematic, as the distinction between commercial activities and non-commercial activities is not always evident. For example, individual users may use advertising on their sites to help defray operating expenses, while still using their site primarily as a means of expression. From the individual's perspective, the "primary purpose" of the site is noncommercial, even though the ads may represent more than half of the site's content. Many nonprofit organizations and entities accept donations online, sell small items such as books or bumper stickers, or seek membership fees through their websites. Even if an organization administers a website solely to facilitate these transactions, the nonprofit itself may be a charitable, religious, educational, or political organization whose only "commercial" activity is fundraising through its website. Under the proposed ban on the use of privacy/proxy services for commercial services, it is unclear if the identity, location, and contact information for the person registering a domain for such an organization could remain protected from public disclosure.

The Initial Report does not provide a definition of "commercial activities" and asks whether it would be useful to adopt one. For the reasons described in this section, the answer is no: it is unlikely that the WG will be able to develop a definition that does not expose many speakers around the world to threats to their privacy and safety, and these threats will undoubtedly chill these speakers' freedom of expression.[25]

[25] Moreover, even if the WG were to develop a definition, implementation of the policy will necessarily shift the negative consequences of the policy to speakers, as the privacy/proxy services will face extremely lopsided risks. If a user's request for anonymity services is denied, no harm befalls the service provider. But if the provider enables the user to speak anonymously, and is deemed to have incorrectly determined that the user's activity is non-commercial, the service provider may lose its ability to conduct business itself. (As noted in Recommendation B above, even if a noncommercial designation is made

Banning the use of proxies based on "commercial" content or services could prevent the individuals and organizations who would benefit most from privacy/proxy services from using them. Content creators marketing their works under pseudonyms and individuals or groups using their domains as both marketplace and soapbox should be able to do so anonymously when necessary to avoid ostracism, bias, and censorship, as discussed above in part A. Indeed, for public interest organizations whose works touches on matters that are culturally or politically sensitive or controversial, anonymity is essential to their freedom to operate.

Although many jurisdictions may require businesses to register contact information,[26] using this evidence to support a limitation on privacy/proxy services for commercial websites ignores two important points. First, the responsibility to register and the commercial/noncommercial designation lie with the business, not an entity responsible for assigning names and numbers. Second, these requirements allow for registration of business names, themselves a kind of proxy. Individuals with personal domains later classified as "commercial" would enjoy no such shield. Moreover, the value of a shield between individuals and their commercial ventures has long been recognized and embodied in the most commercial of entities: the corporation. Privacy/proxy services should be allowed to provide this same value to individuals and organizations online, regardless of the degree to which they use their domains "commercially."

---

correctly at time of registration, the nature of a site can change or evolve over time, and what was an approved use of privacy/proxy services initially may become prohibited without any notice to the service provider.) Thus, in less than clear cases, the scales will weigh heavily in favor of denying anonymity.

[26] *See* FWD Strategies International, "Commercial Use of Domain Names: An Analysis of Multiple Jurisdictions," May 11, 2014, at 10-25.

III. Conclusion

As the Working Group continues its consideration of issues relating to the accreditation of privacy and proxy service providers, we urge it to focus prominently on preserving meaningful opportunities for Internet users to engage in anonymous and pseudonymous speech online. Freedom of expression recognizes a key role for anonymous and pseudonymous speech, which extends to speech online. Not only does protection of registrant contact information comport with the value placed on anonymous and pseudonymous speech, but it also protects registrants from a number of possible abuses that could threaten registrants themselves or their loved ones. Accordingly, the Working Group should ensure that all users can use privacy/proxy service providers, that there is a high threshold for the reveal of privacy/proxy customer data, that rules governing such reveal follow fair procedures, that privacy/proxy service providers are not compelled to assess or monitor registrants' use of domain names, and that the privacy/proxy framework does not draw a distinction between "commercial" and "non-commercial" registrants.

We appreciate the opportunity to comment and look forward to continuing to work with the Working Group in the future in support of privacy and freedom of expression on the Internet.