To: **Göran Marby (ICANN)**

From: **John Horton (LegitScript President and CEO)**

Date: **January 29, 2018**

RE: **COMMENTS ON THE PROPOSED ICANN INTERIM WHOIS COMPLIANCE MODELS**

As outlined below, all three proposed models, to varying degrees, will benefit internet criminals and significantly impede consumer protection, anti-money laundering and anti-abuse efforts designed to protect internet users. LegitScript urges ICANN to reject the second and third models entirely. Although the first model is the least problematic among the three, it too presents critical problems.

The approach implemented by ICANN, whether as an interim or final step, should:

- Offer privacy protections consistent with the GDPR only to registrants who can be verified as:
    - EU citizens
    - Natural (not legal) persons and
    - Not using domain names for commercial purposes (i.e., to sell, acquire or facilitate transactions for goods or services).
- Add a mandatory field in Whois for registrants to self-identify as an EU citizen, and afford a mechanism for that designation to be verified by the registrar (or, in the case of abusive use of a domain name, challenged by a third party).
- Retain open, anonymous access to bulk Whois via Port 43.

General Principles

The internet is, like the physical world, a mix of beauty and ugliness, safety and danger, trust and fraud. Like the physical world, the internet reaches its full potential when there are mechanisms in place to promote trust, transparency and accountability, particularly in the commercial sphere where everyday internet users may be defrauded or hurt.

Open, anonymous bulk access to Whois (currently via Port 43) is arguably the centerpiece of internet trust and safety. By definition, cybercrime is typically a commercial activity involving the fraudulent or illegal sale, acquisition, marketing or other facilitation of goods, services or money in a way that hurts people. In short, cybercriminals are in it for the money. As one might expect, cybercriminals go to great lengths to hide their identities and protect their illicit commercial interests. This is why there has never been found to be a privacy right for entities engaged in commercial activities: the harm from cybercrime is rarely, if ever, disconnected from a cybercriminal's commercial motivations.

In order to strike the right balance between privacy and consumer protection, we urge ICANN to

818 SW 3rd Ave. #353
Portland Oregon, 97204

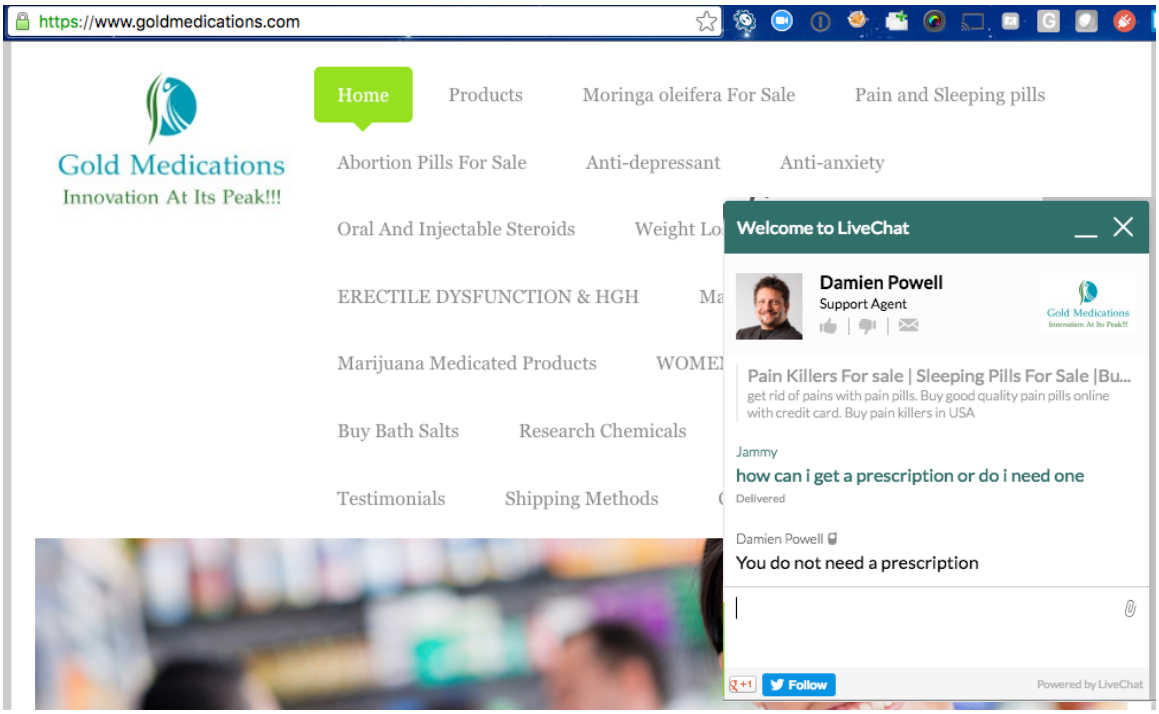
consider the following principles.

- Protection of natural persons only. The GDPR is intended to protect natural persons, not entities engaged in commercial activity. Simply put, there has never been found an established privacy right for commercial entities to conceal or withhold information from the public about who and where they are. Indeed, one has to engage in painful mental gymnastics to construct implausible fact-patterns theorizing how a registrant engaged in commercial activities might warrant the same sort of privacy protection as a natural person. One reason that commercial entities have not been found to warrant the same level of privacy protections is the valid public interest in protecting consumers from criminal and other illicit activities, which in turn requires transparency.
- Protection of EU citizens only. It is difficult to understand what justification -- aside from registrar convenience -- there is for affording non-EU citizens protections under the GDPR. The GDPR is only meant to protect the rights of a small portion of the world's population. It simply is not ICANN's proper place to extend these shields to the remaining (vast) majority of the world's population.
- Bulk Whois Access Critical in Consumer Protection and Cybercrime Investigations and Prevention. It's critical to emphasize that the Whois record of a single domain name used for fraudulent or illegal purposes is often not very helpful in preventing or pursuing cybercrime. That's because cybercriminals usually register dozens, hundreds or thousands of domain names. The proven way to identify the "network" of illicit websites, and even the bad actor himself or herself, is to identify and map all of the domain names under the same individual's control, based on "reverse querying" multiple unique Whois fields such as email and phone number.

A Concrete Example: Why Anonymous, Open Access to Bulk Whois via Port 43 is Critical to Consumer Protection and Anti-Abuse

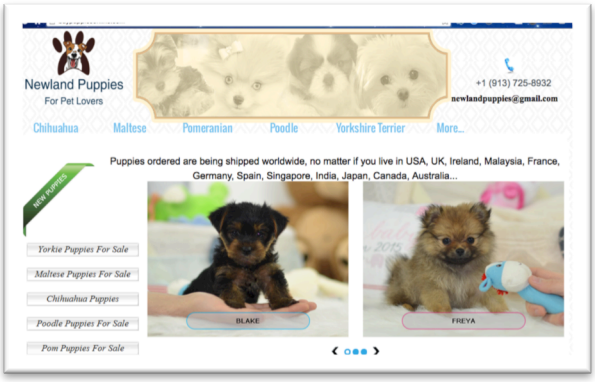
As ICANN may be aware, LegitScript assists a variety of search engines, e-commerce platforms and financial institutions in preventing and detecting abusive activity such as money laundering. The ability to obtain Whois records and reverse query all of the Whois fields against the entire library of all domain name records is a critical tool in preventing this sort of abuse. Below is a single example that shows why the ability to query Whois records in bulk is so important.

The example is goldmedications.com, a rogue internet pharmacy website that was selling opioids and other addictive medicines to internet users without a prescription. The website can readily be verified as a criminal enterprise.



As shown below, LegitScript was able to work with the appropriate financial institution to proactively and preemptively identify the fake commercial website used to obtain a merchant account through which the registrant was paid. However, our starting point was not goldmedications.com itself – rather, it was two seemingly innocuous commercial websites used to launder the money for the rogue internet pharmacy.

The starting point for our analysis were two merchant websites that appeared to sell puppies, amishteacups.com and buypuppiesonline.com. Both, initially, appear to be innocuous, legal commercial websites. LegitScript reviewed these as part of our normal assessment of online merchants.



For the purposes of this explanation, we will focus on the Whois record for amishteacups.com, which was as follows, and referenced “Pelama Pelema Tiogo Arnaud” as the registrant with an email address of *karl636donasen1967[at]gmail.com*.

AMISHTEACUPS.COM

Fetched and parsed on Jun 20 11:30

Domain Name	amishteacups.com
Status	ok
Registrar	1&1 INTERNET SE
Registrar Phone	+1.8774612631
Registrar Email	abuse@1and1.com
WHOIS Server	whois.1and1.com
All WHOIS Emails	karl636donasen1967@gmail.com hostmaster@1and1.com
Registrant Name	Pelama Pelema Tiogo Arnaud
Registrant Address	SHISONG
Registrant State	NW
Registrant City	KUMBO
Registrant Postal Code	00237
Registrant Country	CM
Registrant Email	karl636donasen1967@gmail.com
Registrant Phone	+237.678669325

As part of assessing the amishteacups.com merchant, LegitScript conducted a “reverse Whois query” to identify all of the domain names registered to the same email address. The results included the following:

Domain Name	Whois email
amishteacups.com	karl636donasen1967@gmail.com
australiamedsonline.com	karl636donasen1967@gmail.com
bestsirupshoponline.com	karl636donasen1967@gmail.com
buylaboratorysupplies.com	karl636donasen1967@gmail.com
delnaud-labs.com	karl636donasen1967@gmail.com
educationforchilden.com	karl636donasen1967@gmail.com
k2bathsaltonline.com	karl636donasen1967@gmail.com
newlandmedication.com	karl636donasen1967@gmail.com
goldmedications.com	karl636donasen1967@gmail.com

Most of the domain names above were used to sell illegal drugs, including opioids, on the internet. And sure enough, if one purchased illegal drugs through goldmedications.com, the credit card statement provided either “buypuppiesonline.com” or “amishteacups.com” as the

merchant of record – a clear case of money laundering. And without the ability to process payments, a website is as good as shut down.

In analyzing the example above, it is critical to understand that **the ability to reverse query unique data fields – in this case, Whois emails -- across the entire universe of all domain name registration records** was the critical function that allowed us to detect the money laundering. This, in turn, relied upon open, anonymous access to aggregated Whois via Port 43, as opposed to only having access to a single domain name record. (That is, if we had only been afforded access to the Whois record for amishteacups.com, it wouldn't have done any good.)

Specific Comments on Models 1, 2 and 3

Model 1. As noted above, the first model is the least problematic among all three ICANN models. However, there are some serious problems with it.

1. First, Model 1 appears to treat registrants differently depending on whether they are a natural or legal person. This distinction is immaterial – after all, in the example above, the registrant purported to be a natural person. (Indeed, it's fairly unlikely that this registrant actually set up a legitimate corporation.) What is critical is not what the registrant is, but rather that the registrant was using the domain names for commercial purposes. Accordingly, the distinction should not be based only on the registrant's legal status as a natural or legal person, but also on how the domain name is being used.
2. Second, Model 1 restricts public access to two important unique data fields – the Whois email and the Whois phone number. Registrant names are not, by definition, unique; emails and phone numbers, properly formatted, are. Therefore, they are unique tools in being able to accurately conduct reverse queries and avoid false positives. Even if ICANN wishes to protect these fields for natural EU citizens, there is simply no justification or need to do so where the domain name is used for commercial purposes.
3. Third, Model 1 appears to give registrars discretion in responding to requests from third parties who wish to access the additional (non-public) data fields. Perhaps some registrars would agree to share this information with anti-abuse or consumer protection firms or with law enforcement. But given ICANN's repeated accreditation as registrars of entities that are, are operated by, or that actively shield criminal enterprises (see my testimony before the U.S. Senate here), it is reasonable to expect that the most problematic registrars would simply refuse to share the information under the guise of protecting their clients' privacy.

If ICANN must adopt one of the models, we prefer Model 1, but with modifications as described above. Additionally, if there is some sort of a certification scheme, it is imperative to anti-abuse and consumer protection efforts that bulk access to all Whois records for the broader purpose of abuse mitigation be recognized as legitimate.

Models 2 and 3. The fundamental problem with both Models 2 and 3 is that bulk Whois access via Port 43 appears to be curtailed. Moreover, shielding of Whois data should be implemented as narrowly as possible: the failure to distinguish between natural and legal persons (or, as

noted above, the commercial or non-commercial use of domain names) or EU and non-EU registrants forces a restrictive scheme designed to help only a small minority of the world's citizens on the rest of the internet.

Model 3, in particular, is an extremist approach that fails to take into account the realities of anti-abuse and the cross-jurisdictional nature of the internet. (If a registrant's domain name is used to target only US citizens, and the registrant chooses a Russian domain name registrar, how exactly is US law enforcement supposed to get an enforceable court order that the Russian registrar will honor?) Implemented as described, it would immediately and dramatically reverse countless consumer protection, trust and safety, and anti-abuse efforts underway for years.

The Right Approach

It is not ICANN's proper role to take GDPR protections designed to protect a very limited class of internet users – natural citizens of an EU nations, a very small percentage of the world's population – and create a new privacy scheme for the rest of the world. There is, however, a very limited approach that will protect registrars from liability and adhere to the letter and the spirit of the GDPR.

First, ICANN must recognize the limited applicability of the GDPR. It is only meant to protect EU citizens, and only those acting as natural persons, not legal (commercial) persons. It is within ICANN's ambit to require an additional Whois data field in which the registrant self-identifies as an EU citizen. In this case, LegitScript recognizes that there may need to be some sort of a limited redaction policy in which certain fields are only available by accredited third parties and only if a legitimate purpose has been demonstrated. But, this should only be available for those domain names registered by the EU citizen, and there should be a process for registrars to verify (if only via spot checks) that the claim of EU citizenship is plausible, and for the claim to be challenged in cases where the domain name is used abusively and there is some indication that the registrant is not actually an EU citizen.

Second, the protections should not be available if it can be demonstrated that the domain name is being used for commercial purposes, irrespective of whether the registrant claims to be a natural or legal person and irrespective of whether the registrant, even if a natural person, is an EU citizen.

Third, ICANN should adopt a clear and unambiguous position that anti-abuse, compliance and trust and safety efforts are a legitimate purpose for accessing and maintaining Whois information. The aggregation of Whois data by legitimate entities that demonstrate appropriate controls and protocols to safeguard registrant information should be construed as a legitimate purpose, and advocated as such by ICANN.

LegitScript appreciates the opportunity to submit this feedback. Please do not hesitate to contact me should you have questions.

818 SW 3rd Ave. #353
Portland Oregon, 97204