WRITTEN STATEMENT OF JOHN C. HORTON
PRESIDENT AND CEO, LEGITSCRIPT

BEFORE THE SENATE COMMITTEE on the JUDICIARY
SUBCOMMITTEE ON OVERSIGHT, AGENCY ACTION, FEDERAL RIGHTS AND FEDERAL COURTS

"Protecting Internet Freedom: Implications of Ending U.S. Oversight of the Internet" (September 14, 2016)

Chairman Cruz, Ranking Member Coons, and Members of the Subcommittee:

The question before this Committee is whether the Internet Corporation for Assigned Names and Numbers (ICANN) has demonstrated the requisite level of accountability and transparency to operate free from US government oversight. The answer to that question is No.

Some proponents of the IANA transition argue that ICANN's responsibilities are merely technical — to administer IP address blocks and the Domain Name System. That is inaccurate. ICANN also accredits registrars and oversees their compliance with the accreditation contract. This role is important: who ICANN accredits, and the degree to which ICANN condones bad behavior by accredited registrars, establishes the tolerated baseline for fraud and internet crime. Accordingly, how ICANN performs these roles is central to evaluating the organization's accountability and transparency.

ICANN has on several occasions accredited, and taken little or no action against, companies whose business model relies entirely or in part on harboring criminal activity. For example, for years, ICANN maintained the accreditation of a registrar whose entire portfolio consisted of tens of thousands of illegal online pharmacies targeting the US with addictive medicines. The revenue from the registrar's business, estimated at over $300 million, subsequently funded the principal's involvement in North Korean-sourced methamphetamine distribution, arms smuggling in Africa, the reported diversion of missile guidance technology from the US to the Iranian government, and murders-for-hire.[1]

Still today, there remain other instances in which an accredited registrar and a criminal enterprise are under common control, and the registrar or its principal directly registers domain names used for illegal purposes.

[1] See various court filings, generally, in United States vs. Paul Calder Le Roux, Case No. 1:12-cr-00489-LAP; United States vs. Moran Oz, CASE 0:13-cr-00273-SRN-FLN, and United States vs. Joseph Hunter, Case No. 1:13-cr-00521-LTS. The various guilty pleas and testimony under oath is best summarized in a recently published seven-part series as mastermind.atavist.com, which also reported on the nature of the illegal technology transfers to Iran at https://mastermind.atavist.com/the-next-big-deal.

ICANN's registrar accreditation agreement requires registrars to "investigate" and "respond appropriately" to complaints that domain names are used to facilitate illegal activity.[2] Of course, registrars that are interchangeable with the criminal organization whose domain names they sponsor do not comply with this requirement. Although many registrars do take action against domain names used for criminal activity, some registrars simply ignore or clearly indicate that they will not take any action, irrespective of the amount of evidence of illegality provided. When internet users submit a complaint to ICANN against such registrars, however, ICANN routinely dismisses the complaint, finding that the registrar "responded appropriately" despite apparently doing nothing. This effectively gives the registrar a green light to continue sponsoring and profiting from the harmful or criminal activity. When asked to explain the basis for its decision, ICANN responds that these determinations are privileged — a secret — between it and the registrar as part of an "informal" compliance process.[3]

Against this backdrop, ICANN cannot credibly testify under oath to this Committee that it operates transparently. Indeed, its compliance function is akin to an unaccountable secret court, like Kafka in reverse: registrars are afforded a secret, "informal" compliance process, after which the complaint about a domain name is typically dismissed, and the reasons never disclosed — even while the domain names continue to operate unimpeded. ICANN defends this process by arguing that disclosing this information would impair the quality of its relationships with registrars.

This is nonsense: ICANN is supposed to accredit registrars and ensure their compliance with the accreditation agreement, not be their friend. The problem is a classic conflict of interest: the chief sources of ICANN's revenue are registrar accreditations and domain name applications and registrations, by or through registrars and registries, which constitute an influential political constituency within the ICANN "multi-stakeholder model."[4] Accordingly, it should come as no surprise that when presented with evidence that a registrar is violating its accreditation agreement, ICANN often acts in the interest of the registrar, not the public, and by keeping information confidential, protects the registrar.

Congress has one last chance to fix this pervasive problem. Successive administrations dating back to the late 1990s, including the administration I served in, have failed to require ICANN to implement a structure that ensures disinterestedness in accreditation and compliance dealings with registrars. Until ICANN can demonstrate that its compliance arm is not a handmaiden of the industry whose compliance it is supposed to monitor, and will operate transparently and accountably in the interest of all internet users — not just the domain name registration sector — it cannot be trusted with the future of the internet.

---

[2] See ICANN 2013 Registrar Accreditation Agreement (RAA), Section 3.18, available at https://www.icann.org/resources/pages/approved-with-specs-2013-09-17-en#raa.

[3] This is based on repeated requests by LegitScript and other abuse reporters to ICANN to explain the basis of their findings that registrars who appear to decline to investigate or take any action against a domain name used for illegal activity complied with the requirement to investigate and respond appropriately.

[4] For ICANN's budget, see https://www.icann.org/en/system/files/files/adopted-opplan-budget-fy16-25jun15-en.pdf.

I. Five Examples: ICANN Accreditation and Compliance Failures

The five examples below demonstrate compliance failures and ICANN's lack of transparency. Two are examples of ICANN-accredited registrars that operate or operated as an arm of a criminal network. Three are examples of illegal online pharmacies that remain online because ICANN green-lighted the registrar's refusal to investigate or take action.

A. ABSystems, Inc. In December 2013, Paul Le Roux pleaded guilty to crimes involving North Korean methamphetamine trafficking, the transfer of US technology to Iran, and several murders-for-hire.[5] Mr. Le Roux, a Zimbabwean national who has been described by the New York Times as "one of the world's least known but most successful outlaws" and by the Daily Mail as the "most successful criminal mastermind you've never heard of," remains in US custody, pending sentencing.[6] Le Roux financed his illegal activities by operating as an ICANN-accredited domain name registrar, creating a rogue internet pharmacy network through his ability to register domain names unimpeded. Although his company, ABSystems, Inc., was finally de-accredited by ICANN in 2013 for paperwork-related reasons,[7] it wasn't until 2016 that information about the link between Mr. Le Roux's accreditation by ICANN as a registrar and his diversion of US technology to Iran, murders-for-hire, trafficking in North Korean methamphetamine, and arms smuggling has come to light.

As outlined in several recent articles,[8] by an investigative journalist,[9] and several court hearings for associated defendants, Mr. Le Roux developed a massive rogue internet pharmacy network called "Rx Limited" in the mid-2000s, selling addictive medicines without a valid prescription to US residents. His revenue from these operations is reportedly estimated at $250 million to $400 million. My company, LegitScript, spent several years tracking the connection between Rx Limited and ABSystems, shut down several of their merchant accounts and thousands of their websites, and on several occasions, had communications with Mr Le Roux's lieutenants or marketers.[10]

The sole reason for ABSystems' existence as an ICANN-accredited registrar was to provide bullet-proof domain name registrations for Rx Limited's illegal online pharmacies, so that the websites would not get shut down, and could be created and promoted with impunity. In other words, the

[5] United States vs. Moran Oz, File No. 13-CR-273, Motions Hearing, March 2, 2016, before the Honorable Jeffrey J. Keyes, United States District Court Magistrate.

[6] See http://mastermind.atavist.com.

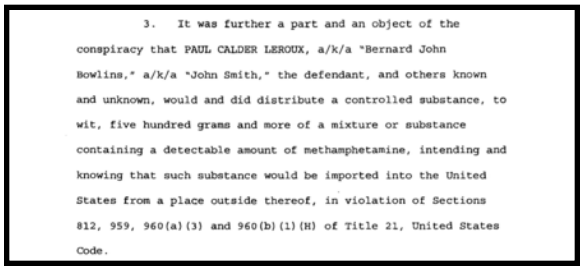
[7] https://www.icann.org/en/system/files/correspondence/serad-to-mcgowan-20dec13-en.pdf

[8] http://www.nytimes.com/2015/02/02/nyregion/us-reveals-criminal-bosss-role-in-capturing-a-mercenary.html and http://www.dailymail.co.uk/news/article-2890164/Revealed-successful-criminal-mastermind-ve-never-heard-real-life-Bond-villain-cocaine-gun-empire-spanning-four-continents-s-turned-super-snitch.html.

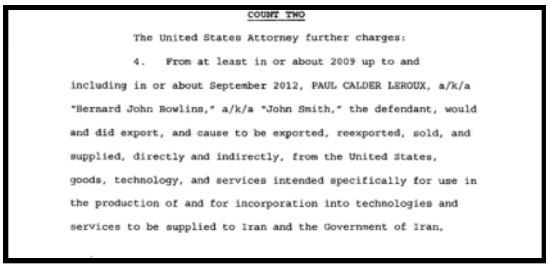
[9] See the articles listed in Footnote 6, as well as mastermind.atavist.com, which is a comprehensive analysis of Mr. Le Roux's activities.

[10] Although it's impossible to know for sure, I agree with these estimates of revenue based on my company's years of tracking Mr. Le Roux's operations, which included numerous conversations with his affiliate marketers or direct employees, identification and monitoring of his websites, and some awareness of his financial operations due to shutting down merchant accounts.

criminal network simply obtained its own ICANN accreditation. ABSystems did not sell domain names to the public, only registering its own domain names, every one of which were, one way or another, part of the Rx Limited criminal network. Here, it's critical to understand that most (but not all) other registrars, like GoDaddy, eNom (now Rightside), and Directi voluntarily shut down any internet pharmacy domain names that were part of this criminal network upon receiving a complaint. Obtaining his own ICANN accreditation was the only way Mr. Le Roux could ensure that his rogue internet pharmacies could operate unimpeded.



3. It was further a part and an object of the conspiracy that PAUL CALDER LEROUX, a/k/a "Bernard John Bowlins," a/k/a "John Smith," the defendant, and others known and unknown, would and did distribute a controlled substance, to wit, five hundred grams and more of a mixture or substance containing a detectable amount of methamphetamine, intending and knowing that such substance would be imported into the United States from a place outside thereof, in violation of Sections 812, 959, 960(a)(3) and 960(b)(1)(H) of Title 21, United States Code.



COUNT TWO

The United States Attorney further charges:

4. From at least in or about 2009 up to and including in or about September 2012, PAUL CALDER LEROUX, a/k/a "Bernard John Bowlins," a/k/a "John Smith," the defendant, would and did export, and cause to be exported, reexported, sold, and supplied, directly and indirectly, from the United States, goods, technology, and services intended specifically for use in the production of and for incorporation into technologies and services to be supplied to Iran and the Government of Iran,

Figs 1 and 2: Excerpts from the indictment against Paul Le Roux. Separate transcripts indicate that Mr. Le Roux believed the methamphetamine to be sourced from North Korea, and that the amount was between 50 and 100 kilograms. One investigative reporter indicates that the technology sold to Iran was US missile guidance technology (see mastermind.atavist.com).

As detailed in a seven-part series published earlier this year at mastermind.atavist.com, Mr. Le Roux's transition in the 2000s from a relatively poor computer programmer to a fabulously wealthy international criminal was due to revenue gained from his rogue internet pharmacy websites, which he was able to create and maintain as a result of his company's ICANN accreditation. He used this revenue as a launching pad into the other crimes to which he has now pleaded guilty or that he has admitted to under oath.

If ICANN had not accredited ABSystems, Rx Limited would have been smaller or nonexistent, and Mr. Le Roux would almost certainly have been unable to generate the revenue required to enter the North Korean methamphetamine, Somalian arms, and diverted missile technology markets. Yet for years, it was obvious to a number of anti-abuse and anti-spam researchers that ABSystems' ICANN accreditation was nothing but a shell for a criminal enterprise.

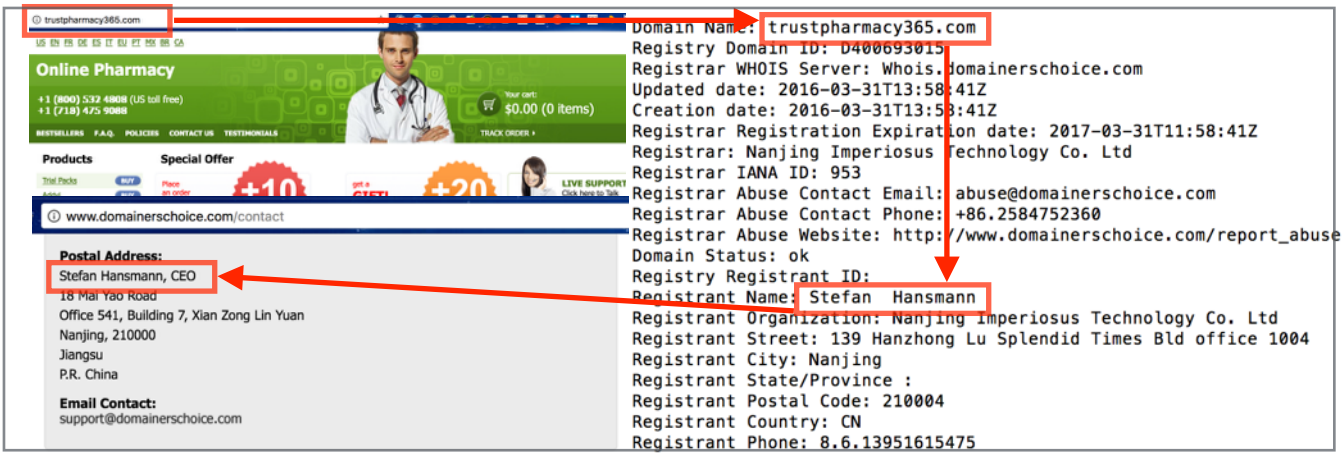
B. Nanjing Imperiosus. This ICANN-accredited registrar is based in China but is operated by a German national, Stefan Hansmann. Nanjing Imperiosus has only about 22,000 domain names under management; of these, several thousand are rogue internet pharmacies or websites engaged in illegal or infringing activity — a substantial portion of the registrar's business.[11]

Just as Mr. Le Roux controlled both the registrar (ABSystems) and the rogue internet pharmacy network (Rx Limited), many of the rogue internet pharmacies registered with Nanjing Imperiosus are

[11] For registrar counts, see https://features.icann.org/compliance/registrars-list. LegitScript, as of this writing, has identified over 2,300 currently active illegal online pharmacies with the company; this does not account for other infringing domain names or domain names we have not yet reviewed.

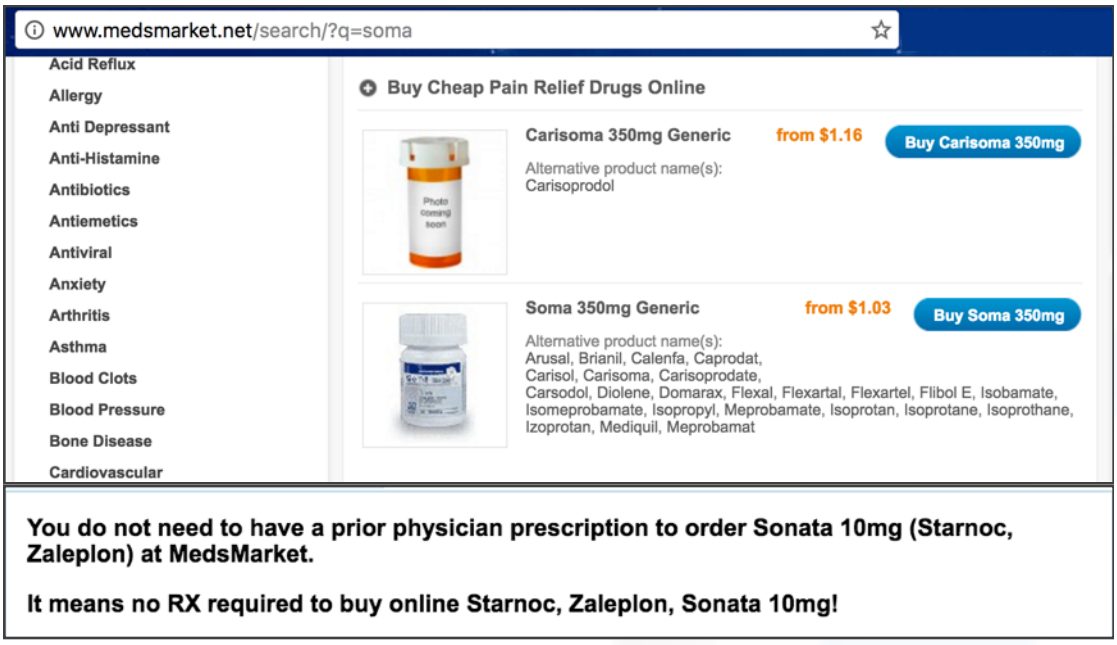
registered to Mr. Hansmann directly. Just a few among a few thousand examples include noprescriptionpharmacycanadian.net, trustpharmacy365.com, and no-prescriptionbuy-ventolin.com.

Here again, the accredited registrar itself *is* the rogue internet pharmacy operator. ICANN has been made aware of this, but Nanjing Imperious remains ICANN-accredited.



Figs 3, 4, and 5: Rogue internet pharmacies such as trustpharmacy365.com are registered with Nanjing Imperiosus. The CEO of Nanjing Imperiosus, Stefan Hansmann, is the registrant of the domain name.

C. medsmarket.net (registrar: DreamHost). The website medsmarket.net sells controlled substances without requiring a prescription. The domain name is registered with DreamHost, an ICANN-accredited registrar in California.



Figs 6 and 7: medsmarket.net indicates that it is selling controlled substances without a prescription. While most registrars around the world would suspend this domain name, DreamHost declined to take action.

On February 24, 2015, LegitScript notified DreamHost that medsmarket.net and numerous other domain names with DreamHost were used to sell controlled substances without a prescription and subsequently outlined additional detail in a multi-page memorandum. Despite clear language on the website indicating that a prescription wasn't required for controlled substances, DreamHost claimed it was unable to verify the illegality: in context, however, it appeared to LegitScript that the registrar was simply unwilling to take any action, no matter how much evidence was provided to the company. (Here, it is worth noting that the vast majority of domain name registrars voluntarily suspend domain names when they receive a verifiable abuse complaint.)

On April 28, 2015, LegitScript submitted a complaint to ICANN against DreamHost, alleging that the company "failed to respond appropriately" to an abuse complaint involving easy-to-verify illegality. ICANN closed the complaint against DreamHost, finding that the registrar responded appropriately despite indicating that it would do nothing. ICANN thereby effectively green-lighted the registrar's continued sponsorship of medsmarket.net. The reason medsmarket.net remains online today, selling controlled substances to US residents without a prescription, is because ICANN, through its own inaction, gave tacit approval to the registrar, DreamHost, to do nothing.

When asked what a registrar has done that constitutes an "appropriate response" to criminal activity, ICANN insists it is privileged information between ICANN and the registrar. Against this background, ICANN cannot credibly testify that its compliance process is transparent.

D. pillsaz.net (registrar: TodayNIC). This is a fake "Canadian" online pharmacy that falsely claims to sell FDA-approved medications. No prescription is required for any prescription drug sold on the website. The domain name is registered with TodayNIC, a Chinese registrar. pillsaz.net is one of roughly 15,000 websites[12] operated by a criminal enterprise known as Worldwide Drugstore.

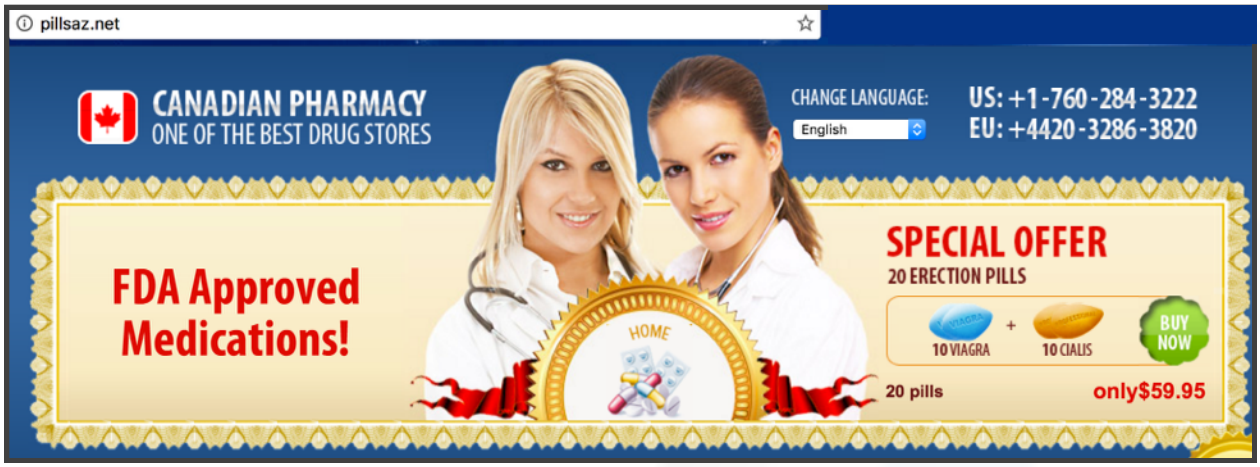
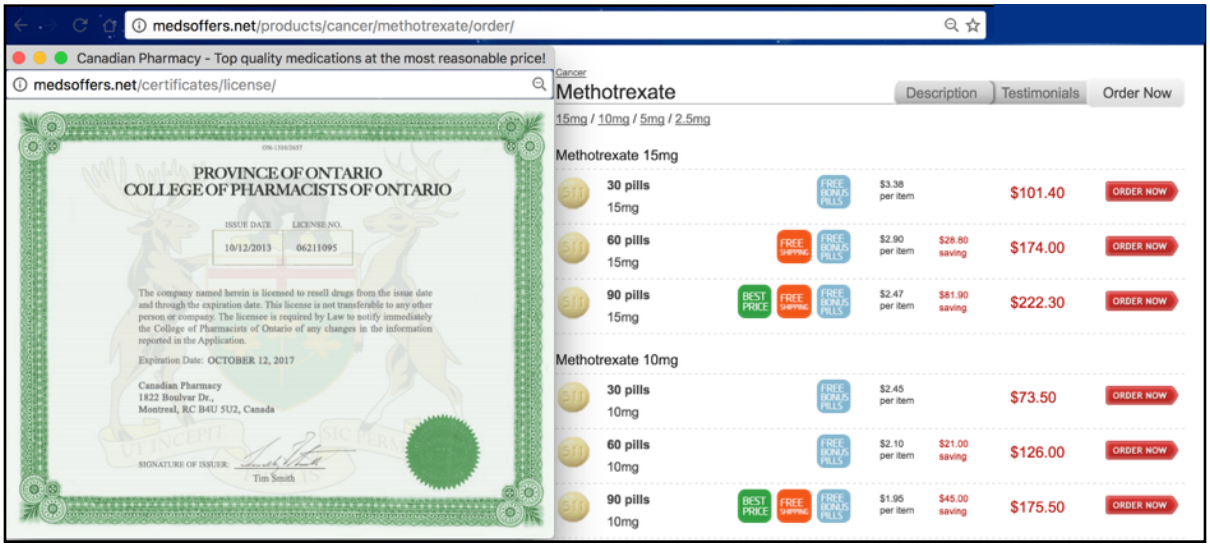


Fig 8: Rogue internet pharmacy pillsaz.net. The registrar, TodayNIC, declined to take action against the domain name; ICANN closed three complaints against the registrar, each time finding, inaccurately, that it "responded appropriately" by terminating the domain name.

[12] Only about 3,000 are online at any one time, give or take a thousand.

LegitScript notified TodayNIC, the registrar, about pillsaz.net four times: on March 15, 2015, May 11, 2015, April 7, 2016, and July 5, 2016. The domain name was also approved as an Operation Pangea target by INTERPOL in 2015. Each time, TodayNIC refused to take action against the domain name. On April 8, 2015, May 3, 2016, and July 25, 2016, LegitScript submitted complaints to ICANN; all were closed after ICANN found that the registrar "responded appropriately" by taking some action against the domain name. In fact, each time, the domain name has remained online.

E. medsoffers.net (registrar: GKG.net, Inc.) medsoffers.net is part of a Russian cybercriminal network commonly known as EvaPharmacy. The website sells counterfeit or unapproved drugs and does not require a prescription. The "pharmacy license" displayed on the bottom of the home page, which purports to be from Canada, is a forgery.



Figs 9-10: Rogue internet pharmacy medsoffers.net, part of a Russian and Eastern European criminal network called EvaPharmacy. Offers for unapproved, potentially counterfeit cancer medications are behind an overlaid pharmacy license, which is actually a forgery.

On December 22, 2015, and again in July 2016, LegitScript notified ICANN-accredited registrar GKG.net, based in Texas, about medsoffers.net and hundreds of other illegal online pharmacies sponsored by the company. The registrar has repeatedly indicated that it would refuse to take any action or conduct any investigation irrespective of the extent of evidence provided. LegitScript thereafter submitted a complaint to ICANN, alleging that the registrar failed to "conduct a reasonable investigation" and to "respond appropriately."

Despite the domain name's forged pharmacy license, despite the registrar's refusal to even verify the pharmacy license with our assistance, and despite the contractual requirement that a registrar "investigate" and "respond appropriately" to claims that domain names are used for illegal activity, ICANN found that this "registrar demonstrated that it took reasonable and prompt steps to investigate and respond appropriately to the report of abuse." medsoffers.net remains online and registered with GKG.net.

II. Accountable and Transparent Accreditation and Voluntary Compliance Models

Against this background, ICANN has a ready litany of excuses. These include:

- "ICANN is not a law enforcement agency."
- "ICANN does not regulate content."
- "We will respond to a court order."
- "You're suggesting we regulate the internet."
- "You forget the international nature of the internet: something may be legal in one country but illegal in another."[13]

These are nothing more than sound bites in search of a retweet. They completely miss the point.[14]

For ICANN to be trusted with independence, it needs to demonstrate that it can perform its accreditation and compliance roles impartially and in the public interest, and that it knows what is going on with the registrars it accredits. Turning a blind eye to registrars' criminal activity, or tolerance of it, has two negative effects on the future of the internet. First, and most obviously, it hurts internet users, who are invariably the victims of these schemes. Second, ICANN's incompetence or unwillingness to voluntarily address abusive activities by its registrars, even when the abuse is an obvious violation of the accreditation contract, gives governments who want control over the internet a ready excuse to step in. The best way to ensure future independence by ICANN is for it to prove that it has a dispassionate, self-sustaining, transparent way of addressing compliance complaints that does not defy all common sense, thus enabling ICANN to credibly tell governments: We don't need you; we've got this under control.

Here, ICANN should look to other sectors that have found a way to implement voluntary compliance mechanisms as a model, including the private shipping sector, search advertising sector, and payment provider sector. For instance, the contract between Visa or MasterCard and the banks who process payments for those companies' credit cards contains basic requirements regarding certain types of high-risk merchants, and prohibits the bank from certain types of self-dealing, mostly obviously in furtherance of various types of illegality and known dangerous conduct. If a violation is found, the contract is enforced and the bank is penalized. Under this model, criminal enterprises are not permitted to simply become their own payment processing solution, and banks engage in reasonable voluntary compliance processes. If these other sectors are able to successfully implement voluntary procedures, it is unfathomable why ICANN cannot.

---

[13] This one is particularly absurd. You can argue that selling prescription drugs without a prescription is legal in Antarctica, or Somalia, or on the open seas, but that's not where the rogue internet pharmacies are doing business.

[14] I and others have explained in writing on several occasions, including in sworn testimony, why these excuses are nonsensical. In the interest of brevity, I will simply cite a couple of documents examining those excuses here: http://www.legitscript.com/download/Rogues-and-Registrars-Report.pdf, Pages 37-44, and https://judiciary.house.gov/wp-content/uploads/2016/02/LegitScript-John-Horton-House-Judiciary-Commitee-Testimony-05-13-15-1.pdf, Pages 19-20.

III. Conclusion: The Consolidation of Power

One reason that some internet users oppose continued oversight by the US (or any) government is the desire to free the internet from an unaccountable centralized authority. Put a different way, too much power in one place can be dangerous; too much power in one place without any accountability or transparency can be devastating.

These fears are valid. But internet users' fears about consolidation of power should not be limited to governments: these fears should be extended to ICANN, which is an institution with some powers comparable to those of a government, but without any accountability or transparency. Even more worrying, ICANN exercises these powers as a global monopoly. In matters of registrar conduct and behavior, ICANN is essentially able to act as the legislative, executive, and judicial branches rolled into one: because there is no transparency in its compliance process, there can be no checks and balances.

By virtue of its powers to determine who can sell domain names online and whether they comply with standards set out in the accreditation contract, ICANN has a significant effect on the future of the internet. And it is seeking additional powers that would further limit the openness of the internet. A working group hand-selected by ICANN's then-CEO has proposed a shift to put all of the world's information about who has registered domain names behind a single "gated" wall, and give ICANN or its contractor the sole power to determine who is authorized to see that data, and for what reason — and to "audit" and impose "penalties" against internet users who access the data for reasons that ICANN considers improper.[15] This is akin to having only one secret phone book in the world: the entity who controlled access to that phone book would have enormous power — too much power over internet users, I would argue— centralized in one unaccountable, non-transparent place. This proposal would put ICANN in the position of regulating, monitoring, auditing, and imposing penalties on internet users.

Proponents of the transition warn that "the credibility of the U.S. government and its commitment to the international community" are on the line.[16] This is nonsense. Before approving a transition, the US government has an obligation to internet users and the international community to ensure that ICANN's operations, including its compliance processes, are accountable and transparent. To date, ICANN has failed this test. I welcome any questions that the Committee may have.

---

[15] Information about the Expert Working Group convened to develop a framework to replace "Whois" information with a new system is generally available at https://community.icann.org/pages/viewpage.action?pageId=40175189; the full report of recommendations is available at https://www.icann.org/en/system/files/files/final-report-06jun14-en.pdf. Information about the "gated" access, and the proposal to "audit" and "impose penalties" on internet users who access domain name registration information for an "unauthorized" purpose is available throughout the document, especially at pages 10-11,

[16] See, e.g, http://www.politico.com/story/2016/09/internet-transition-icann-227864.