THE DOMAIN NAME SYSTEM

The Domain Name System (DNS) was first defined in 1983, and has been vital to the functioning of the Internet ever since. This is the scheme whereby Internet Protocol addresses — which are hard-to-remember numbers — are translated into easy-to-remember names. DNS is hierarchical in structure, global in scope, and works in an automated way so that most of the people who use browsers and email and other Internet applications have no idea that it is there, let alone understand how it works. It is enough that DNS is the magic glue so that someone types a URL into a browser or puts an address on an email, and it simply works. A domain name is an address like www.example.com. An Internet Protocol address looks like 192.168.188.166 (IPv4) or 2001:f38:1f70::b99:df8:7148:6e8 (IPv6). Human beings are much better at remembering and using names, whereas computers are by nature number crunchers. DNS bridges the gap for human beings as users of computers, by translating name addresses to number addresses, and vice versa. It is essential that DNS do this in a way that is accurate, and which makes sense to people. Since its foundation in 1983, DNS has been very successful because of its accuracy and sensibility, and it has become a global classification scheme on a par with that triumph of nineteenth century standardization, the International Postal Union. A big part of the common-sense validity of the Domain Name System comes from the concept of the top-level domain. A top-level domain is the largest-scale category of the name, giving the general sense of the kind of entity that has the name. The first top-level names were organizational, and applied only to the United States. They were .edu, .org, .net, .gov, and others. Educational institutions like universities belonged in .edu; non-profit, non-governmental organizations belonged in .org; Internet entities belonged in .net; governmental agencies belonged in .gov. Until the early 1990s, the Internet was restricted from commercial exploitation, so the top-level domain of .com was effectively a joke. When this restriction was lifted and when the World Wide Web

was invented by Sir Tim Berners-Lee, .com suddenly became serious, and registering a name under .com became an essential part of doing business and eventually to protecting trademarks.

The Internet became international in scope, and DNS expanded with it. Two-letter country codes derived from ISO standards became top-level domains. Now, top-level domains like .ca for Canada and .ua for Ukraine and .za for South Africa and about 200 other designations competed with the traditional organizational ones like .com. With the delegation of authority away from the United States-based university and military researchers, the clarity of DNS began to erode. Should a Canadian company register under .ca or under .com, or should it register under both? My own employer faced this decision, and was lucky to get its corporate trademark registered intact under both .ca and .com, but many other entities had to make compromises, with the result that a customer who is an Internet user does not have the old, comfortable assurances of where a name logically belongs.

Further weakening of DNS occurred with top-level country codes that belonged to states that were too weak to have a viable Internet, but who had two-letter combinations that because of their appearance were valuable as ersatz organizational domains. For example, the South Pacific island nation of Tuvalu has the top-level country code of .tv. To the 10,000 people who live on Tuvalu, the letters ".tv" probably mean Tuvalu, but to the almost 7 billion other people who live on our planet the letters ".tv" bring to mind the word "television." Accordingly, the .tv top-level country code was exploited, early on, by television stations and similar TV-related entities, for their Internet presence, even though that presence had nothing to do with a small South Pacific island.

The original organizational top-level domains such as .edu and .net have since been expanded in number by the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Assigned Numbers Authority (IANA). Names ending in .museum and .aero and .pro and others have joined the list, with varying rules of assignment and varying popularity in terms of adoption. Most recently, the top level domain .xxx was sanctioned, intended for adult entertainment entities. The intent of all of this expansion has been to internationalize and to democratize the Domain Name System, but its practical effect has been to devalue domain names. Before, there was an artificial scarcity, and so a domain like "sex.com" was considered valuable enough that somebody spent 13 million dollars for the right to use it. Now, companies looking to protect trademarks or secure coveted labels are registering in dozens of top-level organizational and country code domains, but it is an investment making diminishing returns.

One reason that chasing after prestigious domain names is becoming a nostalgic pastime is that search engines are now the primary means by which Internet users are finding what they want. It once was the

case that someone using a web browser would guess at a likely name address, and enter it manually in the URL field. It made sense for any business to want to have a named presence that was short, easy-to-remember, and made sense for the kind of entity that they were. Very few people type URLs any more, or even know what they are. Web users are clicking on links, and those links are pushed at them by search engines. There is no longer the requirement that the domain name in the URL be short and meaningful. DNS is still needed to resolve the domain name in a URL to an IP address, but the content of the domain name is of less importance for human eyes than it was before.

I said that DNS thrives because of accuracy and sensibility. I have addressed the issue of sensibility, arguing that the expansion of top-level domains and the increasing importance of search engines has eroded the primacy of short, meaningful domain names as the nonpareil sinecure of anyone's presence on the Internet. What I would not have expected is the need to address the issue of accuracy. The honesty of the Domain Name System as a reliable means to translate a name to a number and vice versa is now under attack from an unexpected source: the United States government. Yes, the U.S. government, which created the Internet through the Defense Advanced Research Projects Agency, is now considering hobbling DNS, by forcing authoritative bodies that control naming service servers to falsify their records. The Stop Online Piracy Act (SOPA) went before the U.S. Congress last year, and it had the backing of lobbyists from the old-line entertainment industries that have seen their monopoly power of distribution badly eroded because of the Internet. The bill sought to bring under criminal law the civil law torts that organizations like the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA) claim. SOPA would have forced search engines not to acknowledge an Internet presence that actually exists, forcng DNS servers not to do their jobs honestly — all at the behest of a "take-down order" issued by someone who claims rights to intellectual property. Thankfully, the immediate threat of SOPA was withdrawn, but the persistent threat of forcing DNS to tell lies remains.

This legalized hacking strikes at the very heart of the Internet. By cutting away at the integrity of search engines and DNS, SOPA and legal measures like it look to do damage to the electronic network economy that has grown up over the past twenty years. Laws like these are being made by people who do not understand the Internet (U.S. Representatives and Senators) at the behest of people who are afraid of the Internet (the old-line entertainment industry). An honest DNS is a bystander victim in the battle of old

media versus the Internet. If DNS dies because of legislated corruption, that would be a shame, as it has been a tremendous success, and it made sense for a long time. However, its demise would be the end of a long-term decline, because the Internet is evolving to new ways of connecting people with information by means of networks and computers. My hope is that SOPA and similar legislative attacks on the Internet in the U.S. and Canada continue to "miss the mark," because these are sledgehammer solutions to non-existent problems, and they cannot work because they don't match what is true about the way the Internet works. 28 years after DNS was invented, some people in power are finally becoming aware of what it is. They don't understand it, they don't like it, and they are afraid of it, and they may succeed in destroying DNS as an honest arbiter. They are too late, because the Internet is moving on, beyond the United States and beyond its twentieth century foundational principles. The Internet is dead — long live the Internet!

Source : https://www.exitcertified.com/blog/michael/2013/the-domain-name-system/