TOR EKELAND LAW PLLC

SUBJECT TO FRE 408
FOR DISCUSSION PURPOSES ONLY

9/27/18

MEMORANDUM FOR THE UNITED STATES ATTORNEY'S OFFICE FOR THE SOUTHERN DISTRICT OF FLORIDA

WHY URLS ARE NOT PASSWORDS

I. URLS ARE NOT PASSWORDS BY DESIGN, BY INDUSTRY STANDARDS, OR UNDER THE LAW

This case turns on whether lengthy, non-unique, publicly accessible Uniform Resource Locators ("URLs") used by Nuance Communications, Inc. ("Nuance") to locate the Protected Health Information ("PHI") on its network can reasonably be considered any type of computer password. If they can, then the government arguably has a case under the Computer Fraud and Abuse Act ("CFAA"). If not, the government has no CFAA case.

No court has ever held that a URL is a password or any type of access barrier. (*See* Memorandum of September 13, 2018). There is also no accepted common sense, technical, or legal understanding of passwords, or other authentication and authorization protocols, under which a lengthy, non-unique URL is considered a type of computer security. The government will not be able to meet its burden of proof in this case that unauthorized access occurred beyond a reasonable doubt, because there was no access authorization element in place.

Nuance publicly exposed the PHI of millions of Americans on the open internet. Now, it would deflect blame for its negligence by pointing to Mr. Stolowitz. But the fact

that Nuance did not have any computer security to protect the millions of PHI files it was entrusted to protect is the entire reason Mr. Stolowitz did what he did. He was taking steps to report Nuance's violation of the Health Insurance Portability and Accountability Act (HIPAA) to the U.S. Department of Health and Human Services (HHS) when he was raided by the FBI. This is evidenced by the draft report the government seized from him. Mr. Stolowitz is prepared to put the government to its burden in this matter, if necessary. No credible understanding of the URLs at issue here involves them functioning as passwords or as any type of access barrier.

The notion that a lengthy and non-unique URL functions as a password, or any type of authentication or authorization protocol, under the CFAA is wrong for numerous reasons, primarily: (1) it is contrary to the design and purpose of URLs; (2) it is contrary to computer industry standards; and, (3) it is technically incorrect as Nuance URLs were public and thus were crawled by automated web scraping and crawling programs.

A. URLs Are Designed to Access Resources, Passwords to Prevent Access

A URL is a locator, like a mailing address, that anyone with knowledge of can use to locate a resource on a network. That's the whole point of a URL. It's designed to make it easy to find and access resources online. Nothing in its design or function is intended to

exclude certain users, any more than knowing a mailing address can exclude certain visitors. The original white paper defining URLs only speaks of a URL as a uniform method for accessing resources on the World Wide Web. There is no discussion of a URL functioning to prevent access to files or functioning as any type of computer security. *See* T. Berners-Lee, L. Masinter, M. McCahill "RFC 1738 - Uniform Resource Locators (URL)" Network Working Group (Dec. 1994), available at https://tools.ietf.org/html/rfc1738. Indeed, this whitepaper specifically warns against embedding secret passwords in URLs. *See id.* Thinking of a URL as a type of password misunderstands what URLs are: addresses, not locks.

In contrast to the invention of the URL in 1994, computer passwords came about at MIT during the 1960s precisely to keep networked files private from other network users. See Robert McMillan, "The World's First Computer Password? It Was Useless Too." Wired (Jan. 12, 2012) available at https://www.wired.com/2012/01/computer-password/. A password is designed to exclude everyone from accessing a file except those properly possessing the password. It functions like a locked door or gate. And unlike a URL, knowing a password does not mean you know the address of the file that password

unlocks. In order to use a password, you need to know what it's a key to. The key is not the address, much like a mailing address is not the door or mailbox key.

No matter how difficult an address may be to remember, guess, or reach, it serves a totally different purpose than a barrier to access. A URL describes location, while a password controls access. URLs are meant to help someone access information on a network, whereas passwords are meant to exclude everyone but the password holder from accessing information on a network.

B. Industry Standards Do Not Recognize URLs as Passwords

Modern web standards reject the notion that URLs, even those containing complex strings, can be passwords.

1. The National Institute of Standards and Technology Definition of Password Doesn't Encompass URLs

The National Institute of Standards and Technology ("NIST") at the U.S. Department of Commerce defines a password as a "Memorized Secret authenticator … a secret value intended to be chosen and memorized by the user." Paul A. Grassi, et al., NIST Special Publication 800-63B, "Digital Identity Guidelines: Authentication and Lifecycle Management," at p. 12 "Authenticator and Verifier Requirements" (2017),

available at https://doi.org/10.6028/NIST.SP.800-63b." A URL, even one containing personal information in its query, is not a secret any more than a street address is. It is not chosen or memorized by the user, and does not authenticate identity in ways similar to the various authenticators outlined in the above NIST publication.

That URLs may contain information associated with specific documents or persons does not make them passwords. To see why, consider the NIST URL above. By changing the last letter in the URL to "a," NIST Special Publication 800-63A is called up by the user's browser. This does not require any authentication or authorization. And just like in Nuance's case, once you know one URL you can easily guess all of them by simply adding or subtracting letters or numbers to the URL string. This is another reason URLs and passwords are fundamentally different. If you know one password this does not necessarily mean you know all the other passwords for a system. But if a user knows one Nuance URL, they can guess all others through simple addition and subtraction, and gain easy access to millions of private health files.

2. HIPAA Does Not Recognize URLs as Passwords

HIPAA requires "technical security measures" to "guard against unauthorized access." In no interpretation of HIPAA is a long or complex URL a technical security

measure. An HHS circular on security standards is informative on this topic. It counsels for using both authentication and authorization protocols, alongside encrypting information where appropriate. *See* HHS, Center for Medicare and Medicaid Services, vol. 2, paper 4, rev 3/2007, "HIPAA Security Series Circular 4: Security Standards: Technical Safeguards," available at: https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf. This circular outlines numerous ways to secure PHI in compliance with HIPAA: (1) access controls; (2) unique user identification; (3) emergency access procedures; (4) automatic logoff; (5) encryption; and (6) authentication (pp. 3-4, 9-10)). Nuance used none of these methods to protect the PHI it was required by law to protect.

First, a URL is not any type of access control because it is a resource address, not an access barrier. Once you had one of Nuance's URLs, you knew all of them by simply adding 1 to the numeric URL string. Access controls typically requiring logging on to a system by entering a username and password. The notion that a lengthy URL is a form of access control will not hold up to expert scrutiny at trial. To date, there is no evidence that these URLs were anything but readily and publicly available.

Second, a URL is not a form of unique user identification, because it does not identify a user any more than possession of someone's home address identifies a visitor. A URL says nothing about the accessor of a file. Rather, it only says where the file a user wants to access is.

Third, Nuance had no emergency access control, because there were no access controls.

Fourth, there was no automatic logoff, because no logon was required to obtain access to Nuance's PHI.

Fifth, there was no encryption, which would have rendered the files unusable even if they were accessed.

Sixth, there was no authentication required to access the PHI. All that was needed was the URL. There was no IP Address white listing, no VPN or proxy blocking, no username requirement, nor any other authentication required to access the PHI.

Simply put, the government will not be able to prove beyond a reasonable doubt that there was any unauthorized access because, among other things, there were no

authorization or access protocols in place that any reputable computer security expert would recognize.

C. Nuance's Unsecured Servers Were Crawled and Indexed

Nuance attempts to deflect blame from the fact that it exposed private patient medical records on the open internet by claiming that a lengthy "hard-to-guess" URL protected them. But it is an indisputable fact of the internet that bots, both innocent and malicious, are constantly crawling and indexing the publicly available information on the internet. And our initial research indicates that Nuance publicly facing servers were crawled and indexed during the period in question. This means that the PHI was publicly and readily available no matter how hard the URLs were for a human to guess.

Automated crawling forms the basis of most search engines. Google, for example, uses complex web crawling software in order to pull and index content into a searchable database. In order to avoid having your website crawled by Google, a website has to opt out. The same is true with Microsoft search engine Bing, and most other search engines. Under the government's theory in this case, both Google and Microsoft are violating the CFAA with their search engine crawlers. As are all bots crawling the internet, whether innocent and malicious, simply for accessing “hard-to-guess” resource locators.

CONCLUSION

Nuance made millions of private medical records publicly accessible on the open internet. It failed to use even basic authentication and authorization procedures familiar to every juror – a logon that requires entering a username and password. If the government proceeds with this prosecution, it must prove beyond a reasonable doubt that a URL is an access barrier. It will have to do this in the face of the facts that Nuance had no access controls, authorization protocols, or encryption in place to protect private medical records the law required it to protect, and that the public entrusted to its safe keeping.

No reasonable juror is going to believe Nuance's story that a lengthy URL is a form of computer security, nor has any court ever so held. The government faces an uphill battle in this case proving that there was any computer security at all protecting these files. Nor will the government be able to point to any evidence that Mr. Stolowitz was attempting to sell or do anything with the PHI except report Nuance's public exposure of sensitive, private medical data. The jury will see this for what it is: Nuance deflecting blame for its negligence in betraying the public trust.