KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

# IS BREAKING WEB ENCRYPTION LEGAL?

**2015-02-20**

Companies finding ways to subvert Internet encryption have been in the news recently. Last month, in-flight Wifi provider Gogo was caught intercepting encrypted web sessions on YouTube and other video sites in order to throttle high-bandwidth users. And earlier this week, it was revealed that Lenovo was installing adware on laptops that intercepted *all* encrypted web requests in order to inject targeted ads into encryption-protected sites. A lot has been written about bad these practices are for consumer security – but are they even legal? The law is far from settled, but I believe that absent *very* clear disclosure to users, breaking encryption likely violates — at the very least — consumer protection law that prohibits deceptive and unfair business practices. Given how important robust encryption is to the privacy of our communications, it is incumbent upon regulators to enforce these regulations on companies that undermine the security of the Internet.

## How Is Encryption Supposed to Work?

*First, a very abbreviated background on what's going on here (feel free to skip ahead if you know this already).* On the web, encryption is typically achieved through use of the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols[1]; these technologies enable users to communicate with websites privately without surveillance by network providers, malicious hackers, or other intermediaries.

Under normal circumstances, when a user connects to a website over an encrypted SSL connection (the web address will begin with "https://…"), the user's browser initiates a "handshake" with the website's server in which the two sides decide on a variety of parameters for the encrypted communication. During this handshake process, the user's browser first requests the site's public encryption key and then checks to see if the site is trusted by a certificate authority. Certificate authorities are trusted third party vendors — such as Symantec or Comodo — that certify the identity of the operator of a website, and technically assure the user's browser that the site's public key is legitimate.[2] Using the site's public key, the user's browser sends a communication back to the originating site (which can only be decrypted with the private key, possessed only by the site operator) negotiating the parameters for and then initiating a symmetrically encrypted session with

[1] SSL is an older protocol and for the most part currently unused. TLS is the equivalent modern version of that protocol. Throughout this letter we will use the abbreviation SSL as shorthand for both SSL and TLS, as SSL is often used to refer to SSL or TLS.

[2] Technically, the certificate authority cryptographically signs a copy of the site's public encryption key along with some other basic identifying information such as the website's domain name. This signed copy of the site's public key and associated metadata is called an SSL certificate.

the site, during which communications between the site and the user are both encrypted, and cannot be viewed by intermediaries.

In setting up this encrypted session, an intermediary network transmitting the user's requests and subsequent communications should not be able to see the contents of that communication; they'll be able to discern some basic attributes of the communication — including the destination IP address and domain (e.g., YouTube.com) — but won't know the actual url (e.g., YouTube.com/JustinBieberBelieve) or the contents of the particular page visited.

Of course, the weakness of encryption is that is relies upon these certificates in the first place. Intermediaries that sit in between the user and the web — such as Gogo and Lenovo — have the opportunity to issue their own certificates for various sites, representing that they operate those sites. Thus, Gogo's network posed as YouTube, and presented a fake, self-generated SSL certificate to the user's browser indicating, erroneously, that it operated YouTube and other Google web domains. (Technically, Gogo's network presented a fake certificate for *any* *.google.com domain, encompassing far more than merely Google's YouTube site.) As a result, Gogo was able to inspect traffic to YouTube and determine it was video (Gogo blocks video sites because of bandwidth constraints on planes). Worse still, Lenovo allowed its advertising partner Superfish to pose as *any* website in order to insert targeted ads into encrypted webpages.

Intermediaries thus have the opportunity to take advantage of their privileged position as a network intermediary to pose as a destination website in order to intercept and inspect encrypted communications. In computer security, this is commonly called a "man-in-the-middle" attack: an entity sitting between two other parties who are trying to communicate with each other (here the user and YouTube) intercepting, inspecting, and potentially altering those communications, and posing to each party as the other party. And that is what happened in these cases — the intermediary posed as the destination site to the end user, and it posed as the end user to the destination site, decrypting and then reencrypting traffic between the two destinations. As a result, they were able to view the unencrypted communications between the two in a way that it could not have if it hadn't falsely issued certificates for those domain. In doing so, they also — especially in the case of Lenovo — made it much easier for other parties to pose as destination websites and intercept encrypted traffic (more about that in a bit).

**OK, So Is That Actually Legal?**

There might be a few statutes where you could make a legal case that this behavior is illegal (the Wiretap Act, for one), but I'm going to focus on Section 5 of the Federal Trade Commission (FTC) Act. While most nations around the world have comprehensive data protection law, the United States is an outlier; the US only protects certain sensitive categories of information through sector-specific laws like HIPAA (health), Gramm-Leach-Bliley (finance), and FERPA (education). That said, using its decades-old consumer protection authority under Section 5, the FTC has been the *de facto* privacy and security regulator in the U.S. in recent years. Broadly speaking, Section 5 prohibits companies from engaging in *deceptive* or *unfair* business practices; the FTC (and state Attorneys General under similar state laws) have applied this standard to dozens of privacy and security cases in recent years (for a full exploration, consider this excellent article by Professors Dan Solove and Woody Hartzog). Under these precedents, there is a very strong argument that breaking encryption will in many cases violate this statute.

*Is Breaking Encryption Deceptive?*

There are a couple arguments for why this behavior might be considered a deceptive business practice.

At a technical level, these SSL-breaking technologies trick your browser by forging SSL certificates, implying that their service operates encrypted websites like YouTube.com and BankofAmerica.com. In fact, instead of passing encrypted traffic on to the appropriate destination, these technologies enact the previously described "man-in-the-middle attack," gaining access to potentially sensitive information that should rightly be kept between you and, for example, your bank or health care provider. Though these practices do not directly deceive the end user, they do effectively deceive the user's software that acts as a "user agent." It's not settled that this is prohibited by deceptive practices authority; in the past, the FTC has been reluctant to pursue deceptive practices cases merely on the grounds of tricking a browser: the FTC declined to pursue companies that issued bogus machine-readable P3P policies to get around Internet Explorer privacy restrictions or against companies that evaded Apple Safari's default cookie settings in order to place third party cookies.[3] On the other hand, six state Attorneys General did bring a deceptive practices claim under their own version of Section 5 against companies that tricked Safari browsers into accepting third-party cookies.

Alternatively, the FTC could argue that failure to disclose that encrypted transmissions were being intercepted constituted a *material omission* — that is, failure to explain the practice would be a deceptive means to prevent a consumer from meaningfully evaluating the product. The FTC has brought a number of cases arguing that failure to disclose highly invasive or controversial practices either in a privacy policy or in clear, upfront language could constitute a deceptive practice. For instance, the FTC has found that failure to disclose access to your phone's contact information or precise geolocation could constitute a material omission.

From what I can tell, neither Gogo nor Lenovo went out of their way to tell users about these practices. If anything, Gogo's privacy policy would lead users to think that their SSL-protected communications were safe from eavesdropping.

For Lenovo, a post to one of its user forums says that users had to agree to the Superfish privacy policy and terms of service. I don't know what these documents said exactly, though the Superfish documents available on their website say nothing about these practices. Even if Lenovo had disclosed in fine print what it does, regulators could make the case that SSL interception was so controversial that permission needed to be obtained outside of a boilerplate legal agreement. A service could certainly try to make a

[3] The FTC's only action [http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented] against a company for evading Safari's cookie controls was not based on the underlying conduct, but instead was premised on an erroneous FAQ page that stated that the company couldn't place cookies on Safari browsers.

value proposition to consumers that some feature was worth the cost of breaking web encryption – but that's not what happened here.

Moreover, after-the-fact statements that dismiss the significance of the vulnerability (such as "We have thoroughly investigated this technology and do not find any evidence to substantiate security concerns,") are unlikely to help. By the same token, telling (or implying to) consumers that uninstalling the software will solve the security problem could also be deceptive; the FTC has previously found that offering opt-out solutions that don't work can be deceptive.

*Is Breaking Encryption Unfair?*

The FTC may have an even stronger case under unfairness, at least in the case of Lenovo. The "unfairness" prong of its authority is where the FTC has brought most of its enforcement actions for weak data security practices — over fifty since 2005. In order to be "unfair" under Section 5, a business practice has to meet three criteria – it must:

1. Cause significant consumer harm,
2. Not be reasonably avoidable by consumers, and
3. Not be offset by countervailing benefits to consumers.

If breaking encryption exposes consumers to significant security vulnerabilities, regulators will likely have a very strong case for an unfairness violation.

On causing significant harm, this seems fairly straightforward in Lenovo's case: its partner Superfish configured its software to intercept all SSL requests — *using the same decryption key across all devices*. This key was easily reverse engineered soon after the story broke, meaning that any malicious attacker could use this key to intercept *any* encrypted communication. That's a huge security vulnerability, and at least as concerning as several other vulnerabilities that the FTC has previously alleged to have harmed consumers. Gogo's SSL interception also raised security concerns — it arguably inures users to security warnings and exposes them to attackers posing as Gogo's network — but the risk is probably not as great as in the Lenovo case. The FTC has brought actions against device manufacturers in the past for weakening security; in its case against phone manufacturer HTC, the FTC alleged that badly designed software that let app developers piggyback on HTC's access to certain phone functionality without user permission was an unfair business practice.

On the second part of the unfairness test, it's hard to argue how these practices are avoidable by ordinary consumers. They may have clicked though legalistic agreements, but as far as we can tell, none of these documents made any disclosure about these sorts of tactics — or the vulnerabilities to which they exposed consumers. Certainly, neither Gogo nor Lenovo presented information outside of a legal document where consumers were likely to notice. As a result, consumers weren't provided with actionable information that they could have used to avoid these problems.

Finally, it's hard to see that the security vulnerabilities introduced by SSL-interception were outweighed by any benefits to the practice. Gogo used this tactic to block bandwidth-heavy video applications on planes with limited internet access — a worthy goal, but one better accomplished through less destructive means. Lenovo allowed its partner to break encryption in order to view private communications for targeted advertising.  It is doubtful that many consumers would find this trade-off beneficial, even if it lowered prices significantly; in any event, Lenovo claims that they didn't make much money from its deal with Superfish, and the pre-installed adware was simply designed to improve the user experience. Since exposure of these practices, both companies have backtracked and ended use of the encryption-breaking technologies.

*So Will Regulators Take Action?*

We don't know yet whether the FTC — or a state Attorney General — will take action in either of these cases. At least in the FTC's case, investigations are confidential and often take several months (if not longer).

One factor to consider is whether a company has remediated its behavior.  Regulators will often be less interested in bringing a case against a company that voluntarily ceases the practice prior to contact. Gogo, at least, appeared to act pretty quickly in response to press attention to its interference with SSL; by at least January 13 (eleven days after initial media reports), it was telling people that it had completely ceased the controversial practice.

Lenovo's case is trickier — Lenovo claims to have stopped shipping Superfish-infected machines, but apparently stores are still selling Lenovo products with Superfish installed. Moreover, machines that were already sold still have this vulnerability in place — and Lenovo does not have the ability to remotely fix the root certificate authorities on these computers. They may be able to release a patch for consumers to download, but consumers will first have to know about the problem and solution first; alternatively, they may have to partner with OS and browser makers to update their software. In fact, Microsoft already appears to be using the built-in Windows anti-virus software, Windows Defender, to remove Superfish as well as remove any bogus certificates immediately – an important step.

Probably the biggest factor that regulators consider in bringing cases is the deterrent effect they will have on the rest of the industry. Given the fundamental importance of web encryption and the sudden willingness of certain companies to break it, this seems like an area where the FTC or others need to step in.[4]  Otherwise, consumers won't be able to trust the privacy of their online communications, resulting in a fundamental lack of trust in the internet. Regulators cannot let that happen.

[4] Interception of SSL requests is somewhat more common in some education and enterprise environments, where a school or employer wants to restrict access to certain content. Though these practices raise privacy and security issues, there is an argument that this sort of behavior is more expected in these environments. In any event, schools and employers are likely not covered by the FTC's consumer protection statutes discussed here.