From the Bench

SCOTUS Will Hear DOJ Plea for Microsoft's Overseas Emails

The Supreme Court of the United States agreed on October 16 to hear a Department of Justice appeal of a decision protecting Microsoft's privacy of emails stored on company servers overseas.

The 2nd U.S. Court of Appeals in New York earlier ruled that the emails, stored in Microsoft servers in Dublin, Ireland, are off limits, but the Trump administration—backed by 33 states and Puerto Rico—appealed to the U.S. Supreme Court arguing that the lower court's ruling "gravely threatens public safety and national security" and hurts feds' ability to "ward off terrorism and similar national security threats and to investigate and prosecute crimes."

The case centers on federal prosecutors' ability to obtain emails pertinent to a drug trafficking investigation. The 2nd U.S. Court of Appeals ruled the emails fell outside the purview of U.S. domestic search warrants, even though the company is based in the United States, citing the 1986 Stored Communications Act.

Microsoft has received support from dozens of technology and media companies as well as some unlikely bedfellows: the American Civil Liberties Union and the U.S. Chamber of Commerce. The information technology sector is concerned that giving prosecutors access to overseas servers could make customers less likely to use cloud services over privacy fears.

Health Held Hostage

Medical device ransomware is the new professional-liability reality hospitals and other health providers face.

By Sandra Brown and David Langolf

For years, the legal industry has been warning that hacking of medical devices is the next security nightmare. In May 2017, the first medical devices were hit by ransomware in U.S. hospitals, making this nightmare a new reality.

Sandra Brown

Ransomware is malicious software designed to prevent or limit users from accessing their system until a sum of money is paid. Most ransomware attacks target computer systems, blocking use of emails or files. However, ransomware can affect any type of device that is connected to the internet, making electronic medical devices a target for attacks.

David Langolf

Hospitals have been victims of ransomware attacks before. In February 2016, a Los Angeles hospital paid approximately $17,000 in bitcoin to a hacker who seized control of the hospital's computer systems and would restore access only when the ransom was paid.

The stakes are raised, however, when a cyber attack goes beyond affecting hospital computer systems and locks medical devices. In May 2017, the WannaCry ransomware attack hit worldwide, targeting computers running the Microsoft Windows operating system, encrypting data and demanding ransom payments in bitcoin. The WannaCry attack affected over 65 hospitals in the United Kingdom and up to 70,000 devices—including computers and MRI machines—causing some hospitals to run on an emergency-only basis during the attack. The very next month, a Pittsburgh hospital was hit

London Market Builds High-Tech Tracking Systems

The London Market Association's Claims Committee plans to fund a satellite imagery and intelligence service for all Lloyd's managing agents to bolster claims processes and exposure management for natural catastrophes. McKenzie Intelligence Service is working with the LMA and Lloyd's to develop the technology across multiple classes of business to allow claims professionals to manage and adjust claims remotely via MIS's custom-built portal. The LMA Claims Committee has also approved establishing a Claims Expert Management Hub for Lloyd's carriers so they can better assess the cost-effectiveness of their use of claims experts while tracking against budgets. The hub will focus on better data capture to manage the use of lawyers, adjusters and other third-party experts throughout the life of a claim. The group will use a single solution that will integrate with Lloyd's central market systems. The LMA and Lloyd's hope to help managing agents improve claims strategy, outcomes and customer experience. ■

in a major cyber attack using another ransomware.

Whereas the WannaCry hackers' motivation appears primarily financial in nature, many types of cyber attack are less obvious. Destruction of data, theft of medical records, doxxing (malicious publication of private or identifying information about an individual), botnets, etc. are all potential motivations for attackers. Insecure medical devices and non-medical devices (e.g., industrial control systems, security cameras or appliances) that either temporarily or permanently connect to a hospital's network are all potential points of attack and expose the hospital's staff and patients to possible harm. Essentially any device that connects directly or wirelessly to a network is at risk for a ransomware attack.

The vulnerability of medical devices threatens not only the confidential information but also the safety of patients. Pacemakers and insulin pumps are two examples of connected medical devices. A motivated ransomware attack could target these, threatening the health and safety of patients. Several incidents have occurred over the years, including the well-known example of former Vice President Dick Cheney, who asked his doctors to disable the wireless component of his pacemaker because he was worried about a cyber attack against his heart. The WannaCry attack proves that this is not just paranoia, as medical devices can now be remotely hacked. A medical device can also serve as an entry point to larger hospital networks.

The growing threat of cyber attacks has led the FDA to regulate medical devices. The first FDA guidance for designing new products came out in 2014, and late last year, the agency released guidelines for products that are already in the market. The guidance stipulates that devices should be designed to be secure, to be able to be updated if flaws are found, and to be safeguarded in case of an attack.

On Oct. 28, 2016, the Library of Congress updated the Digital Millennium Copyright Act (DMCA) to provide an exemption for security researchers acting in good faith to conduct research on consumer devices. The Library of Congress approves exemptions on a temporary basis, and exemptions must be renewed. If that exemption were revoked, third-party research on medical device security vulnerabilities would be illegal under the DMCA.

The issue for many hospitals remains that they rely on old, unsupported systems. A medical device is expected to live in the field for 30 years while the underlying software components have a much shorter lifespan. Hospitals also tend not to invest in qualified cyber-security personnel and, therefore, are not following technological threats and advances as assiduously as needed. This combination makes hospitals an easy target for ransomware attacks. Hospital policies need to be evaluated. Devices and systems should be updated with suitable technology. Upgrades on medical devices should be performed as recommended. And knowledgeable IT personnel should be on staff to monitor potential threats. Having IT personnel is crucial, because, if an attack happens, they will be in the best position to mitigate the damage of the attack.

Perpetrators of ransomware attacks have cleverly set the price to decrypt victims' data relatively low when compared to the high cost of the loss of data and the high cost of liability in the aftermath. It's the victim's willingness to pay combined with the widespread use of network-connected devices that makes it unlikely we'll see these types of attack go away anytime soon.

As the technological landscape surrounding medical devices quickly evolves, the liability ramifications for doctors, administrators, hospitals and device manufacturers also expands into uncharted territory. All professionals involved in patient care should work towards best practices regarding exposures associated with network-connected devices involved in patient care and facility operations. ■

Sandra Brown is an attorney at Kaufman Borgeest & Ryan. sbrown@kbrlaw.com

David Langolf is assistant VP, CNAX Finance, at Arch Insurance Group. dlangolf@archinsurance.com

Russian Antivirus Software Used by Russian Hackers: Go Figure

Russian cyber spies have been using Moscow-based Kaspersky Lab antivirus software to gain access to the firm's customer databases and source code, which could enable cyber attacks against government, commercial and industrial networks. Israeli counterintelligence discovered the activity in 2014 and reported it to its U.S. counterparts, but it was just this September that the U.S. ordered Kaspersky software pulled from federal computers. Kaspersky denies knowledge of or involvement in the Russian intrusions.

The vulnerability of medical devices threatens not only the confidential information but also the safety of patients.