Strategies for Businesses Protecting Electronic Data within California: Part Three

06.24.2015

Part Three: Stored Communications Act, 18 U.S.C. § 2701 Et Seq.

In Parts One and Two of this e-alert series, we discussed the federal Computer Fraud And Abuse Act ("CFAA") and its California corollary the California Computer Data Access And Fraud Act (CDAFA). In Part Three, we provide a presentation of the federal Stored Communications Act, 18 U.S.C. 2701 et seq. ("SCA"). The act is similar to the CFAA; however, unlike the CFAA, the SCA provides for the recovery of attorney's fees and does not contain a minimal loss requirement. We conclude this e-alert with suggested best practices for preserving data security.

Congress enacted the Stored Communications Act ("SCA") in 1986 as Section II of the Electronic Communications Protection Act (18 U.S.C. § 2701 et seq.):

> The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, *cf. Prosser and Keeton on the Law of Torts* § 13, at 78 (W. Page Keeton ed., 5th ed. 1984), the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility.

In applying the CFAA and the SCA, federal courts have noted that their general purpose was to create a cause of action against computer hackers (e.g. electronic trespassers).

1. Summary of Prohibitions

The SCA creates criminal and civil liability for certain unauthorized access to stored communications and records. Among other things, the act creates a private right of action against anyone who "intentionally accesses without authorization a facility through which an electronic communication service is provided; or

intentionally exceeds an authorization to access that facility, and thereby obtains, alters, or prevents authorized access to wire or electronic communication while it is in electronic storage in such system. . . ." "Electronic storage" means either "temporary, intermediate storage incidental to electronic transmission, or storage for purposes of backup protection.
As noted above, under Section 2701(a), in order to state a claim under the SCA, a plaintiff must allege that the defendant accessed without, or in excess of, authorization a "facility through which an electronic communication services is provided." An "electronic communication service" is any service which provides to users thereof the ability to send and receive wire or electronic communications. There is a split of authority on whether an individual's computer, laptop or mobile device fits the statutory definition of a "facility through which an electronic communication service is provided."

2. Without, Or Exceeding, Authorization

Federal courts have interpreted the meaning of "without authorization" and "exceeds authorized access" in the same way that they have interpreted use of those terms under the CFAA.

3. Damages and Other Relief

While there are similarities between the CFAA and the SCA, there are some significance differences. There is no minimum damages requirement under the SCA. In fact, the SCA provides for a statutory damages award of at least $1,000, presumably per violation. The SCA further empowers the court to assess punitive damages for willful or intentional violations. The SCA explicitly provides for a disgorgement of profits, while such disgorgement is only implicit in the CFAA's provision for "equitable remedies." Unlike the CFAA, the SCA provides for recovery of reasonable attorney's fees. Like the CFAA, the SCA provides for "such preliminary and other equitable or declaratory relief as may be appropriate." Also, similar to the CFAA, the limitations period under the SCA is "2 years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation."

The CFAA, California Penal Code Section 502 and the SCA provide a helpful triumvirate for businesses seeking to remedy an unlawful data breach. The federal acts provide a basis for federal court jurisdiction which is likely to result in speedier relief. Both the California statute and the SCA provide a basis for claiming attorney's fees and the California statute allows for an award of a penalty by way of exemplary damages.

While businesses can use these statutes as tools for remedying data breaches, the best case scenario is exercising data security best practices to avoid reliance on the statute in the first place. Below is a set of best practices we recommend.

Best Practices: An Ounce of Prevention

1. Conduct an annual security assessment using either a third party consultant or in-house expertise and establish and implement a security plan and policy.
2. Audit third party vendors where feasible, particularly those that provide in-house services such as filing, copying, mailing and production services.]
3. Periodically change employee passwords and assure that the passwords are complex.]
4. For remote access to computer systems, have two-factor or two-step authentication. Two-factor authentication is a process involving two subsequent but dependent stages to check the identity of someone trying to access services on your network and systems. An example is use of an ATM card (something you have) and a PIN (something you know) to access one's bank account at an automated teller machine. Another example is

requiring input of a user ID and password and then a single use code or PIN sent to another device such as the user's mobile phone or tablet.

5. Use encryption for data at rest and data in transit. Encryption protects your data and allows client server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. Encryption methods include encrypting your computers' hard drives; implementing "Transport Layer Security ("TLS") for email delivery; and using "Secure Sockets Layer" ("SSL") VPN connections when connecting remotely to your network.
6. Ensure that your software is up to date.
7. Have a clearly defined policy in an employee manual regarding confidentiality and use of company information both electronic and otherwise.
8. Have employees execute confidentiality agreements at the time of hire.
9. Immediately disable logins and electronic passwords of separated employees.
10. Clearly identify trade secret information and limit access to it.
11. Formalize agreements in writing with outside technical consultants making it clear that the business owns any software developed, including written materials; the consultant's access to electronic systems may be terminated at any time; and the consultant shall not lock the business out of access to its computer system.

Should you experience any data breach, the attorneys at Nossaman stand ready to assist you in remedying the consequences of that breach.