

New State Privacy Laws: Regulating the Use of Social Security Numbers and Requiring Wireless Security Warnings

EXECUTIVE SUMMARY

In the last few years, growing public concern over identity theft and electronic information breaches has prompted many states to reexamine their existing privacy regimes and supplement those regimes with new mandates. California leads these efforts with initiating regulations that focus on a business's use and disclosure of a consumer's Social Security number ("SSN"). At least 16 states, including New York, have enacted their own laws following California's example. In addition, California recently enacted a law that requires manufacturers of wireless network devices to include specific disclosures on the devices that warn consumers of wireless security risks. If the past is a model, we may soon see other states follow suit with similar disclosure requirements. This alert summarizes these new requirements in more detail.

RESTRICTIONS ON USE OF SOCIAL SECURITY NUMBERS

CALIFORNIA STARTS THE TREND

As it has with many other privacy requirements, in 2001, California enacted the nation's first comprehensive law regulating companies' use and disclosure of SSNs. Its principal objective was to curb easy access to the SSN identifier, because, together with date of birth and mother's maiden name, it permits identity thieves to obtain loans under the stolen identity, access bank accounts, create false identification cards, and commit other acts of fraud. The California

SSN law became fully effective in July 2005 and prohibits businesses and individuals from:

- Posting SSNs or making them available to the general public (online or offline);
- Requiring consumers to transmit a SSN over the Internet unless the connection is secure or the number is encrypted;
- Requiring consumers to log onto a website using a SSN without a password;
- Printing SSNs on identification cards or badges; or
- Printing SSNs on anything mailed to a consumer unless required by law or the document is a form or application.

The law contains a few limited exceptions. Significantly, it allows businesses and individuals to continue using SSNs for internal verification and administrative purposes provided they have reasonable procedures in place to protect the confidentiality and security of the personal data.

In addition, the law contains a narrow grandfather clause: if the business or individual was using a consumer's SSN before the law was enacted in a way that would not comply with the law's requirements, the business or individual may continue such use if:

- The use is continuous without any interruptions;

- Annual disclosures of such use are provided to the consumer, along with an opportunity for him/her to opt out of such use;
- The business or individual promptly stops using the SSN in response to a consumer's written request to stop; and
- The business or individual does not deny services to a consumer who makes the opt-out request.

Note that while the California SSN law focuses specifically on the use and disclosure of SSNs, these types of obligations are already imposed on businesses regulated by the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA).

To address this concern, many businesses over the last few years have voluntarily replaced customer identifiers with a number other than the SSN, changed website log-ins so that consumers may not use their SSNs as an identifier, and restricted use of the SSN for internal and administrative use only. The California SSN law makes those types of voluntary efforts mandatory.

AT LEAST 16 STATES FOLLOW CALIFORNIA'S LEAD

After California enacted its law, at least 16 other states have enacted their own SSN laws, and many more have introduced similar legislation over the past few years. We anticipate more states will continue this trend. For the most part, the state SSN laws are a close replica of California's model, including those enacted in Arizona, Arkansas, Connecticut, Illinois, Maryland, Michigan, Minnesota, Missouri, New

Mexico, New York, Oklahoma, Texas, Utah, and Virginia.

But some differ on the details. For example, some states limit the application of their SSN laws to certain business sectors. Utah's SSN law, while similar to the California model, applies only to insurers, and Oklahoma's law focuses its provisions on employers' practices.

Other states add additional requirements. In New Mexico, the SSN law includes language that is similar to California's law, but, in addition, it (1) prohibits businesses from requiring a consumer's SSN as a condition for the consumer to lease or purchase products or services from the company; and (2) requires the company to implement policies that limit access to SSNs to authorized employees and to hold such employees responsible for unauthorized release of SSNs.

In Rhode Island, the SSN law is more narrow than the California model. It prohibits a company from requiring a consumer to disclose his or her SSN in order to purchase goods or services, or to disclose his or her SSN or driver's license number as a condition of receiving a discount card.

The cost of non-compliance can be significant. In Illinois, improperly using or disclosing a consumer's SSN is an unlawful practice under the state's Consumer Fraud and Deceptive Practices Act, permitting both private and attorney general actions. As a result, a company that violates the law could be subject to actual damages, restitution, injunctive relief, and civil penalties of up to \$50,000 (or up to \$60,000 if the conduct affects individuals over 65 years of age) per violation. New York's law provides for thousands of dollars in civil

penalties if its SSN law is violated, and Rhode Island treats violations as a misdemeanor criminal offense and permits civil damages, attorneys' fees, costs, and injunctive relief. Other states provide for similar remedies, varying mostly with respect to the extent of civil penalties and damages. Because the laws are relatively new, examples of violations have yet to emerge. That said, regulators and the private bar are certainly aware of these laws. We expect to see several cases brought in the latter part of 2006 and in 2007.

CALIFORNIA ENACTS WIRELESS SECURITY DISCLOSURE LAW

On September 30, 2006, Governor Schwarzenegger approved California Assembly Bill 2415, which is intended to provide additional protections to consumers who use wireless networks in small offices, home offices, or in their homes. Acknowledging the increased risk to personal information presented by unauthorized access to wireless networks, the law requires that manufacturers of wireless network devices sold in California implement policies to increase the security of these networks. The Act applies only to devices manufactured after October 1, 2007.

Under the new law, any wireless network device that includes integrated and enabled wireless access points and is used in federally unlicensed spectrum must be manufactured to include one of the following:

- A security warning that appears during the device's configuration process that informs consumers of the risk to personal information presented by unsecured wireless networks and provides information on how to secure the net-

work to prevent unauthorized access;

- A temporary warning sticker, which must be removed by the consumer before using the product, and which provides information on how to secure the wireless network;
- Additional notice that informs the consumer of the risks of wireless networks, presents information on how to avoid these risks, and requires affirmative action by the consumer before the product can be used; and
- Other measures that protect a user's wireless network connection from unauthorized access.

The law does not identify whether non-compliance would subject a business to statutory penalties or private actions. Those details are likely to be worked out in subsequent litigation. Accordingly, to avoid leading that charge, if your business is involved with the manufacturing and sale of wireless devices in California, you'll want to take note of these new disclosure requirements and ensure that your business is complying with them.

* * *

Although these recent state mandates may require some adjustments to current business practices, they are a helpful reminder that privacy and data security compliance is not a static check-list. New legal obligations, evolving technology, and a recognition that there are bad actors intent on breaching unsecured personal information mean that a privacy and security program should be dynamic. Businesses would be well served by taking steps that reflect an awareness of these factors and proactively responding to them.

KELLEY DRYE COLLIER SHANNON

ADVERTISING AND MARKETING
PRACTICE GROUP

Kelley Drye Collier Shannon's Advertising and Marketing practice comprises attorneys with proven success in advertising litigation and NAD proceedings; expertise in the area of advertising, promotion marketing, and privacy and data security law; and experience at the FTC, FDA, and the Offices of State Attorneys General.

We are a leader in advising clients on information privacy issues and have been at the forefront of developments in this growing area of law. Our privacy law group regularly advises clients regarding all aspects of privacy and data security law, including the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act, the Children's Online Privacy Protection Act, the EU Data Protection Directive (as well as EU members' state laws and the Safe Harbor negotiated between the US and the EU), the FTC Act, and state privacy and data security laws.

GOVERNMENT RELATIONS AND
PUBLIC POLICY PRACTICE GROUP

Our Government Relations practice helps clients interpret and shape governing laws, enabling them to maintain or achieve market leadership. Our experienced privacy attorneys work closely with our Government Relations and Public Policy practice group to stay abreast of new laws and regulations.

FOR MORE INFORMATION

For more information about this development, please contact one of our team members at (202) 342-8400 or via email:

Partners

Steve Augustino	SAugustino@KelleyDrye.com
Reed Freeman	RFreeman@KelleyDrye.com
James S. Gilmore, III	JGilmore@KelleyDrye.com
William C. MacLeod	WMacLeod@KelleyDrye.com
Joel Hewer	JHewer@KelleyDrye.com
Lewis Rose	LRose@KelleyDrye.com
John E. Villafranco	JVillafranco@KelleyDrye.com

Associates

Christie Grymes	CGrymes@KelleyDrye.com
Jeffrey A. Kauffman	JKauffman@KelleyDrye.com
Jason K. Levine	JLevine@KelleyDrye.com
Gonzalo Mon	GMon@KelleyDrye.com
Dustin Painter	DPainter@KelleyDrye.com
Alysa N. Zeltzer	AZeltzer@KelleyDrye.com

Independent Contractors

Elisa A. Nemiroff	ENemiroff@KelleyDrye.com
Julie G. O'Neill	JONeill@KelleyDrye.com

www.kelleydrye.com