BUSINESS LAW TODAY

"Who Am I Talking To?"—The Regulation of Voice Data Collected by Connected Consumer Products

By Michael Silvestro and John Black

The Internet genie has escaped its bottle. For many years, the Internet was something confined to personal computers and far-flung servers. Now, it is all around us—the proliferation and miniaturization of wireless Internet and computing technologies has fostered the creation of the "Internet of Things." In simple terms, many consumer products are now connected to the Internet, and those that are not soon will be. Your current refrigerator may not be able to independently order more ketchup when you are running low, but there is a good chance your next one will.

Parallel to the proliferation of the Internet of Things, there have been rapid advancements in voice recognition and control technologies. For generations, the idea of speaking to your watch was the stuff of fantasy (unless you were Dick Tracy). Now, it is unremarkable. Millions of people every day are controlling their cars, phones, computers, and myriad other gadgets with their voices alone.

Voice-control options are becoming the new norm for many classes of consumer goods that are part of the Internet of Things. The potential benefits to consumers are great—as are the opportunities for manufacturers and advertisers presented with another potential vein of data-mining gold in the form of voice data. Given that many new consumer devices are "always listening" for voice commands, concerns over potentially Orwellian privacy abuses have recently begun to arise.

In early 2015, these concerns hit the national news following reports about the controversial use of voice data by certain Internet-connected "smart" televisions. In response, the State of California passed a statute, effective January 1, 2016, that, among other things, prohibits the sale of voice recordings for advertising purposes and restricts the ability of law enforcement to require that surveillance features be included. The California statute applies only to smart televisions, however, and portends a patchwork of new voice-data privacy regulations. This article explores the privacy concerns connected with the collection and use of voice data, the current and potential regulatory response, and liability concerns arising from the collection or dissemination of voice data.

I Always Feel Like Somebody's Watching Me

Many newer consumer goods with voice-control features have an "always listening" function. In most instances, the device is equipped with a microphone and voice-processing features that allow for a variety of commands and inputs. Although the device is "always listening," often it is not actually processing or transmitting that voice data until it is activated by a specific voice command. Nonetheless, the device is always listening to ambient noise—including any conversations within earshot—waiting for the voice command that will wake it up. Devices that do not have an "always listening" feature typically require an active physical input, such as pressing a microphone button on a remote control.

Last year, the fine print of one manufacturer's smart television privacy policy raised privacy concerns and made national head-

lines. The manufacturer's smart televisions offered voice-control features that captured voice data and associated texts for the stated purpose of evaluating and improving certain features. This was achieved by transmitting voice data over the Internet to a third party for text conversion to facilitate data analysis. The clause in the privacy policy that sparked privacy fears, however, was a notification that if a user's spoken words included personal or other sensitive information, that information would be among the data captured and transmitted to a third party.

Online debates, news stories, and think pieces ensued, raising a number of questions about that technology. Who was the third party receiving the voice data? What specific voice data was collected and converted to text? For what purpose were the voice data and associated texts used? Are they traceable back to an individual user? Was the voice data securely transmitted and properly encrypted? Is my television now watching me?

The issue struck a nerve with some consumers. For many, televisions are very personal devices with which they have a different and deeper connection than other consumer gadgets. Moreover, televisions often are found in places in the home where the private activities of day-to-day life occur—in the living room, the kitchen, and the bedroom. A television often is within earshot of many of one's most private and personal conversations and activities, and the notion that a television could be recording every word or sound is particularly unnerving.

California's Connected Televisions Statute

In response to such privacy concerns, California became the first state to regulate the collection and use of voice data through televisions. Through the passage of Assembly Bill 1116, California added Chapter 35, entitled "Connected Televisions," to Division 8 of the Business and Professions Code. Given that the California statute is the first of its kind nationwide and may provide a roadmap for future regulation, it is worth exploring the specifics of the law.

The California Connected Televisions statute contains several interesting concepts regulating the conduct of smart TV manufacturers. One key provision is a notification requirement for enabling voice-control functions. Section 22948.20(a) provides: "A person or entity shall not provide the operation of a voice recognition feature within this state without prominently informing, during the initial setup or installation of a connected television, either the user or the person designated by the user to perform the initial setup or installation of the connected television."

In short, this section requires manufacturers to provide notice of voice-control features during the initial set up of a connected television. Notably, the statute employs a notification framework rather than an "opt in" approach that would require affirmative user consent to activate voice-recognition features. The law does not specify what form "prominently informing" consumers must take, however, offering manufacturers some leeway in deciding how to provide consumers with notice of voice-control features. This section requires notice only "during the initial setup or installation of a connected television" and not at subsequent times.

A centerpiece of the statute is sections 22948.20(b) and (c) restricting the sale or use of voice data for advertising purposes, which limits the data-mining potential of collected voice data. Section 22948.20(b) provides: "Any actual recordings of spoken word collected through the operation of a voice recognition feature by the manufacturer of a connected television for the purpose of improving the voice recognition feature, including, but not limited to, the operation of an accessible user interface for people with disabilities, shall not be sold or used for any advertising purposes." Section 22948.20(c) is almost identical, but applies to any "third party contracting with a manufacturer for the purpose of improving the voice recognition feature," rather than manufacturers.

Notably, these restrictions are narrowly tailored to "actual recordings of spoken word" and do not encompass text transcripts or other data derived from those voice recordings. Moreover, sections 22948.20(b) and (c) also apply only to actual voice recordings collected "for the purpose of improving the voice recognition feature, including but not limited to, the operation of an accessible user interface for people with disabilities." As such, voice recordings collected for other purposes are not explicitly regulated by the statute.

The statute also restricts the ability of law enforcement to use voice-recognition features for surveillance. Section 22948.20(d) specifically prevents law enforcement from ordering the creation of features allowing surveillance access and provides: "A person or entity shall not compel a manufacturer or other entity providing the operation of a voice recognition feature to build specific features for the purpose of allowing an investigative or law enforcement office to monitor communications through that feature." It is worth noting that this regulation only prohibits manufacturers from the requirement to build in surveillance features.

Importantly, a manufacturer's liability under the statute is limited only to functionality at the time of the original purchase. Section 22948.20(e) provides: "A manufacturer shall only be liable for functionality provided at the time of the original sale of a connected television and shall not be liable for functionality provided by applications that the user chooses to use in the cloud or are downloaded and installed by a user." Thus, additional voice-control features added later through a software update or through the use of applications later installed on the smart television are excepted.

The Connected Television statute also contains specific limitations to its application in sections 22948.21(a)–(c). Subsection (a) limits the statute only to a "connected television," which is defined as "a video device designed for home use to receive television signals and reproduce them on an integrated, physical screen display that exceeds 12 inches, except that this term shall not include a personal computer, portable device, or a separate device that connects physically or wirelessly to a television, including, but not limited to, a set-top box, video game console, or digital video recorder." As such, additional devices that may have voice features, such as remote controls, streaming boxes, and tablets are exempted from the statute.

Section 22948.21(b) defines a "user" as "a person who originally purchases, leases, or takes ownership of a connected television. A person who is incidentally recorded when a voice recognition feature is activated by a user shall not be deemed to be a user." This definition is significant, given that notice is not required to be provided to secondary purchasers and individuals who use, but did not purchase, own, or lease the television. Moreover, notice is not required to be provided to persons who are "incidentally recorded when a voice recognition feature is activated by a user," such as houseguests or individuals within earshot of a smart television used in a public space like a bar or restaurant.

Finally, section 22948.21(c) defines a "voice recognition feature" as "the function of a connected television that allows the collection, recording, storage, analysis, transmission, interpretation, or other use of spoken words or other sounds, except that this term shall not include voice commands that are not recorded or transmitted beyond the connected television." Although "voice recognition feature" is broadly defined, it again bears mentioning that the limitations on the sale and use of data collected through a voice-recognition feature set forth in sections 22948.21(b) and (c) are narrowly tailored to include only "actual recordings of spoken word."

With regard to enforcement, the Connected Television statute explicitly does not create a private cause of action. Instead, actions for relief under the statute can only be brought in civil court by the California Attorney General or a district attorney. The maximum penalty for knowingly engaging or proposing to engage in violation of the statute is capped at $2,500 for each nonconforming, connected television sold or leased. Given the large quantity of smart TVs sold, however, monetary penalties could be substantial.

The enforcement provision, section 22948.23(c), is not limited to manufacturers, however. Instead, it creates potential liability for any "person who knowingly engages, has engaged, or proposes to engage" in violation of the statute. Accordingly, manufacturing partners such as external software developers, retailers, and importers could conceivably be liable for monetary penalties in the event that they knowingly sell connected televisions that fail to provide adequate notice or otherwise do not comply with the statute.

A Patchwork of Privacy Regulations

Given that the California statute is the first of its kind in effect in the United States, it provides a potential blueprint for future statutes or regulations in other jurisdictions and highlights topics that other legislators and regulators may wish to address. As with many other areas of data-privacy law, which are addressed by a combination of state and federal legislation and regulation, it is likely that there will be a patchwork of legislation and regulation in the future addressing the collection and use of voice data through consumer products.

As noted above, the California statute is narrowly tailored only to televisions, explicitly carving out other types of devices, such as set-top boxes and game consoles that may interface with a computer or the Internet. Given the rapid proliferation of other kinds of connected devices that employ voice control and the potential value of voice data, consumer privacy concerns are only likely to increase. As with other technology-focused legislation, it is possible that legislators and regulators may effectively be playing catch-up as new categories of products enter the market and new privacy concerns are perceived.

One possible regulatory approach may be to enact similar statutes on a piecemeal, product-category basis. Alternatively, broader regulations applying to larger swaths of product categories may be enacted. It is also possible that carefully tailored statutes, like the one enacted in California, will serve as a building block, which could be modified or expanded in the future to cover other product categories or data-use scenarios.

Future voice-data regulations may also expand the scope of regulated voice data beyond "actual recordings of the spoken word." Other information collected from voice recordings—such as text transcripts or analysis of audio recordings—may eventually be regulated. It is also possible that some jurisdictions will restrict the types and volumes of audio data that can be collected and/or disseminated, as well as the retention of that data beyond a certain period of time. Potential limitations on law enforcement access may also be fiercely debated, particularly in light of the recent dispute between Apple and the FBI over access to an encrypted phone as part of a terrorism investigation.

Recent comments by FTC Chairwoman Edith Ramirez on March 31, 2016, to the ABA's National Institute on the Internet of Things may offer some hints as to potential federal regulation. Ms. Ramirez opined that Internet of Things business practices must appropriately address privacy concerns, for instance minimizing the amount of collected consumer data and then effectively controlling its use. She also called on businesses to give consumers clear notice, and preferably a choice to opt in or opt out of potentially unexpected uses of their data. Whether any of these suggestions form the basis of future regulations or enforcement actions remains to be seen, but Ms. Ramirez noted the limits of the FTC's regulatory powers in this area and called upon Congress to pass comprehensive federal data-security legislation.

Comprehensive federal data-security legislation seems unlikely in the near future, however. Thus far, data-security legislation at the federal level has been addressed on a sectoral basis, and many data-security bills have languished in Congress over the years. In the short term, to the extent that other states explore similar regulations, the likely result will be a mix of regulations with which manufacturers and others may need to comply. As with other areas of data-privacy regulation, this may present compliance challenges for certain businesses. However, given the national market for consumer electronics, it is likely that many manufacturers will tailor their product offerings to comply with the most stringent applicable law. It is important for other businesses in the product stream—including retailers and importers—to be mindful of regulatory developments as

some regulations, like the California statute, may expose them to liability.

Liability Concerns

Voice data is, ultimately, just another form of consumer data that businesses might collect and use. Nonetheless, the possibility that voice data may include actual audio recordings of sensitive information should only heighten the attention paid to securing this type of data. The voice data collected through voice-control features may contain personal information about consumers protected under current privacy laws and regulations, even if a user is aware that their personal information may be collected. Moreover, to the extent such information is protected by state statutes or regulations for residents of that state without regard to the location of the collection or storage of that data, it is important for businesses to pay close attention to data privacy laws in all jurisdictions where current or potential customers may reside.

Some data-privacy regulations require specific, personal data-protection procedures, such as encryption and written information-security programs that could apply to voice data. See, e.g. 201 Mass. Code Regs. 17.00. Companies involved in the collection, dissemination, or use of voice data, even if they are not manufacturers of consumer electronics, should be mindful of compliance with data-privacy regulations that may apply in the event that protected personal information is collected. These concerns are of import not only to those who interact with actual audio voice recordings, but also with textual transcripts or other derived data that could include personal or other confidential information.

The transmission of voice data is another issue that merits close attention. There have been reports that some consumer electronics have transmitted voice data and text transcriptions from the device over the Internet without secure encryption. Businesses that provide voice data to third parties must also be aware of the information-security procedures and practices of those third parties. Proactive measures to ensure that third parties who might receive collected voice data are properly securing that data is an important component of mitigating the risk of a data breach and any potentially resulting liability.

Consumer behavior and education also plays a role, just like it does in data-privacy management in business and other settings. It is likely that many consumers using electronic devices with voice-control functions at home or in the workplace are not aware that voice data can be collected and disseminated to third parties through voice-recognition features. This notice concern was a motive behind the notice requirement of the California Connected Television statute and is likely to feature in any similar future regulations. There also could be liability exposures for businesses using devices with voice-control devices in public settings, such as restaurants, bars, and retailers, and future regulation may include expanded notification requirements when such devices are used in public. Indeed, voice data collected from customers of a wide range of businesses could contain confidential or private information subject to regulation and potential liability if that data is not properly protected.

Finally, the security of any connected device that can capture voice data must be considered. As the Internet of Things grows, and more physical objects that we interact with on a daily basis are connected online, so too do the risks posed by hackers. Exploitation of security flaws in connected devices can create threats in the physical world. As just one example, last year it was revealed that an Internet-connected teakettle, which could be remotely turned on and heated, had security vulnerabilities that could allow hackers to remotely hijack and control the kettle. A hack that would allow a third party to control and record a private audio conversation from a consumer product with voice-recording capabilities, whether at home or at work, could be a devastating invasion of privacy that exposes manufacturers and other businesses to serious liability.

Conclusion

The widespread adoption of connected devices with voice-control features is an exciting development. There are myriad applications for users as well as the potential for businesses to leverage a new trove of valuable consumer data. However, privacy concerns are magnified by the personal nature of the audio recordings and the potential for abuse. As the Internet of Things multiplies and more types of devices are able to capture voice data, new laws and regulations will be necessary. As in other areas of data privacy law, the regulatory landscape will continue to evolve to address the implementation of these new technologies and the concomitant privacy risks.

Michael Silvestro and John Black are principals at Skarzynski Black LLC in Chicago, IL.

ADDITIONAL RESOURCES

For other materials related to this topic, please refer to the following.

Business Law Section Program Library

Developing Online Privacy Notices: Key Challenges and Practical Solutions (PDF) (Audio)

Presented by: Consumer Financial Services

Location: 2016 Committee Meeting