Business Law

NEWSLETTER

June 2019

From the Colorado Bar Association Business Law Section

Can Attorneys Guarantee Confidentiality in the Era of Smartphones and Voice-Activated Devices?

By Herrick K. Lidstone, Jr., Burns, Figa & Will, P.C.

Among a lawyer's many obligations to clients is the duty of confidentiality found in Colorado Rules of Professional Conduct (Colo. RPC) 1.6. As early as 1992, the CBA Ethics Committee warned:

> In recent years, there have been significant advances in communications technology. In addition, the cost of many modern communications devices has been decreasing such that the use of cordless telephones, cellular telephones and facsimile machines has become commonplace. It can be expected that new or improved methods of communications devices will continue to be developed. The use of these communications devices carries the increased risk of intentional or inadvertent eavesdropping onto what are intended to be confidential discussions. Therefore, lawyers must be mindful of their duty under Rule 1.6 of the Colorado Rules of Professional Conduct and Canon 4 of the Code of Professional Responsibility to preserve client confidences when utilizing advanced communications technology.[1]

In 1992, the big news for technological concerns were analog cell phones that could be more easily intercepted and cordless telephones in one location being listened to through baby monitors in another location. These issues have disappeared, being replaced by any number of issues related to advances in technology. This article talks about the confidentiality risks of voice-activated devices such as Apple's HomePod (powered by Siri), Amazon's Echo (powered by Alexa), and Google's Home (powered by the Google Assistant) as well as confidentiality risks related to the smartphones that we all carry which have unknown tracking and listening devices.

Voice Activated Devices Are Always Listening and Frequently Recording

It is important to understand that voice-activated devices are always on – listening and waiting to hear the "wake" word. Sometimes it hears a word it believes to be the "wake" word when that was not intentionally said. So, the lawyer who has a voice-activated device in the office waiting for "Alexa, play Beethoven's Fifth" must understand that the device is also

[1] CBA Ethics Committee Formal Opinion 90, adopted November 14, 1992, available in 22 The Colo. L. (CBA) at No. 1 (Jan. 1993) at p. 21. The CBA Ethics Committee updated Formal Opinion 90 in July 2018, published in The Colo. L. (CBA) October 2018 at p. 88.

listening to any attorney-client conversations going on in the office or on the telephone – and at least occasionally recording.

These voice-activated devices are storing the conversations they record with third-parties – conversations listened to by the Amazon Echo are uploaded to Amazon and, in at least one case, forwarded to a third party in a contact list. That case garnered national media coverage in 2018 when a Portland family's conversation was recorded and sent out to a contact through their Amazon Echo device. Even the title of the article from CNBC is scary: "*Amazon Echo secretly recorded a family's conversation and sent it to a random person on their contact list*."[2] While calling this "an extremely rare occurrence," Amazon blamed the mistake on Alexa, explaining:

> Echo woke up due to a word in background conversation sounding like "Alexa." Then, the subsequent conversation was heard as a "send message" request. At which point, Alexa said out loud "To whom?" At which point, the background conversation was interpreted as a name in the customers contact list. Alexa then asked out loud, "[contact name], right?" Alexa then interpreted background conversation as "right." As unlikely as this string of events is, we are evaluating options to make this case even less likely.

Merely the fact that these voice-activated devices are always listening to us and recording those conversations[3] can be disconcerting to all of us for our personal privacy, but especially for lawyers who may have these devices where they hear and record confidential communications which are accessible to hackers and too many other people. More concerning than the devices always listening is what happens to these recordings once they're uploaded to the cloud or sent to a company's computer system, especially in the context of these devices listening in on potentially confidential conversations. In an NBC News article, Jennifer King, director of consumer privacy at the Center for Internet and Society at Stanford University, said "Considering these devices listen on a continuous loop, I would have grave concerns about using one in my own home as a privacy researcher."[4]

Privacy experts question how your privacy can be secured when using these devices, but suggest, among other things, to delete your voice recordings (and recordings archive) every day, and to turn off the device's microphone and camera when they are not in use.[5] While the mistakes that these devices may make are rare, as claimed by Amazon with respect to the Portland family's communication, what level of risk are lawyers willing to accept?

Your Smartphone Has Significant Privacy Issues As Well

---

[2] Kim, Eugene (May 24, 2018), available at https://www.cnbc.com/2018/05/24/amazon-echo-recorded-conversation-sent-to-random-person-report.html. *See also* John Kruzel, PolitiFact, May 31 2018, available at https://www.politifact.com/truth-o-meter/statements/2018/may/31/ro-khanna/your-amazon-alexa-spying-you/.

[3] Fowler, Geoffrey A., *Hey Alexa, come clean about how much you're really recording us*, The Washington Post (May 24, 2018), available with subscription at https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/?noredirect=on&utm_term=.0e8ada0132d4.

[4] NBC News, *Alexa privacy fail highlights risk of smart* speakers, (May 26, 2018) available at https://www.nbcnews.com/tech/innovation/alexa-privacy-fail-highlights-risks-smart-speakers-n877671.

[5] Rawes, Erika, *How to secure your Alexa device*, available at https://www.digitaltrends.com/home/how-to-secure-your-alexa-device/.

While our digital smartphones do not have the risks of the earlier analog versions and they are not recording us unless we ask them to do so, there are a number of other issues which may impact attorneys and our compliance with Colo. RPC 1.6.

Geoffrey Fowler with *The Washington Post* has written numerous articles on the subject.[6] In one article, Fowler details a week long investigation into the data sharing and tracking that his iPhone engaged in.[7] Warning against Yelp, DoorDash, and a number of other common apps, he reported that the investigation uncovered over 5,400 trackers installed on his iPhone that would amount to 1.5 gigabytes of data being transmitted to third party services over one month.[8] The data sharing isn't limited to iPhones either. A 2018 study reported that Google sends your location, routes taken through Google Maps, and Chrome information to third parties.[9]

These trackers, working through apps on your phone or the cookies run around the internet, share information on your phone with third parties often for research purposes or to create targeted advertisements.[10] The information being shared ranges from your phone number and email address to your digital fingerprint and exact location.[11] The sharing is happening passively, and often times users aren't aware it's happening or that active steps must be taken to ensure their data's protection.[12] To add insult to injury, these transmissions of data impact the permissible data under cellphone plans.

Again, from the attorney's duty of confidentiality perspective, this provides information accessible by subpoena on a lawyer's travel – including perhaps to confidential locations to meet clients on client business.

What steps can you take to guard the information on your devices?

Comment [8] to Colo. RPC 1.1 (*Competence*) is very important with respect to issues regarding protection of confidential information from voice activated devices and from the use of smartphones. Comment [8] provides:

---

6 Fowler, Geoffrey A, *Archive*, available with subscription at: https://www.washingtonpost.com/people/geoffrey-a-fowler/?utm_term=.dfcdc9da8564.

7 Fowler, Geoffrey A, *It's the middle of the night. Do you know who your iPhone is talking to?*, Washington Post (May 28, 2019), available with subscription at https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/?utm_term=.d4e8b43062e0.

8 *Id.*

9 Marrian Zhou, Carrie Mihalcik, *New study finds Google's Android is sharing even more data than we thought*, CNET (August 22, 2018), available at https://www.cnet.com/news/new-study-finds-google-android-is-sharing-even-more-data-than-we-thought/.

10 Fowler, Geoffrey A, *It's the middle of the night. Do you know who your iPhone is talking to?*, Washington Post (May 28, 2019), available with subscription at https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/?utm_term=.d4e8b43062e0.

11 *Id.*

12 *See* Fowler, Geoffrey A., *Hey Alexa, come clean about how much you're really recording us*, The Washington Post (May 24, 2018), available with subscription at https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/hey-alexa-come-clean-about-how-much-youre-really-recording-us/?noredirect=on&utm_term=.0e8ada0132d4.; Diaz, Jesus, *Android Sucks 10X More of Your Private Data Than iPhone* (Aug. 22, 2018), available at: https://www.tomsguide.com/us/android-privacy-vs-iphone,news-27856.html.

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, ***including the benefits and risks associated with relevant technology***, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. [***Emphasis supplied.***]

I suggest that part of each lawyer's obligation is to understand the technology being used, its risks as well as its rewards.

For voice activated devices, among the ways to reduce the risk is to turn off the device when confidential communications are ongoing. Delete archived recordings and then continue to delete them on an ongoing basis. Most voice-activated devices allow the owner to change the "wake" word – it should be changed to something that Alexa, Siri, and Google Assistant cannot misunderstand – consider "supercalifragilisticexpialidocious" from the *Sound of Music*.

For your smartphone, generally there is no option to completely erase your phone's ability to track your data.[13] There are, however, some steps that can be taken to limit the tracking. One option a commentator suggests is downloading Privacy Pro SmartVPN, an app that helps block any unwanted tracking of your web history and app usage.[14] It's available on iPhones through the iTunes app store or through the Galaxy App Store on Android devices.

Another option is changing settings on your smartphone to disable location services. On the iPhone, go to "settings → privacy → location services". There you can turn off location services for any app that you do not need to disclose your location, and you can change it to "when using" for apps that you occasionally want to use your location for convenience. (Think, OpenTable to find a nearby restaurant.)

You should also limit ad tracking (settings → privacy → advertising → turn on limit ad tracker), and turn off background refresh for apps (settings → general → background app refresh → turn off).[15]

For Android, disable cloud-based backup (Settings → Backup & Reset → switch off the option to Back up my data), turn off advertisement tracking (Settings → Ads → switching the setting on), and turn off location settings **(**Settings → Location**,** turn off Google Location and location History).[16]

---

[13] Stern, Joanna, *iPhone privacy is broken … and apps are to blame*, Wall Street Journal (May 31, 2019) available at: https://www.wsj.com/articles/iphone-privacy-is-brokenand-apps-are-to-blame-11559316401.

[14] Fowler, Geoffrey A, *How to limit iPhone app tracking*, Washington Post (May 29, 2019), available with subscription at https://www.washingtonpost.com/technology/2019/05/28/how-limit-iphone-app-tracking/?utm_term=.cb0fe88e308e.

[15] Fowler, Geoffrey A, *How to limit iPhone app tracking*, Washington Post (May 29, 2019), available with subscription at https://www.washingtonpost.com/technology/2019/05/28/how-limit-iphone-app-tracking/?utm_term=.cb0fe88e308e.; Stern, Joanna, *iPhone privacy is broken … and apps are to blame*, Wall Street Journal (May 31, 2019) available at: https://www.wsj.com/articles/iphone-privacy-is-brokenand-apps-are-to-blame-11559316401.

[16] For privacy and security, change these Android settings right now, available at https://www.zdnet.com/pictures/android-phone-tablet-privacy-security-settings/9/.

In all cases, users of devices should consider an "app census"[17] to determine which apps are tracking you and how you can protect yourself. Even if this may not all be an issue under Colo. RPC 1.6, it may improve your personal privacy score.

***Conclusion*.**

To conclude as we started, it is the attorney's ethical obligation under Colo. RPC 1.1 (*Competence*) to understand and use technology in a manner that does not violate other rules, such as Colo. RPC 1.6 (*Confidentiality*). Although some of these stories discussed above are shocking for the common users of voice-activated devices and smartphones, attorneys and other professionals with strict confidentiality requirements should consider how the ethical rules of their profession impact their decision to use these devices at work.

Subject to certain exceptions found in Colo. RPC 1.6(b), Colo. RPC Rule 1.6(a) requires attorneys to protect the confidentiality of all "information relating to the representation of a client" and Colo. RPC 1.6(c) requires us to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."

Voice-activated devices that always listen may cause a problem with a state's confidentiality rules "or even compromise the attorney-client privilege due to third-party disclosure."[18] Smartphones tracking your every move and your every keystroke have equally troublesome issues for the attorney-client relationship. It is, after all, the attorney's obligation to be competent in understanding technology that is being used in practice and to understand where and how a client's confidential information is being stored and used by the electronic devices.[19]

---

[17] Fowler, Geoffrey A, *It's the middle of the night. Do you know who your iPhone is talking to?*, Washington Post (May 28, 2019), available with subscription at https://www.washingtonpost.com/technology/2019/05/28/its-middle-night-do-you-know-who-your-iphone-is-talking/?utm_term=.d4e8b43062e0. The author recommends a privacy app available at https://itunes.apple.com/us/app/privacy-pro-smartvpn/id1057771839?mt=8.

[18] Christopher Riordan, *Ethics on using digital billing assistants*, American Bar Association (March 27, 2018) available at https://www.americanbar.org/news/abanews/publications/youraba/2018/april-2018/digital-billing-assistants-and-professional-responsibility/

[19] *See* Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R, at 6 (2017) (discussing technology uses in practice); MODEL RULES OF PROF'L CONDUCT, r. 1.1 cmt comment 8 (Am. Bar Ass'n 2016).