Smartphones and Privacy Versus Progress

With personal information more available than ever, where do we draw the line?

Raise your hand if you can comfortably go a day without your smartphone. Can you bring yourself to *not* access the Internet on that phone? What about GPS? Can you be equally efficient manually charting your course via a Thomas Guide? Can you still buy a Thomas Guide?

Ninety-one percent of American adults have cell phones, 56 percent of which are smartphones. One third of cell phone owners use their phones as the primary or only way they access the Internet, according to the Pew Internet & American Life Project.

Our need for staying connected, juxtaposed with the myriad apps available to consumers—apps that, more often than not, require users to assent to substantial intrusions into their privacy—illustrates a dilemma. How do we balance users' privacy with government and nongovernment entities' aspirations to collect their private information?

To stay connected, users must assent to substantial intrusions into their privacy.

In 1990, while its embassy in Russia was being built, the United States determined that the Soviets had planted "breathtaking numbers" of bugs into the building, resulting in the building being scrapped, and costing the U.S. upward of $270 million. Those were the days when "surveillers" spent millions of dollars, untold effort, and countless hours sneaking around, trying to install devices to surreptitiously watch and listen to our every move.

Now we're paying top dollar to help them do it.

Microphones, cameras, and GPSs are in our PCs and tablets and televisions. And if we want to exploit the features in our smartphones, we are compelled to sacrifice our privacy to do so.

It's understandable that Google Maps needs my location to provide driving directions, but does it need to read my address book too? DragonGo "may allow the app to share or save your calendar data, regardless of confidentiality or sensitivity." But why? (Nuance did not respond to a request for comment.) Firefox records audio, and takes pictures and videos on smartphones. Are these invasions reasonable?

Utter! BETA is an offline voice-controlled virtual assistant that does not share or upload personal data to external servers. Stating the "requests are for device level only," developer Ben Randall acknowledges that while utter! BETA does not collect personal data, Android has access to everything that takes place on the device and therefore can leverage anything without additional apps. Randall believes the system is "seriously flawed" and "desperately needs modifying."

It's Not What You Have to Hide. It's What You Have to Lose.

Equally alarming are the lack of regulations regarding collection of our biometric data. "Biometrics are personal information," voice biometrics analyst Judith Markowitz explains. While other countries have privacy regulations protecting personal information, the U.S. does not. "Organizations may collect biometrics and other personal information without the person's approval or even their knowledge," Markowitz says.

Defining and implementing privacy protections requires foresight. If the government institutes a policy that concerns a fundamental right, the policy is presumed invalid unless the government can demonstrate a compelling interest to justify it. Nongovernment actors are not bound by this strict scrutiny.

With the mission of preventing business practices that are anticompetitive, deceptive, or unfair to consumers, the Federal Trade Commission has articulated Fair Information Practice Principles, which also provide privacy protection. Here are the five core principles:

- Give users notice *before* any personal information is collected.
- Allow users to choose how their personal information will be used.
- Allow users to see information about them that has been collected.
- Take reasonable steps to ensure data integrity.
- Implement processes that ensure compliance.

Expectation of Privacy

"The expectation of privacy a person has when he enters a restroom is reasonable and is not diminished or destroyed because the toilet stall being used lacks a door."

This quote comes from a set of very different facts and applies to government actors, but the analogy is striking. In this case, an individual was arrested after officers clandestinely observed him engaging in sex acts with another man in a public restroom. The court held this to be unauthorized surveillance in violation of the Fourth Amendment.

Perhaps the standard should be not only whether the individual's expectation of privacy is reasonable, but whether the information gatherer's intrusion into the individual's privacy is reasonable. ☒

Robin Springer is an attorney and the president of Computer Talk, Inc. (www.comptalk.com), a consulting firm specializing in speech recognition and other hands-free technology services. She can be reached at (888) 999-9161 or contactus@comptalk.com.