

From the Magazine: The Growing Issue of Wireless Privacy

Elliot Drucker

Recent unauthorized disclosures regarding the extent of National Security Agency (NSA) cellphone data gathering have a lot of Americans wondering just how much privacy we can expect in our personal communications. Perhaps even more significantly, the flap over NSA activities gives rise to a much broader issue of whether some of the spectacular technology packed into the smartphones further erodes our privacy, not just in our communications but in our everyday lives.

As first disclosed by whistleblower Edward Snowden, and later confirmed by major news organizations, the NSA program collects so-called “metadata” for virtually all calls and text messages to and from cellphones operating on the nation’s major wireless networks. Metadata does not include the actual content of a call or message, but rather such information as the phone number called (for outgoing calls and messages) or the originating number (for incoming calls and messages), the date, time, and duration of the call, and the identity of the wireless network and the cell or cells serving the call. Snowden also leaked information about the NSA’s mass collection of data on Americans’ Internet activities, and about similar programs operated by Britain’s Government Communications Headquarters.

The NSA has stated that the cellphone metadata they collect is used only for purposes of fighting terrorism and other national security threats. They give as an example the case where they learn the number of the cellphone being used by a suspected terrorist. By looking at this person’s movements (gleaned from the cell ID information) and identifying the numbers of the phones he or she is communicating with and the frequency and durations of those calls and messages, the NSA and law enforcement agencies like the FBI are able to draw inferences on activities this person might be planning. The NSA claims that this sort of intelligence has led to the disruption of a number of significant terrorist plots.

Whether you view the NSA program as a prudent component of the fight against terrorism or an overreaching invasion of privacy, it’s pretty clear that the potential for abuse, and consequential harm to innocent people, is significant. And it’s not just individuals that could be impacted; many important services provided over by telephone – the suicide crisis hotline comes to mind – would be far less effective if it’s known that their callers could be identified. On the other hand, metadata has always been collected by network operators, not just for cellphones but for most

From the Magazine: The Growing Issue of Wireless Privacy

Published on Wireless Week (<http://www.wirelessweek.com>)

landline services as well. The real question therefore appears to be whether there is a significantly elevated risk of misuse with the data in the hands of a behemoth federal agency.

Unfortunately, the issue of privacy in wireless services does not end with the NSA metadata flap. Modern smartphone features and applications offer many ways in which the privacy of their users can be assaulted. Some, of course, are voluntary. I am constantly amazed, for example, by how much personal information people post, for all the world to see, on social media like Facebook and Twitter. Such imprudence aside, more insidious threats to privacy lurk in smartphone features like “family tracking” and various downloadable applications that include user location.

Family tracking, typically offered as a value-added feature by wireless service providers, is usually set up to allow members of a family plan to view the mapped locations of other members on their smartphones or on a computer through password protected Internet access. It’s a popular feature, particularly for parents of teenagers, and since it’s voluntary on an opt-in basis it’s hard to fault it on privacy concerns. But being able to surreptitiously keep track of someone’s location seems to me to be an awfully attractive target for hackers and even for more serious criminals. One therefore hopes that the folks that manage family tracking programs are fervently devoted to data security.

Unfortunately, it’s a pretty good bet that among the thousands of smartphone app providers there are some that are definitely not so devoted to security. This could become a huge privacy concern because many popular apps involve the collection of user location information. Want driving directions with current traffic data taken into account? That can be a really helpful app, but it obviously requires that the server know your location. So too do the free apps, offered by many companies, that provide location based services such as showing the location of the nearest Denny’s restaurant.

It’s important to understand that in most cases commercial collection of mobile user location data does not require the direct participation of the wireless network operator. Through on-board GPS receivers, or simply knowing the ID of its serving cell or Wi-Fi router, the typical smartphone can provide this information to a web-based location server on the “user plane,” meaning that the wireless network (or the serving Wi-Fi system) is only providing the data communication. Therefore, aside from assuring security of its own location-based features (and of the metadata discussed above), it’s not likely that network operators can help much in protecting the privacy of its users’ location data.

Of course, user location is not the only privacy issue associated with today’s

From the Magazine: The Growing Issue of Wireless Privacy

Published on Wireless Week (<http://www.wirelessweek.com>)

smartphones. The typical phone likely carries contact lists, call history logs, text message contents, private images, and all manner of other personal data. Mobile banking and “ewallet” apps can involve storage of extensive financial information. All of this data is potentially vulnerable to malicious extraction. As smartphones become more and more central to our everyday lives, it’s clear that security of the personal data they carry is emerging as a huge issue for the wireless industry.

Addressing the problems of personal privacy and security for wireless users will require a number of initiatives. Most obviously, makers of smartphones and their operating systems need to provide security for personal data residing in user’s phones. Third party providers of anti-malware products like McAfee and Norton will likely also get involved, perhaps in protecting against malicious apps. Congress and government agencies probably need to consider laws and regulations limiting how personal cellphone data can be obtained, used, stored, and shared by commercial enterprises. Perhaps most importantly, users themselves need to be informed about risks to privacy and how to manage them.

It’s unfortunate that current fears of terrorism have put society in the position of having to balance the need for security against the desire for privacy. But beyond whatever legitimate need the government has to amass personal data, we should all be able to control who knows what about our private lives. It is therefore important that the wireless industry understand and address the vulnerabilities to privacy that its products and services present.

Source URL (retrieved on 12/08/2013 - 1:08pm):

<http://www.wirelessweek.com/articles/2013/08/magazine-growing-issue-wireless-privacy>