

# Bloatware Comes to the Smartphone

Patrick McDaniel | Pennsylvania State University

Chances are, if you purchased a new cell phone in the last year, you also received a large number of applications you didn't ask for, don't want, and can't get rid of. This practice—known as *bloatware*—is now pervasive in the smartphone industry. Many cellular carriers load each new phone with dozens of applications that often can't be removed. Whereas some industry leaders suggest that the inclusion of such software is a way to demonstrate phone and network features, others provide a more frank (and, in my opinion, credible) explanation: it's about cost. Simply put, the subsidies the bloatware application developers provide offset the high cost of the handset and provide better profits for the cellular carriers.

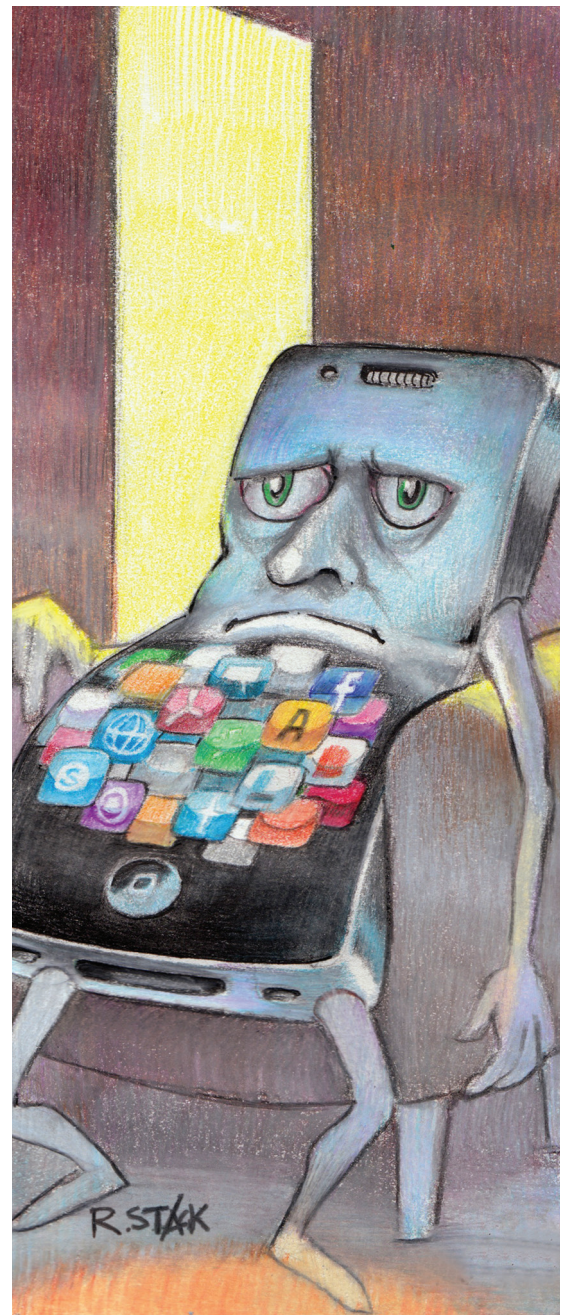
My research group recently purchased a new Android-based Droid RAZR phone from a major carrier. (Herein, I focus on one carrier, but bloatware is pervasive throughout the industry.) It's a great phone with nice features and a terrific interface. Unfortunately, when we first booted up the phone, we saw pages and pages of applications that we had no need for. There were more than 60 applications for services, games, and tools that we didn't want. We tried deleting them but couldn't. After consulting technical support and newsgroups, we concluded that the applications were there forever unless we took it upon ourselves to jailbreak the phone.

Here, I explore the security

and privacy implications of the now-common industry practice of installing bloatware on phones sold by cellular carriers. Is it merely annoying, or do smartphone users face more serious concerns? Do the economic advantages outweigh the security and privacy concerns?

## A History of Subsidized Applications

Before delving into these discussions, it's instructive to reflect on the history of bloatware in the PC market. Bloatware isn't a recent phenomenon. Commodity desktop and laptop computers are often sold with dozens of "subsidized" productivity, game, and utility applications pre-installed. (Historically, this has been most prevalent in Windows-based systems.) The economic model driving bloatware in the PC market is a consequence of market pressures and changing consumer demands. As more companies enter the PC market, margins become tighter, and pennies per unit make a difference in bottom-line profitability. Manufacturers and resellers found that customers would accept bloatware if they could purchase a PC at a lower cost. Lower unit costs are subsidized by application developers. Developers pay the manufacturers to pre-install software and recoup costs when users adopt the software and purchase licenses. As consumers found the cost advantage acceptable, the market embraced bloatware as common practice.



The amount of bloatware placed on new systems became unwieldy as the practice grew. Resources were drained; computers ran slower and became buggier. Customers began to get angry. Vendors who were more aggressive in providing bloatware were criticized by the technical community and press, and their brands were damaged. The public reaction led to a reduction of bloatware by some manufacturers and in some markets, but the practice is still widely used today.

At the heart of the debate over bloatware is the complexity of removing it. Often, removing it is difficult and hazardous—a PC often can become unstable after removing a seemingly innocuous application. Consequently, a secondary market for bloatware uninstaller utilities emerged and continues to thrive.

### Moving toward the Smartphone

The smartphone market has recently rediscovered the economic advantages of bloatware. Increased competition, constant consumer demand for the “latest and greatest” phone hardware, moves to new network technologies such as LTE (3 GPP Long Term Evolution), and other factors have greatly affected the costs of handsets and the networks that serve them. Many industry leaders argue that revenue sources are necessary. Where once the wholesale cost of cheap cell phones was less than US\$100, new smartphones now commonly cost more than \$500. At the same time, the explosion of smartphone-supported information services has created more opportunities for extracting profits from value-added services. For this reason, partnerships between cellular carriers and software developers are naturally symbiotic and profitable. Thus, many cellular carriers in the smartphone market have begun to

include bloatware, sometimes in large quantities, on sold phones.

Notably, Apple has largely prevented bloatware from being placed on iPhones resold by carriers. Apple carefully protects the user experience on resold devices, both in the US<sup>1</sup> and internationally.<sup>2</sup> Given Apple’s history and the strength of the position it has taken regarding its platforms, it seems unlikely that this will change.

There are indirect consumer costs for smartphone bloatware. First, counter to what many claim, these preinstalled applications do affect the system, even if the consumer never uses them. Applications in systems such as Android comprise *background* and *foreground* programs. User interfaces are provided through foreground processes. Background processes are used by applications that poll data or constantly update state even when not in use, for example, by polling for new instant messages. Many applications will start background processes when the phone boots up, regardless of whether they’re used. My group’s new phone starts about a dozen background processes when booted. As far as I know, we’ve never opened the interfaces associated with many of these background processes or used the services they support, yet they continue to consume computing resources. From an interface perspective, users have to sift through pages of applications on the phone to find the ones they need. The interface is an ugly, unwieldy mass of useless applications.

Another cost is the potential loss of privacy. Researchers have found that many applications leak private data, such as GPS location, hardware IDs, and phone numbers.<sup>3,4</sup> Could these installed but largely unknown applications carry such privacy-violating functions? Given the pervasiveness of the practice in current markets, it

seems reasonable to assume that some do. Moreover, users don’t know how and when their privacy and security are being violated. The interfaces used to communicate applications’ rights and behaviors are coarse, and the developers’ intent is opaque. For example, the Android platform defines a single permission, INTERNET, to enable communication over network interfaces. Once granted, the application isn’t restricted in the way in which it can use the network. Users have no idea what the application intends to do with the network, and more often than not, the end-user license agreement (EULA) is no help. Moreover, applications often fail to disclose behaviors that users might not like in EULAs. Because users can’t opt out of these applications, user privacy is at risk by default.

Although it’s debatable whether it’s bloatware, the recently exposed CarrierIQ software might have the potential to violate user privacy.<sup>5</sup> Purportedly placed on phones by several carriers to enhance the user experience, critics have suggested that it can be used to spy on users by listening to and recording phone conversations, collecting text messages, tracking user location, recording interface keystrokes, and much more. There’s a good deal of controversy about how carriers use the software and what it does, but if critics’ reports are true, it has the ability to invade users’ privacy without their knowledge or consent. Oddly, until recently, some carriers deployed Apple’s iPhone with CarrierIQ. Apple has removed it in response to the public outcry following its discovery.

But what about security? Do cellular carriers analyze applications to ensure they don’t contain malware or expose exploitable bugs? It’s unclear what precautions providers take, but it’s an important question. Independent of these factors, the

introduction of many applications can only increase the phone's threat surface. Many of the most serious PC security vulnerabilities were the result of noncritical and underutilized software interfaces. Thus, the inclusion of dozens of applications from myriad developers with whom the user has no relationship seems, at best, like bad practice.

### Who Owns My Phone?

The real debate on this topic seems to be about control. Can and should carriers be able to lock users into applications that potentially violate user privacy and security? More generally, is the phone the user's property or the provider's? Should users be able to remove sponsored applications that they don't trust, or do they relinquish that right by saving money on the initial purchase?

Undeletable applications, particularly coming from third-party providers are inherently hazardous. Forcing users to possess and run unwanted applications means forcing them to accept a security stance that might not be acceptable to them. This is particularly troubling for organizations. Smartphones are now commonly used for professional communication, and the exposure to risk might not be acceptable. An informal review of popular vendors' EULAs was inconclusive; it wasn't entirely clear whether removal of bloatware violated the service contract.

On the other hand, users can often (but not always) purchase phones that aren't bound to a specific provider at a premium and avoid the bloatware that comes with them. The cost is higher, but users have more control. Is the lesson that if you want security and privacy, you have to pay for it by bypassing carrier subsidies of the phone? Maybe.

Interestingly, the Android community has started to react to bloatware. Android recently introduced software that lets users "disable"

applications. Users can permanently prevent an application from running but can't remove it. There are early indications that some vendors are allowing the disabling of some bloatware (our phone had a "hide" feature, although we couldn't authoritatively determine what this feature did). But whether the industry will broadly adopt this is unclear.

### The High Price of Cheap Phones?

The fundamental truth is that bloatware opens the door to a loss of security and privacy "at purchase." Although cellular carriers and cell-phone manufacturers might use due diligence in evaluating applications, ultimately, they are (or should be) responsible for any damages they cause. Just like the market increasingly holds software vendors responsible for the systems they produce, so too should the market punish bad applications foisted on customers.

The central technical question of bloatware is whether the provider—or anyone—can verify that an application is trustworthy. Sadly, such a query is definitionally flawed. There's no one set of behaviors or permissions on which everyone will agree is appropriate for an application. The most we can hope for is a clear and accurate description of what preinstalled applications will and can do to users and their data. Yet, we as a technical community don't have the tools or knowledge to answer this question for arbitrary applications, and the application developers haven't been forthcoming on application behaviors in EULAs.


Like many things in privacy and security, the human-scale issue underlying bloatware hinges on informed consent. Users should be able to buy cheap phones, but only with the knowledge of the indirect

costs associated with the preinstalled applications. Will users be willing to pay an additional fee not to be exposed to the risks and resource costs of these additional applications? It isn't clear. The market will sort this out, but only when and if users are given the opportunity to make an informed decision based on the yet-to-be-understood risks of bloatware. ■

### References

1. R. Ritchie, "True Cost of Apple Control: No Carrier Bloatware on iPhone," *iMore*, July 2010; [www.imore.com/2010/07/22/true-cost-apple-control-bloatware-iphone](http://www.imore.com/2010/07/22/true-cost-apple-control-bloatware-iphone).
2. J. Aimonetti, "Apple Holds Strong over Bloatware in Japan," *CNET*, Nov. 2011; [http://reviews.cnet.com/8301-19512\\_7-57325506-233/apple-holds-strong-over-bloatware-in-japan](http://reviews.cnet.com/8301-19512_7-57325506-233/apple-holds-strong-over-bloatware-in-japan).
3. W. Enck et al., "A Study of Android Application Security," *Proc. 20th Usenix Security Symp.*, Usenix Assoc., 2011; [www.enck.org/pubs/enck-sec11.pdf](http://www.enck.org/pubs/enck-sec11.pdf).
4. W. Enck et al., "TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones," *Proc. 9th Usenix Symp. Operating Systems Design and Implementation (OSDI 10)*, Usenix Assoc., 2010; <http://appanalysis.org/tdroid10.pdf>.
5. Z. Lutz, "Carrier IQ: What It Is, What It Isn't, and What You Need to Know," *Engadget*, 1 Dec. 2011; [www.engadget.com/2011/12/01/carrier-iq-what-it-is-what-it-isnt-and-what-you-need-to](http://www.engadget.com/2011/12/01/carrier-iq-what-it-is-what-it-isnt-and-what-you-need-to).

**Patrick McDaniel** is a professor at Pennsylvania State University's Computer Science and Engineering Department. Contact him at [mcdaniel@cse.psu.edu](mailto:mcdaniel@cse.psu.edu).

 Selected CS articles and columns are also available for free at <http://ComputingNow.computer.org>.