

# ACLU: Slow smartphone updates are privacy threat

April 17 2013, by Raphael Satter

---

One of the leading U.S. civil-rights organizations is taking on an unusual cause: spotty smartphone updates. The American Civil Liberties Union is asking the U.S. Federal Trade Commission to investigate what it considers a failure by U.S. wireless carriers to properly update the Google-built operating system used on Android phones. The ACLU says that sluggish fixes have been saddling many smartphone users with software that is out of date and therefore dangerous.

"At its core, it's not all that different from any other defective product issue," said the ACLU's Chris Soghoian, who drew the [analogy](#) between a vulnerable smartphone and "a toaster that blows up."

Experts and [government officials](#) have long warned that failing to fix known [security flaws](#)—whether on phones or computers—gives [hackers](#) opportunities to steal data or use the devices to launch larger attacks.

The ACLU's 17-page complaint, filed Tuesday, accused carriers AT&T Inc., Sprint Nextel Corp., T-Mobile USA and Verizon Wireless of ignoring those warnings. It cited figures showing that only 2 percent of [Android](#) devices worldwide had the latest version of [Google's operating system](#) installed. The complaint said that as many as 40 percent of all Android users are still using versions of software released more than two years ago.

The complaint said the carriers were exposing Android customers to "substantial harm" by not moving fast enough on upgrades. The ACLU

asked the FTC to force carriers to either warn customers about the issue or start offering refunds.

The FTC said it received the ACLU's complaint but declined to comment further. The agency does not necessarily have to take the complaint up. If it does, an investigation would likely take months.

Carriers who replied to queries from The Associated Press denied delays in the updates, often described as patches. In emailed statements, Sprint said it followed "industry-standard best practices" to protect its customers, while Verizon said its patches were delivered "as quickly as possible." AT&T and T-Mobile did not return emails seeking comment. Google Inc., which was not targeted by the complaint, declined comment.

Carriers are in a tricky position. Google makes its Android operating software available for phone makers to use and modify as they see fit. Phone makers, in turn, let [wireless carriers](#) make additional changes, such as restricting software upgrades. The three-part process involves "rigorous testing," according to Verizon.

Making sure newer versions of Google's operating system run smoothly with all the various devices and carriers involved is particularly important for older phones, which may have trouble running the latest software or apps. Customers may not notice or care whether their Android device is running the latest and safest operating system, but they will notice if a misconfigured update means they can't make calls or run their favorite apps.

Yet Travis Breaux, a computer science professor at Carnegie Mellon University in Pittsburgh, said the testing process was straightforward. He suggested that carriers were struggling to adapt to the realities of fast-changing smartphone software.

"There are standard practices for testing and evaluating patches," Breaux said. "Microsoft does this all the time."

Jeffrey Silva, a telecom policy analyst with New York-based Medley Global Advisors, said he had a tough time understanding the delays given the highly competitive U.S. cellphone market.

"It's hard to know why they haven't done it to date," he said. "They have all the incentive in the world."

Soghoian said that pressuring carriers to update their phones more quickly wasn't a bid to turn the ACLU into a consumer-protection body. Instead, he said, the organization wanted to advertise the sorts of steps that could be taken to boost the nation's online defenses without the need for invasive new laws. In particular, he referred to a cybersecurity bill now before Congress. Critics—including the White House—say that bill doesn't adequately protect private data.

"This is part of our attempt to reframe the cybersecurity agenda," Soghoian said. "Before violating anyone's privacy, the government should first be addressing the low-hanging fruit that everyone can agree on."

**More information:** The ACLU on smartphone security:  
[bit.ly/11fTiDy](http://bit.ly/11fTiDy)

Copyright 2013 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed.

Citation: ACLU: Slow smartphone updates are privacy threat (2013, April 17) retrieved 25 April 2024 from <https://phys.org/news/2013-04-aclu-smartphone-privacy-threat.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.