The New York Times

# Our Cellphones Aren't Safe

Security flaws threaten our privacy and bank accounts. So why aren't we fixing them?

**By Cooper Quintin**
Mr. Quintin is a senior staff technologist at the Electronic Frontier Foundation.

Dec. 26, 2018

America's cellular network is as vital to society as the highway system and power grids. Vulnerabilities in the mobile phone infrastructure threaten not only personal privacy and security, but also the country's. According to intelligence reports, spies are eavesdropping on President Trump's cellphone conversations and using fake cellular towers in Washington to intercept phone calls. Cellular communication infrastructure, the system at the heart of modern communication, commerce and governance, is woefully insecure. And we are doing nothing to fix it.

This should be at the top of our cybersecurity agenda, yet policymakers and industry leaders have been nearly silent on the issue. While government officials are looking the other way, an increasing number of companies are selling products that allow buyers to take advantage of these vulnerabilities.

Spying tools, which are becoming increasingly affordable, include cell-site simulators (commonly known by the brand name Stingray), which trick cellphones into connecting with them without the cellphone owners' knowledge. Sophisticated programs can exploit vulnerabilities in the backbone of the global telephone system (known as Signaling System 7, or SS7) to track mobile users, intercept calls and text messages, and disrupt mobile communications.

These attacks have real financial consequences. In 2017, for example, criminals took advantage of SS7 weaknesses to carry out financial fraud by redirecting and intercepting text messages containing one-time passwords for bank customers in Germany. The criminals then used the passwords to steal money from the victims' accounts.