

Quotes by security experts

"People wear a seat belt in the car to be safe, and they should use a security app when using public Wi-Fi."

Jude McColgan, President of Mobile at Avast.

<http://finance.yahoo.com/news/avast-exposes-huge-security-risks-131600897.html>

"When users access unencrypted networks, attackers can easily hijack the session and not only gather all sorts of sensitive information, including passwords, but also potentially inject malicious code to compromise the device,"

Rajiv Shah, General Manager, Australia for BAE Systems.

<http://securitywatch.co.nz/story/public-wifi-and-byod-backdoor-route-cyberattacks/>

"The ability for a bad guy to essentially suck information out of any wireless-enabled device is extremely easy, especially in a public area"

Jason Hart, VP Cloud Solutions at Gemalto.

<http://www.dailymail.co.uk/news/article-2917099/How-criminals-easily-suck-information-smartphones-using-public-Wi-Fi-networks.html>

"If those of us in positions of responsibility fail to do everything in our power to protect the right of privacy, we risk something far more valuable than money. We risk our way of life."

Tim Cook (CEO of Apple)

<http://www.theguardian.com/technology/2015/feb/13/apple-ceo-tim-cook-challenges-obama-privacy>

"Protecting privacy is about making certain that people have the ability to make informed decisions about how they engage in public. I do not think we've done enough here"

Danah Boyd (Social media scholar and advocate working at Microsoft Research, New York University Media Culture & Communication and the Harvard Berkman Center for Internet & Society.)

<http://www.wsj.com/articles/SB10001424052970204190704577024262567105738>

"The dirty secret of the Web is that the "free" content and services that consumers enjoy come with a hidden price: their own private data"

"Many of the dangers posed by digital dossiers do not occur regularly, but are incredibly destructive to people's lives when they do. An unlucky few will be stalked, fired, surveilled, arrested, deported or even tortured, all as a result of the data kept about them by companies and governments. Much more common are the harms of identity theft or public embarrassment. Even when companies follow best practices—and few do—it is impossible to be completely secure."

Christopher Soghoian (Principal technologist at the American Civil Liberties Union)

<http://www.wsj.com/articles/SB10001424052970204190704577024262567105738>