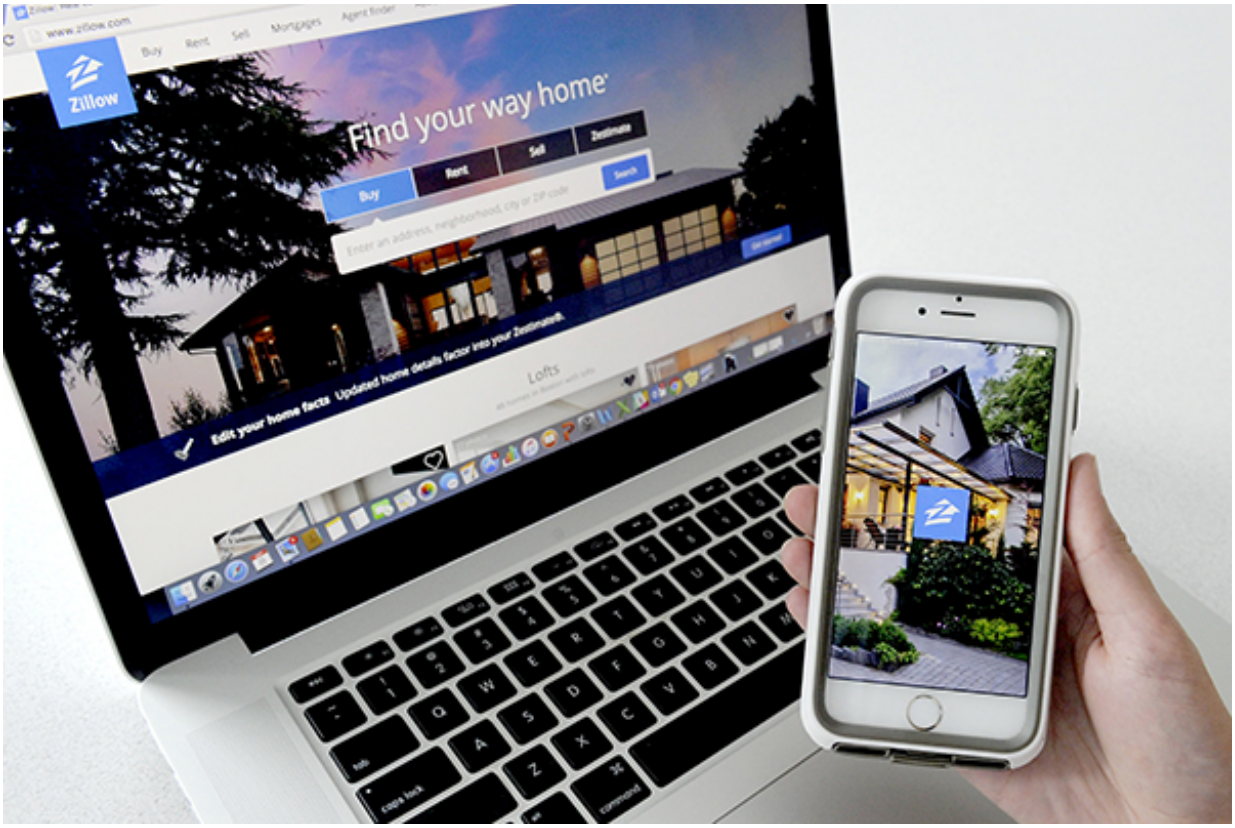
App vs. website: Which best protects your privacy?

September 12 2016, by Thea Singer



Both apps and websites leak personal information, including names, gender, phone numbers, and e-mail. But don't despair. Northeastern researchers, led by assistant professor David Choffnes, have developed an automated system to help you know which platform to use for your online interactions. Credit: Matthew Moodono/Northeastern University

That's the question that Northeastern researchers, led by assistant professor David Choffnes, ask in new research that explores how free app- and web- based services on Android and iOS mobile devices compare with respect to protecting users' privacy.

In particular, the team investigated the degree to which each platform leaks personally identifiable information—ranging from birthdates and locations to passwords—to the advertisers and data analytics companies that the services rely on to help finance their operations.

The answer? "It depends," says Choffnes, a mobile systems expert in the College of Computer and Information Science. "We expected that apps would leak more identifiers because apps have more direct access to that information. And overall that's true. But we found that typically apps leak just one more identifier than a website for the same service. In fact, we found that in 40 percent of cases websites leak more types of information than apps."

Those types of information vary, based on the platform. For example, the researchers found that websites more frequently leak locations and names, whereas only apps were found to leak a device's unique identifying number.

The researchers will present their findings in a paper at the 2016 Internet Measurement Conference, in Santa Monica, California, in November.

The team's aim is to help users make informed decisions about how best to access online services. To that end, they have integrated their findings into an easy- to- use interactive website that rates the degree of leakiness of 50 free online services, from Airbnb to Zillow, based on each user's privacy preferences.

Here's how it works: Users select from a drop- down list of 50 services

and check off whether their operating system is Android or iOS. Next they're asked to rate various types of personal information, from their birthdates to their devices' unique identifiers, they care most about keeping private. Then, automatically, the site generates two "leakiness indexes" for the service selected—a sky blue bar for the app version, a lime green one for the web—and recommends which platform is best for that particular user.

"There's no one answer to which platform is best for all users," says Choffnes. "We wanted people to have the chance to do their own exploration and understand how their particular privacy preferences and priorities played into their interactions online.

For the study, the researchers selected 50 of the most popular free online services in a variety of categories, including business, entertainment, music, news, shopping, travel, and weather. Each service had to offer the same functionality on both its website and app. To ensure that they were interacting with the services as everyday users would, the researchers conducted manual, rather than automated, tests, personally logging in, entering requested user data into text fields, and navigating the environment.

Both apps and websites, they found, leaked locations, names, gender, phone numbers, and e- mail addresses to varying degrees. But there were surprises. "We didn't expect to find the diversity of information collected across the different platforms even for the same service," says Choffnes. Moreover, four services sent encrypted passwords to another party: the Grubhub app, unintentionally, due to a bug, which has been fixed; the JetBlue app, for authentication purposes; the Food Network app and website, for identity management; and the NCAA website, for identity management.

"The reasons for the intentional leaks are legitimate, and I'm sure that

the services have appropriate agreements with the other parties to protect the passwords," says Choffnes. "But the practice still raises an important issue: Users have no idea that their passwords are being sent to another party." Consider: JetBlue customers making an airline reservation likely assume they are submitting their passwords to JetBlue for authentication, when in fact their credentials are being managed by a third party, Useablenet.

Choffnes hopes that the findings will start a dialogue between consumers and online services about the kinds of information that should be collected, balancing the services' revenue needs with consumers' privacy needs. "My goal is not just to tell people a scary story but to issue a call to action," he says. "Part of that action could be that users start requesting or even demanding the privacy and transparency considerations they want from the companies they interact with."

Provided by Northeastern University