Opinion: Privacy laws not adequate in age of Internet

By Jamie Court

Two federal courts in California recently took up the question of whether invasion of privacy laws should apply to unauthorized opening of email, in one case, and interception of unencrypted home WiFi communications in another.

Wiretapping law stood the test against “Wi-spying” last week. A panel of Ninth U.S. Circuit Court of Appeals judges held that data transmitted over a WiFi network is protected because it is not as easily accessible as a radio communication and intercepting it takes technical stealth akin to tapping a telephone.

The question of whether reading and collecting the contents of our emails meets the wiretapping standard remains unanswered.

What’s notable is that the defendant in these cases was not the National Security Agency or a rogue “war driver,” techies who cruise neighborhoods with equipment to suck up unencrypted data, but the largest company on the Internet: Google.

Google’s argument in both cases was essentially the same: Invasion of privacy laws don’t apply online.

The Wi-spy case sprung from revelations that Google’s Street View cars not only were photographing the roads they traveled but were also collecting “payload” data – including emails, documents, photos, passwords and other private information – transmitted over WiFi networks as the cars drove by.

Google’s defense against a class-action lawsuit (which the consumer group I run is co-counsel in) alleging millions of violations of the wiretapping laws was basically “anybody can

do it," so it's not wiretapping.

The court didn't buy it, finding that Google engineers' knowledge and values didn't reflect the public's. "Members of the general public do not typically mistakenly intercept, store and decode data transmitted by other devices on the network," the judges said.

In the email case, Google argues that those who e-mail Gmail users, and have their email contents read and scanned by Google for marketing purposes, "have no legitimate expectation of privacy."

"Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use Web-based email today cannot be surprised if their emails are processed by the recipient's (e-mail provider) in the course of delivery," Google's lawyers stated in their brief.

The statements caused a big public backlash against Google because we think of Google as the post office, not an executive's assistant. We don't expect the postmaster to read our mail, particularly when we don't use a Gmail account and are simply emailing to Gmailers.

The overarching problem is companies with the power and wealth of Google and Facebook will continue to push the envelope of our telephonic privacy laws because they have yet to be updated for the Internet Age.

Google argued in the Gmail case that telephone lines are not the same as the Internet, and the invasion of privacy laws simply don't apply.

Dozens of states and several countries have fined or settled with Google for the Wi-spy incident, but the millions of dollars are a slap on the wrist to a $150 billion company. The $25,000 Google was fined by the Federal Communications

Commission for obstructing its investigation of the Wi-spy scandal is probably less than the weekly cappuccino bill at the Googleplex.

California's Constitution contains an "inalienable right" to privacy in Article 1, but the legislative session that ended Friday produced little in the way of privacy protections, despite scandals de jour.

What's needed now more than ever is an unequivocal do-not-track-online right.

All the major Internet browsers now allow us to send a do-not-track-me signal, but very, very few websites and Internet systems respect it. Google analytics and its advertising networks, for example, track us as we surf online to market us regardless of the signals we send.

That's why when you search for a Pottery Barn lamp, the advertisement for it seems to be stalking you at the next sites you visit.

A recent Pew study reaffirms that the public overwhelmingly wants the right to be anonymous on the Internet. But the White House clearly has no interest in that, given its vigorous defense of the NSA.

In California, the best Sacramento could muster this year is a right to be told whether your do-not-track signal is being respected – AB370, which is awaiting the governor's signature.

More disclosure about the privacy rights we don't have is simply not enough for a public in an age of driverless cars, wired refrigerators and wearable devices like Google Glass, which can surreptitiously video record us. Our current privacy laws can only stretch so far, and the Internet is quickly colonizing all the space around us.

A ballot measure is now the public's only hope to win the

right to privacy online and to not be tracked. If we don’t set the boundaries soon, we will quickly lose control over all the personal information in our life, from what we eat, to where we drive, to when we get seen in someone else’s Glass. And as we all know, online and off, information is power.

Jamie Court is president of Consumer Watchdog, a nonprofit nonpartisan public interest group in Santa Monica. He is drafting a do-not-track-online measure for the November 2014 ballot.