

Canon



Easily protect
your most critical data. ▶ Rollover to Learn More

Privacy Legislation: Time Has Come

Analysis: What's worse than privacy legislation? No privacy legislation The Internet has had 10 years to "self regulate" and hasn't.

Dan Tynan

Sunday, August 08, 2010 07:57 AM PDT

Jim Harper is a smart guy. I've had the pleasure of interviewing him on several occasions, and I've always appreciated his contrarian views on privacy even when I didn't agree with them.



Illustration: Jeffrey Pelo

In a thoughtful essay in [The Wall Street Journal](#), Harper argues that without data sharing, the Web wouldn't be what it is today, and the tradeoff between baring our Web surfing habits to advertisers and receiving "free" content is a fair one.



PC TOOLS
SPYWARE Doctor
with AntiVirus 2010

Recommended Download

Protect your PC with the best!

PCMag.com Editors' Choice (October 15, 2009)

Free Virus, Spyware, Adware, Trojan, & Rootkit Scan

DOWNLOAD

FOR FREE PC SCAN

He's right about much of that. But he's wrong about much more.

[See also: [Whom do you fear: Apple, Google, Microsoft, or God?](#)]

Harper is director of information policy studies at [The Cato Institute](#) -- a dyed-in-the-wool libertarian who believes private industry can do a better job policing itself than government can. And for more than a decade, Internet content providers and advertisers argued that very case, convincing Congress to let the Web self regulate [on privacy issues](#).

Here we are ten years later, still wrestling with the same issues -- as well as much bigger issues, like [who owns our geolocation data](#). If self regulation had worked, would we still be talking about this?

Harper argues people are getting their boxers unduly bunched [over tracking cookies](#) -- tiny text files Web sites deposit on your machine that can identify your browser when you return to that site or others in the same advertising network.

Usually such cookies are anonymous; they might help someone determine that browser X visited Web sites ABCDE and saw ads from XYZ. Sometimes, though, they could get tied to your identity, if you register for a Web site and that site (or its advertising network) marries your personal information to your clickstream.

What happens after that? Good question. And good luck finding out.

Per Harper:

"But rather than indulging the natural reaction to say 'stop,' people should get smart and learn how to control personal information. There are plenty of options and tools people can use to protect privacy-and a certain obligation to use them. Data about you are not 'yours' if you don't do anything to control them."

There's so much in that graph to pick on I don't know where to start. Plenty of options and tools to protect your privacy? Sure, if you like your tools to be hopelessly complicated and largely ineffectual. I've been writing about Internet privacy for a dozen years and have yet to find a simple solution that works.

Your data isn't yours if you don't do anything to control it? Tell me, please, how to control the data Google collects about me that's floating out there on the InterWebs. I'm all ears. Or, for that matter, how to make the typical privacy policy comprehensible to humans who lack a law degree.

Then there's this graph:

"'Surreptitious' use of cookies is one of the weaker complaints. Cookies have been integral to Web browsing since the beginning, and their privacy consequences have been a subject of public discussion for over a decade. Cookies are a surreptitious threat to privacy the way smoking is a surreptitious threat to health. If you don't know about it, you haven't been paying attention."

Until about 1960, people thought smoking was good for you. Or at least, that's the line the tobacco companies tried to push. (Note: Of course, I wasn't alive back then, so most of my knowledge of that era comes from "Mad Men.")

We are in the Web equivalent of the early 1960s. Cookies are one of the most poorly understood concepts on the Net. Quick, what cookies are being deposited by this Web site right now? Do you even know how to find out? I didn't think so.

Harper is wary of a world where every Web site and every Web ad has to obtain your consent before it can use your information. I get that. But instead we have a world where every consumer has to parse the legalese of every Web site and Web advertiser to find out what information they collect and what they're doing with it. And then have to go back and check to see if anything's changed. Over and over and over.

And when something does change and users don't like it -- see Facebook and its ever-shifting privacy policies -- their only option is to pack up and go home.

If the Internet really wants to self regulate, content providers and advertisers need to make privacy brain-dead simple. The first time I log onto a Web site that tracks my surfing habits and/or location, show me a splash screen with five bullet points summarizing what information it's collecting what happens to it. Give me a link to a plain-English description of the site's privacy policies and the option to click "no thanks" right there.

Is that so friggin' difficult? Do we really need another ten years of discussion for this to happen?

In the libertarian world view, a company would come along and offer that kind of service. The handful of privacy services that have arisen in the past ten years have all failed, however. The reason? There's not enough profit in protecting privacy, and way too much money to be made by violating it.

I'm really not a fan of government regulation, but sometimes it's necessary for the wellbeing of everyone. You can't force people to care about their personal privacy enough to jump through hoops to protect it. But you can force companies to care about it. That's what laws are for.

[ITworld TY4NS blogger Dan Tynan](#) is usually a lot less serious than this. Follow his unique brand of juvenile humor at [eSarcasm \(Geek Humor Gone Wild\)](#) and on Twitter: [@tynan_on_tech](#).

1998-2010, PCWorld Communications, Inc.