# Tracking your digital fingerprint online raises privacy issues

July 28 2014, by Robert Merkel

Your computer has a special fingerprint that can give away details of your online browsing. Credit: Flickr/Sandra Nahdi, CC BY-NC-SA

Just how much information we give away about ourselves as we browse the web has been raised again by a tracking device used in thousands of websites.

Researchers at Belgium's University of Leuven have revealed the widespread use of a technique called "canvas fingerprinting" that tracks the activities of people on a website without their knowledge.

More than 5,600 websites were identified using the fingerprinting technique including Australian websites such as Australia Post, the Fairwork Ombudsman and the Sea Shepherd conservation group.

While this technique is relatively new, it represents another front in a very long battle to find out what users do online, and raises concerns about our ability to control our online privacy.

## Here, have a cookie

Technical mechanisms for uniquely identifying web users date back to the introduction of the cookie in the Netscape browser in 1994.

When the user loads a webpage they get all the information necessary to display the page, such as the text, layout and images. But they also a small amount of "cookie" data sent along too, which is stored by the browser on the user's computer.

When the user requests another page from the same website, the browser appends the cookie to the request to the server. In this way, the server hosting the website knows that the request came from the same computer.

Cookies are extremely useful and without them there would be no support for website logins.

But they can also be used to provide a complete record of a user's use of a website. The use of "tracking cookies" allows this recording to extend across many, many websites, providing a comprehensive picture of a

user's browsing history to whoever controls the tracking cookie.

This becomes particularly intrusive if this browsing history can then be tied to any identifying data.

## Privacy management

Understandably, many internet users aren't terribly enthusiastic about their browsing history being so readily available to third parties. Tools to manage cookies have been incorporated into internet browsers and third-party privacy tools.

Deleting cookies, or controlling whether particular cookies are sent back to particular websites, gives the user more control over the extent of monitoring.

The technical response of browser developers has been combined with legal measures, such as the European Union's privacy directive.

Under these rules, cookies used in a potentially privacy-invading manner must be disclosed to website visitors and explicit consent obtained.

## Browser fingerprinting

Some internet companies have now turned to another ingenious technique for uniquely identifying and tracking users.

Rather than relying on browsers to send back a previously sent cookie, they collect enough information about the user's browser environment to uniquely identify the user.

Modern computers have specialised hardware that greatly speeds up the

computations needed to draw pictures on the screen. These graphics chips, made by companies such as NVidia, have made possible the amazing graphics of modern games, and speeded up your browsing and spreadsheets on today's high-resolution monitors.

But the wide variety of such hardware, and the software used as "drivers" to control them, means that different computers will render such pictures in subtly different ways.

Images rendered by the graphics hardware (and thus subtly different on different computers) can be created from within a browser, analysed and sent back to a web server.

On its own, this is not enough to uniquely identify a user. But when combined with information such as the browser name and version number, and the list of fonts available on the system, it can provide a unique "fingerprint" of a user's computer.

This provides a tracking mechanism that can be operated across many websites; a "super-cookie" that can't be deleted as it is inherent to the computer it's running on.

Again, this is most intrusive if it can be combined with personally identifying information. But even without this, it is very much against the spirit of the cultural norm (and the EU law) that requires internet sites to explicitly gain the consent of their users to enable tracking.

The University of Leuven research indicates that around 5% of the world's top 1,000 websites make some use of this fingerprinting method, which was originally identified by University of California researchers in 2012.

Interestingly, however, the vast majority of websites using browser

fingerprinting had done so by incorporating a third-party element into their website.

## Free tools come with a hidden price

The primary product of AddThis is sharing tools – an easy-to-add component that website developers can incorporate on their sites that allow visitors to easily share the page they are viewing on social media such as Facebook and Twitter.

While AddThis charges for some use of some these components, others are available for free. Free and good-looking website components are to website developers what honeypots are to bears, so it's not surprising that they have been widely adopted.

But AddThis extracts an additional quid pro quo – collecting browser data about those who visit sites usings their tools, much more than either the visitors, or the website owners, would have realised.

AddThis's Rich LaBarca said it carried out a six month test using the fingerprinting and that any data collected was used for "internal research". The code has since been disabled.

But the White House blog on the website of the US President didn't realise that incorporating AddThis tools to its website violated its own privacy policy.

## Taking what most of us give away anyway

As a computer geek from way back, I can't help but grudgingly respect the ingenuity of those who perfect these privacy-invading tools, even as I deplore their ethics.

But my outrage is also tempered by the knowledge that these companies are taking by stealth what most of us choose to give away freely to other companies.

As media theorist Douglas Rushkoff observed, we – or, more precisely, our personal information – are "products" to many online companies such as Facebook, Google and AddThis.

The greatest fortunes of the 21st century have been founded on collecting and exploiting the personal information of billions of people, with a level of detail that companies such as AddThis can only dream of accessing.

And they've found that providing an easy way for us to share webpages of amazing cat videos and pictures is compelling enough that most of us will freely give them that information.

## So what of ethics?

Do those who actually build these technologies – the programmers, analysts, testers and other IT professionals – have any obligation to consider the ethics of the tools they build? In theory, they do.

The two largest global professional bodies of the IT profession – the Association for Computing Machinery (ACM) and Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS) – have jointly developed a Software Engineering Code of Ethics. The Australian Computer Society also has its own code of ethics.

Unfortunately – and unlike law, medicine or other fields of engineering – professional societies and their codes of ethics have virtually no influence within the information technology community.

Despite occasional efforts to set themselves up as gatekeepers through licensing, they have had little success. As such, however virtuous these codes of ethics may appear, they have no teeth.

Much as I would personally like it to be otherwise, it's unlikely that attempts to violate the privacy of individuals will reduce through the self-regulation of IT professionals.

The financial incentives for companies to do so are likely to continue. Privacy protection will have to come through some combination of public pressure, legal means, and individual adoption of technical and behavioural countermeasures.

*This story is published courtesy of* The Conversation *(under Creative Commons-Attribution/No derivatives).*

Provided by The Conversation