http://www.wsj.com/articles/SB10001424052748704679204575646704100959546

WHAT THEY KNOW

Race Is On to 'Fingerprint' Phones, PCs

By Julia Angwin And Jennifer Valentino-DeVries
Updated Nov. 30, 2010 12:01 a.m. ET

IRVINE, Calif.— David Norris wants to collect the digital equivalent of fingerprints from every computer, cellphone and TV set-top box in the world.

AUDIO

- **Listen:** Jennifer Valentino-DeVries discusses the next generation of online tracking tools.

He's off to a good start. So far, Mr. Norris's start-up company, BlueCava Inc., has identified 200 million devices. By the end of next year, BlueCava says it expects to have cataloged one billion of the world's estimated 10 billion devices.

Advertisers no longer want to just buy ads. They want to buy access to specific people. So, Mr. Norris is building a "credit bureau for devices" in which every computer or cellphone will have a "reputation" based on its user's online behavior, shopping habits and demographics. He plans to sell this information to advertisers willing to pay top dollar for granular data about people's interests and activities.

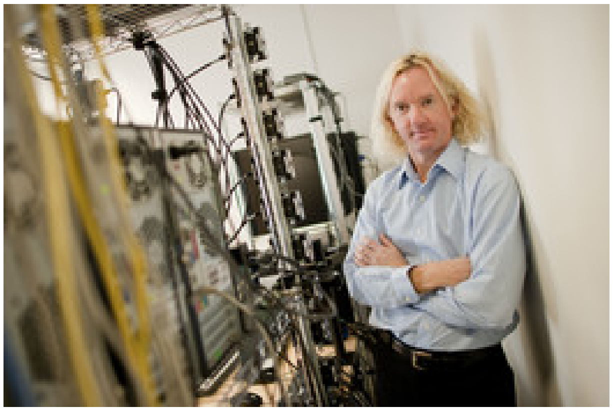
Device fingerprinting is a powerful emerging tool in this trade. It's "the next generation of online advertising," Mr. Norris says.

It might seem that one computer is pretty much like any other. Far from it: Each has a different clock setting, different fonts, different software and many other characteristics that make it unique. Every time a typical computer goes online, it broadcasts hundreds of such details as a calling card to other computers it communicates with. Tracking companies can use this data to uniquely identify computers, cellphones and other devices, and then build profiles of the people who use them.

Until recently, fingerprinting was used mainly to prevent illegal copying of computer software or to thwart credit-card fraud. BlueCava's own fingerprinting technology traces its unlikely roots to an inventor who, in the early 1990s, wanted to protect the software he used to program music keyboards for the Australian pop band INXS.

Tracking companies are now embracing fingerprinting partly because it is much tougher to block than other common tools used to monitor people online, such as browser "cookies," tiny text files on a computer that can be deleted.

As controversy grows over intrusive online tracking, regulators are looking to rein it in. This week, the Federal Trade Commission is expected to release a privacy report calling for a "do-not-track" tool for Web browsers.



BlueCava CEO David Norris plans to fingerprint billions of devices. Tracking cookies 'are a joke,' he says. MICHAL CZERWONKA FOR THE WALL STREET JOURNAL

of Internet users.

Deep packet inspection, a potentially intrusive method for peering closely into the digital traffic that moves between people's computers and the broader Internet, is being tested in the U.S. and Brazil as a future means to deliver targeted advertising.

MORE FROM DIGITS

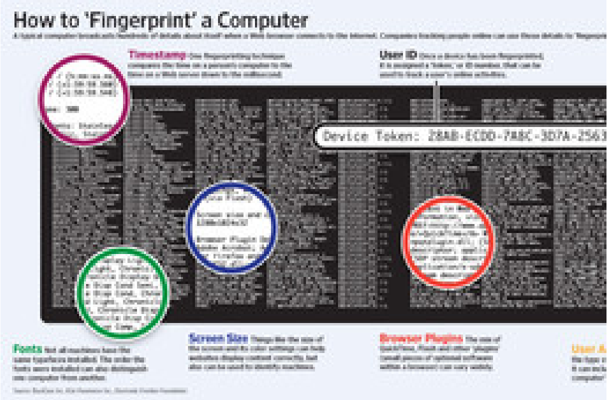
- 'Evercookies' and 'Fingerprinting': Are Anti-Fraud Tools Good for Ads?
- How to Prevent Device Fingerprinting
- A New Type of Tracking: Akamai's 'Pixel-Free' Technology

Akamai Technologies Inc., AKAM -1.52% ▼ an Internet-infrastructure giant that says it delivers 15% to 30% of all Web traffic, is marketing a technique to track people's online movements in more detail than traditional tools easily can.

It's tough even for sophisticated Web surfers to tell if their gear is being fingerprinted. Even if people modify their machines—adding or deleting fonts, or updating software—fingerprinters often can still recognize them. There's not yet a way for people to delete fingerprints that have been collected. In short, fingerprinting is largely invisible, tough to fend off and semi-permanent.

HOW TO 'FINGERPRINT' A COMPUTER

A typical computer broadcasts hundreds of details about itself when a Web browser connects to the Internet. Companies tracking people online can use those details to 'fingerprint' browsers and follow their users.


How to 'Fingerprint' a Computer
Timestamp
User ID
Device Token: 28AB-ECDD-7ABC-3D7A-2563
Fonts
Screen Size
Browser Plugins

Device fingerprinting is legal. U.S. Rep. Bobby Rush (D.,Ill.), proposed legislation in July that would require companies that use persistent identifiers, such as device

Fingerprinting companies are racing to meet the $23 billion U.S. online-ad industry's appetite for detailed consumer behavior. Previously, the companies focused on using device fingerprints to prevent software theft or to identify computers making fraudulent transactions, in hopes of preventing future attempts.

Mr. Norris's firm, BlueCava, this year spun off from anti-piracy company Uniloc USA Inc. to start offering services to advertisers and others. One of the leading e-commerce fraud-prevention firms, 41st Parameter Inc., has begun testing its device-fingerprinting techniques with several online-ad companies. Another anti-fraud company, iovation Inc. of Portland, Ore., says it is exploring the use of device profiles to help websites customize their content.

BlueCava says the information it collects about devices can't be traced back to individuals and that it will offer people a way to opt out of being tracked.

Still, Mr. Norris says it's tough to figure out how to alert people their devices are being fingerprinted. "We don't have all the answers, but we're just going to try to be really clear" about how the data is used, he says.

Ric Richardson, BlueCava's secret sauce, in Byron Bay, Australia. MELANIE TJOENG FOR THE WALL STREET JOURNAL

Neither BlueCava nor 41st Parameter explicitly notified the people whose devices have been fingerprinted so far. Both companies say the data-gathering is disclosed in the privacy policies of the companies they work with. BlueCava says it doesn't collect personal information such as people's names. Its privacy policy says it gathers "just boring stuff that most people couldn't care less about."

Ori Eisen, founder of 41st Parameter, says using fingerprinting to track devices is "fair game" because websites automatically get the data anyway.

Some advertisers are enthusiastic about fingerprinting. Steel House Inc., a Los Angeles-based ad company, has been testing 41st Parameter's technology for three months on websites of its clients, which include Cooking.com Inc. and Toms Shoes Inc. (Clients weren't notified of the test, and fingerprints weren't used to display ads.)

In its examination of 70 million website visits, 41st Parameter found it could generate a fingerprint about 89% of the time. By comparison, Steel House was able to use cookies for tracking on only about 78% of visits, because some people blocked or deleted cookies.

"It's almost like a revolution," says Mark Douglas, founder and CEO of Steel House. "Our intent is that it can completely replace the use of cookies."

the privacy people," Mr. Douglas says.

Computers need to broadcast details about their configuration in order to interact smoothly with websites and with other computers. For example, computers announce which specific Web browsers they use, along with their screen resolution, to help websites display correctly.

There are hundreds of parameters. "We call them the 'toys on the table,'" says Mr. Norris of BlueCava. "Everyone has the same toys on the table. It's how you rearrange them or look at them that is the secret sauce" used to fingerprint a specific computer.

BlueCava's secret sauce hails from Sydney, Australia, in the early 1990s. Back then, inventor Ric Richardson was helping musicians including the band INXS to use new software for playing their electronic keyboards.

MORE FROM THE SERIES

- A Web Pioneer Profiles Users by Name
- Web's New Goldmine: Your Secrets
- Personal Details Exposed Via Biggest Sites
- Microsoft Quashed Bid to Boost Web Privacy
- On Cutting Edge, Anonymity in Name Only
- Stalking by Cellphone
- Google Agonizes Over Privacy
- On the Web, Children Face Intensive Tracking
- 'Scrapers' Dig Deep for Data on Web
- Facebook in Privacy Breach
- Insurers Test Data Profiles to Identify Risky Clients
- Shunned Profiling Technology on the Verge of Comeback
- The Tracking Ecosystem
- Follow **@whattheyknow** on Twitter
- **Complete Coverage:** What They Know

"They'd say what sound they wanted, and I'd do it," says Mr. Richardson, who today works out of a van parked near an Australia beach.

Mr. Richardson was frustrated when he tried to sell the music software, because there was no way to let people test it before buying. So he designed a "demonstration" version of the software that would let people test it, but not copy it.

His idea: Configure his software to work only after it was linked to a unique computer. So, he developed a way to catalog each computer's individual properties. He found many subtle variations, among even outwardly similar machines.

Ori Eisen, founder of 41st Parameter PHILIP MONTGOMERY FOR THE WALL STREET JOURNAL

"It was amazing how different they were," he says. "There are literally hundreds of things you can measure."

In 1992, he borrowed $40,000 from his parents, filed a patent application for a "system for software registration" and founded a company, Uniloc Corp.

This year, Uniloc started trying to broaden its business away from software-piracy advertisers, to seek new uses for its technology. "What I saw was this different way of looking at things on the Web," Mr. Norris says.

Mr. Norris became CEO and spun off BlueCava to market device fingerprinting both to fraud-prevention and online-ad firms. Eventually, he hopes Blue Cava can fingerprint everything from automobiles to the electrical grid. In October, Texas billionaire Mark Cuban led a group of investors who put $5 million into BlueCava.

BlueCava embeds its technology in websites, downloadable games and cellphone apps. One of its first customers was Palo Alto, Calif.-based IMVU Inc., which operates an online game where 55 million registered players can build virtual identities and chat in 3-D. It wanted to combat fraudsters who were setting up multiple accounts to buy virtual clothing and trinkets with stolen credit-card numbers. Kevin Dasch, a vice president at IMVU, says BlueCava's technology "has led to a significant decline in our fraud rates."

Ric Richardson uses this van as his office. MELANIE TJOENG FOR THE WALL STREET JOURNAL

Later this year, BlueCava plans to launch its reputation exchange, which will include all the fingerprints it has collected so far.

Unlike most other fraud-prevention companies, BlueCava plans to merge its fraud data with its advertising data. Rivals say they don't mix the two types of data.

Greg Pierson, chief executive of iovation, says the company will never disclose specific information about people's Web-browsing behavior, "because it's unnecessary and it's dangerous. It's close to spying."

Mr. Norris says collecting that data is "standard practice" in the online-ad business.

Mr. Dasch of IMVU says he doesn't mind fingerprints of IMVU customers being added to the exchange, provided that they don't contain personally identifiable information such as user names, and that his company can use other exchange data in return.

The idea behind BlueCava's exchange is to let advertisers build profiles of the people using the devices it has identified. For instance, BlueCava will know that an IMVU fingerprint is from someone who likes virtual-reality games.

Other advertisers could then add information about that user. BlueCava also plans to link the profiles of various devices—cellphones, for instance—that also appear to be used by the same person.

Blue Cava also is seeking to use a controversial technique of matching online data about people with catalogs of offline information about them, such as property records, motor-vehicle registrations, income estimates and other details. It works like this: An

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**