



Wintergreen Resort
 Earn Free Rooms
 On Group Bookings!

VIRGINIA LAWYERS WEEKLY

[LOGIN](#) [SUBSCRIBE](#) [DAILY ALERT](#)

Search powered by

- NEWS** Today's News
- This Week
 - Calendar

- ARCHIVES** Search
- Browse
 - Weekly Edition
 - Opinion Digests
 - Verdicts & Settlements
 - Special Features
 - VLW Blog
 - Browse Court Opinions
 - Supreme Court of Virginia
 - Virginia Court of Appeals
 - Virginia Circuit Courts
 - 4th U.S. Circuit Court of Appeals
 - U.S. District Court, Eastern District
 - U.S. District Court, Western District
 - U.S. Bankruptcy Courts

- RESEARCH** Archives
- Important Opinions
 - Virginia Courts
 - Virginia Code
 - Virginia Law Firms
 - Virginia Legal Blogs
 - State Government
 - Other Resources
 - User Manual

VERDICTS & SETTLEMENTS [Submit a V&S Report](#)

- PRACTICE AREAS** Business Law
- Criminal Law
 - Employment Law
 - Family Law
 - Personal Injury
 - Real Property

- SPECIAL FEATURES**
- Virginia's Largest Law Firms
 - Virginia's Largest Verdicts
 - Million Dollar Settlements
 - New Associates' Salary Survey
 - Leaders in the Law
 - Summer Associates Salary Survey
 - Other Features

ADVERTISE Media Kit
[Contact a Rep](#)

- CLASSIFIEDS** Find a Job
- Lawyer to Lawyer
 - Experts
 - Real Estate
 - Legal Products & Services

- OUR PUBLICATIONS** Virginia
- Lawyers Weekly
 - Virginia Medical Law Report
 - Business Law Bulletin
 - Attorneys' Handbooks
 - Gift & Event Guide
 - Editorial Team
 - Virginia Lawyers Media
 - Dolan Media Company

Weekly Edition



Footprints: Many devices create electronic trail lawyers and police can use

By Peter Vieth
March 2, 2009

Like a hiker making his way through the forest, every person these days leaves a set of footprints nearly everywhere he goes. Only the tracks aren't in mud, dirt or foliage – the footprints are electronic, creating a trail that can be used by authorities or lawyers to establish where someone was...or was not.

For some people, the electronic trail reveals misdeeds they had hoped to hide. Even if we're not misbehaving, however, privacy advocates say people need to be aware of the information we inadvertently share about our activities.

By now, most of us have accepted that the phone company knows where our cell phone is. We know our credit card purchases are tracked in some bank's computer files. What we may not realize are the traces left behind by other tools, including some items we may not even recognize as electronic.

How about your grocery store courtesy card that you use to get discounts on breakfast cereal? Or your hotel room key card? Or that lumpy tag hanging from your new coat? All represent ways in which we may unwittingly "bug" ourselves, allowing someone to follow our movements if they have the proper equipment or permission.

Other tattletale devices include your car's GPS unit, the EZ Pass tag on your windshield, and the airbag computer under the dashboard.


Police detectives and private investigators regularly use these devices as electronic bloodhounds, tracking a target – or tracing a trail – to catch a wrongdoer.

Divorce lawyers hit a gold mine with the EZ Pass – a toll road collection system used in 14 states in the mid-Atlantic and northeastern U.S. A driver can place an electronic tag near the windshield and breeze through toll plazas as a scanner charges the account.

Attorneys found the list of toll charges could be used to disprove the alibis of a wayward spouse. A husband who claimed to be at a business meeting in Pennsylvania was undone by toll records showing he was in New Jersey that night, according to an Associated Press story.

Of course, police can follow the EZ Pass trail, too. New Jersey authorities used toll records to reconstruct the movements of a woman who killed her husband, dismembered the body, and disposed of the remains in the Chesapeake Bay.

If you're not in law enforcement, getting those toll road records may depend on which state the target travelled in. The AP found that seven of those states, including Virginia, will turn over records in response to a court order in either a criminal or civil case, including a divorce. Other states will



Appeals

Focus on what you do best.
You handle the trials. When it comes time to appeal (or to resist an appeal), call Steve Emmert at (757) 965-5021 direct. You'll never sweat another appellate deadline.

Recent Honors
THE BEST LAWYERS IN AMERICA
SUPER LAWYERS 2008
VIRGINIA'S LEADERS IN THE LAW

L. STEVEN EMMERT
Appellate Practice
www.virginia-appeals.com
SYKES, BOURDON, AHERN & LEVY
VIRGINIA BEACH

WEEKLY EDITION ARCHIVE

March 2009

M T W T F S S

1

2 3 4 5 6 7 8

9 10 11 12 13 14 15

16 17 18 19 20 21 22

23 24 25 26 27 28 29

30 31

« [Feb](#) [Apr](#) »

NEWS FROM VIRGINIA LAWYERS WEEKLY

Rate-a-Doc: Online services prompt some to use privacy agreements

When clients pay with plastic

Last gasp for breath test machine?

FOIA covers judicial salaries, council says

VBA Professionalism principles debuted

Chesterfield court vacancy – again

IMPORTANT OPINIONS

Medical Malpractice - Expert Witness Certification - Discovery

Tort - Defamation - Public Official - Navy PR Officer

Attorneys - Rule 11 Sanctions - Oral Statement

Criminal - Death Penalty - Carjacking - Juror Misconduct

Creditor's Rights - Satisfied Judgments - Bank Delay - Credit Score - Pa. Law

in response to a court order in either a criminal or civil case, including a divorce. Other states will allow the records only in criminal cases.

While it's easy to see how your grocery store courtesy card can keep track of your purchases, a newer and more sophisticated tracking technique is under fire from privacy advocates in part because users can be so unsuspecting. The technology, called RFID (radio frequency identification), is promoted as a souped-up barcode, a high-tech version of those stripes that are printed on every product at the store.

Higher tech means less privacy, critics say. Unlike printed barcodes, an RFID chip in a product has a serial number that is unique to that item. If the serial number is associated with the purchaser's identity, during the checkout transaction for instance, the item leaves an ownership trail wherever it goes.

Moreover, RFID tags are remotely readable, sometimes from as far as 30 feet away. So an RFID card in your pocket can be read without your knowing. If RFID catches on as envisioned, your identity, your clothes, and other products on your person can all be detected without warning as you pass near a reader. You would never know it happened.

"They can perform a sort of invisible frisk," said privacy activist Katherine Albrecht.

It's not just marketing-savvy retailers who want to exploit the potential of RFID. The U.S. government issues passport cards with RFID chips for easier border crossings with neighboring countries. The state of Washington now offers an "Enhanced Driver License" and ID card that also serves as an alternative to a passport at border crossings.

The traveler cards do not have personal information on them, only a code that points to a stored record in government databases. Reading and cloning the code is not hard, however, as evidenced by a television demonstration (viewable on YouTube) where a hacker drives around San Francisco with an RFID reader and a laptop, gleaning numbers from passport cards. A similar reader is available on eBay for just under \$1,000.

The ease of such invisible snooping "creates an enormous potential for people to be tracked and monitored," said Albrecht.

U.S. Sen. Patrick Leahy, D-Vt., is among those wary of the new identification technologies. "These all raise exciting possibilities, but they also raise potentially troubling tangents," Leahy said in a 2004 speech. "While it may be a good idea for a retailer to use RFID chips to manage its inventory, we would not want a retailer to put those tags on goods for sale without consumers' knowledge, without knowing how to deactivate them, and without knowing what information will be collected and how it will be used."

An older, more familiar technology also leaves electronic footprints invisible to the user. Hotel room key cards can create a record of when they are used to open the door. Hotel key records undermined a killer's alibi in a case several years ago, according to Henrico County

Commonwealth's Attorney Wade Kiser.

"The defendant was traveling to Atlantic City," Kiser said. "He gave a story to police about when he was there and not there. His story did not correspond to the electronic key records."

The man ended up pleading guilty to the murder of his wife, Kiser said.

While some folks fall victim to their own electronic tattletales, new technology means it's child's play for anybody to plant an electronic tracking device on an unsuspecting target.

Just ask George Ford Jr.

The former New Jersey contractor is facing a 25-years-to-life sentence in New York after he was convicted of the second-degree murder of a 12-year-old babysitter.

Ford told police he accidentally ran over the girl while turning his truck around on a remote road. He said he was trying to show her his horses in a nearby pasture. With no other witnesses to the "accident," Ford was facing only a reckless endangerment charge.

Then, Ford's wife went to authorities with some unexpected information. She had planted a GPS tracking device on Ford's truck because she suspected he was being unfaithful. Using the tracking data, detectives were able to show that Ford had been alone with the girl at a single remote location for several hours before the fatal incident.

The evidence that the two were alone together for a period of time undermined Ford's accident explanation. Prosecutors upgraded the charge to second-degree murder, arguing that Ford killed the girl to keep her from talking about whatever happened during their time alone.

This month, a judge found Ford guilty on the murder charge.

While it was homegrown detective work – not government surveillance – that brought Ford to justice, what if suspicious police officers planted a tracking bug on a suspect without a warrant?

That's what helped to catch David Foltz.

A year ago, Fairfax County police were trying to catch a man who had assaulted nearly a dozen women in several Northern Virginia communities. Foltz was a suspect, but nothing tied him to the crimes except prior similar attacks.

Without asking for a warrant or getting limitations on their surveillance, the police put a GPS tracking device on Foltz' van. After four days, they looked at the record of his travels and decided that he was "hunting" for another victim.

Police then decided to physically follow Foltz, suspecting that he was about to commit another assault. The suspicions were confirmed the next day when Foltz dragged a woman into a dark area

and assaulted her. A detective rescued the woman within seconds and arrested Foltz, who now is serving a life sentence.

Despite their obvious good hunches that caught a bad guy in the act, Foltz' lawyer claimed the police took GPS surveillance too far. Chris Leibig argued that, unlike previous GPS tracking cases approved by the courts, the police here allowed an unmonitored computer to do their gumshoe work for them, without regard for the limits that would apply to an actual detective. "It's much more intrusive," Leibig said. "It makes no distinction between public and private areas."

The judge in Foltz' trial disagreed. "The defendant has failed to show that there has been any actual invasion of his privacy," said Arlington Circuit Judge Joanne F. Alper, according to a published account.

Leibig hopes the Supreme Court of Virginia will review the case to determine whether police suspicion is enough to justify warrantless, unattended GPS tracking.

Whether or not we have anything to hide, privacy advocates maintain that convenience in the modern world should not require a complete lack of anonymity and the unnerving sense that everything we do is being logged into someone's database.

Albrecht, the privacy activist, makes the case for limits on electronic identification, even if it's benign: "There's got to be a place of psychological respite, where we know we're not being watched."

© Copyright 2009, by Virginia Lawyers Media, all rights reserved

[< Previous article](#)

[Next article >](#)



[Subscribe >](#)

READ COMMENTS

We're All Truman Burbank | Probable Cause, on March 4th, 2009 at 10:46 am said:

[...] Horton, according to NNDB.com (ironic motto: "tracking the entire world") died of a stroke in 2004. But I was reminded of him this morning while reading an article about electronic trails, lawyers and law enforcement. [...]

POST A COMMENT

Your name: *

E-mail: *

The content of this field is kept private and will not be shown publicly.

Homepage:

SUBMIT

We need to make sure you are a human. Please solve the challenge below, and click the I'm a Human button to get a confirmation code. To make this process easier in the future, we recommend you enable Javascript.



I'm a Human

Submit Comment



**Wintergreen Resort**

**Earn Free Rooms
On Group Bookings!**



[About Us](#)

[Contact Us](#)

[User Agreement](#)

707 East Main Street, Suite 1750, Richmond, VA 23219 (800) 456-5297 Fax: (804) 783-8337