NEWSLETTER

Identity Theft 911®

VOLUME 5
ISSUE 11
NOVEMBER
2008

AMERICA'S LEADING IDENTITY MANAGEMENT AND EDUCATION SOURCE

THIS MONTH'S TOPIC...

Saving Lives, Fighting Crime... Invading Privacy?

New technology bring new challenges

Notes from our Chairman, Adam K. Levin

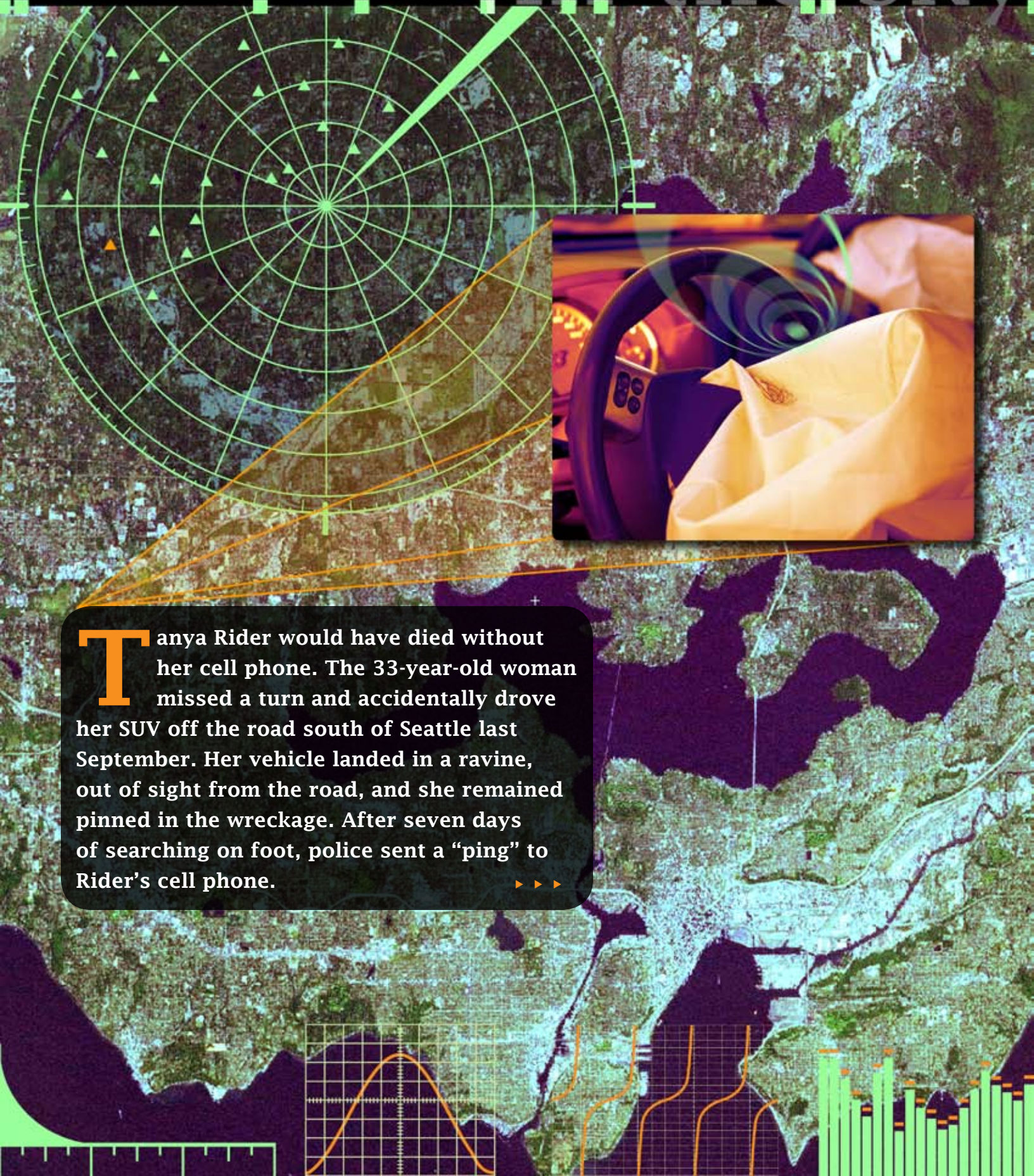
Amid all the new technologies we have to find each other, it's quite easy to get lost. In the last five years we've seen hundreds of new applications that use GPS, cell phones, RFID or WiFi devices to track what was previously untrackable. It's easy to forget that as these technologies help make us safer, more efficient, more profitable and better connected, they also have the power to rob us of our privacy, and put our identity at risk.

What we present in this month's newsletter article, "The Eye in The Sky: Better People-Tracking Though Technology" is not an exhaustive list of new tracking technologies. Instead we attempt to highlight the fastest-growing, most popular applications, and explore their ability to cause both good and harm. This month's editorial, "Who's Shadowing You?" is the beginning of a conversation, but by no means the end, about how we might harness this new power without losing the rights we cherish most.

For a complete newsletter archive, visit: www.identitytheft911.org/newsletters
To learn about the latest scams on identity theft, visit: www.identitytheft911.org
Comments, questions? Contact us: newsletter@identitytheft911.com

the eye in the sky

better people-tracking through technology



Tanya Rider would have died without her cell phone. The 33-year-old woman missed a turn and accidentally drove her SUV off the road south of Seattle last September. Her vehicle landed in a ravine, out of sight from the road, and she remained pinned in the wreckage. After seven days of searching on foot, police sent a "ping" to Rider's cell phone.

"The phone sent a faint electronic response to the nearest cell phone tower, which helped police narrow their search and rescue Rider, who was on the verge of dying from hypothermia and internal injuries. Had it been any longer, she might not have survived," State Patrol Trooper Jeff Merrill said at a press conference.

Meanwhile, a few miles away in downtown Seattle, attorney Albert Gidari Jr. was noticing a disturbing trend. As a lawyer who specializes in telecom issues and privacy, Gidari monitors requests for access to records that document the exact location of cell phone owners. In hundreds of cases, Gidari noticed, federal law enforcement agents won access to those records without proving probable cause to suspect that the individual in question might have broken a law, and without obtaining a warrant. The practice continues today.

"It's full tracking capability," Gidari told the *Washington Post*, "It's a scary proposition." Giadari did not return phone calls seeking comment for this story.

A New Day for Spying

Technology is making it easier than ever to find people. The advances are being used to improve safety and save lives and to solve smaller but vexing problems, such as getting lost in a new city or losing friends in a crowd.

Some new uses raise serious privacy concerns, however. Whether it's a jilted lover spying on an ex, a corporation using location data to create precise consumer profiles or a government agency collecting data on innocent civilians, privacy experts worry that the new generation of tracking devices threatens to make America's long-held beliefs about privacy obsolete.

"We have the ability to track with a level of accuracy that most people probably don't know is possible," says Harry Trombitas, an FBI special agent who uses leading-edge techniques as head of the bank robbery unit in southern Ohio. "We can get it down to within a few feet."

All that data must be stored somewhere. Without proper passwords and encryption, it could easily fall into the hands of identity thieves, who could use it to build a precise picture of your shopping habits and daily routine.

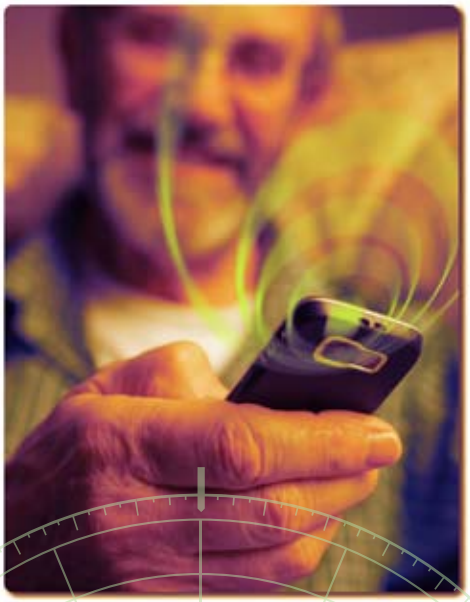
"Location data is extraordinarily rich," says Lee Tien, senior attorney at the Electronic Frontier Foundation. "If you track every movement I make for a week, you'd have a pretty good idea of what I do, who my friends are and what kinds of relationships I have. It gets very invasive very quickly."

The Technologies at Work

This new era of tracking is driven less by new technology than by the artful packaging of old technology, especially the Global Positioning System (GPS) and cell phones. The Federal Telecommunications Act of 1996 required all cell phones to be capable of communicating their location to emergency responders, either by sending a signal to cellular towers or by installing GPS chips into phones. Since then, GPS itself has evolved from an expensive novelty into a common, stand-alone product.

Other location devices have remained obscure so far, but may yet grow in popularity. There's Skyhook, a Boston-based company that maps all the Internet hotspots around the country and uses them to home in on the location of wireless devices, from Personal Digital Assistants to laptops. There's also Radio Frequency Identification (RFID) which uses tiny transponders to communicate bits of data via radio waves.

"All of these technologies can be used for tracking," said Jim Van Cleave, vice president of Spectrum Management, which was started in 1980 as one of the first companies specializing in tracking technology. "The only question is how do you want to use them? What problem needs to be solved?"



When Tracking Equals Safety

Perhaps one of the best examples of putting tracking devices to good use is Project Lifesaver. The Virginia-based nonprofit gives bracelets equipped with

GPS, radio frequency and cellular trackers to people with Alzheimer's disease. Oftentimes, these patients can become disoriented and wander off, which quickly can become a life-threatening situation if they get injured or become dehydrated.

With Project Lifesaver, caregivers call local police and inform them that a patient is missing. The police use the bracelet's three tracking devices to home in on the person, cutting days of searching down to a few minutes.

"I can't tell you how many times we've gotten there in the nick of time to find traffic stopped with a patient standing there in the middle of the road," says Barry Thacker, operations chief for Project Lifesaver.

Crossing the Line?

In other situations, the value of tracking is heavily debated. In a well-known case in Washington State, police and prosecutors argued they did not need a warrant to place a GPS device on a suspect's car because doing so is the same as assigning a police officer to trail the suspect.

The Washington Supreme Court disagreed, saying in a unanimous decision that GPS tracking is a more invasive form of surveillance, and therefore requires a warrant. Most other states have no consistent rules on the subject, however, leaving police free to enforce the law as they currently interpret it.

This is what concerns privacy advocates. "The whole logic that this is the same as traditional tracking is facetious," says Tien. "Assigning police officers to follow someone is an expensive proposition. When you can do the same thing with an inexpensive GPS system, it opens up a world of surveillance possibilities that never would have been conceivable before."

A Delicate Balance

Another type of location information that often winds up in courts comes from E-ZPass and other electronic toll booth systems, where motorists pre-buy toll credits that are stored in miniature computers and relayed to the toll plaza via RFID. Each pass through a toll booth is recorded and stored in a database permanently. That data is regularly subpoenaed by police trying to establish the movements of a suspect, and oftentimes by divorce lawyers trying to prove that a spouse is having an affair.

Here privacy advocates tread a fine line. If data can be used to solve a crime or settle a legal dispute, it may be of value. Then again, motorists buying into E-ZPass probably never suspect that their movements will be tracked and recorded permanently.

"I don't want to be seen as supporting infidelity," says Paul Stephens, director of policy and advocacy for Privacy Rights Clearinghouse. "But when the technology is available it will be used, for good or ill."

Other car-based tracking systems raise concerns, too. Progressive Insurance is rolling out a new program that uses GPS to track how far and fast people drive, offering lower premiums to safe drivers. A similar system is OnStar, installed on all General Motors cars. Starting this year, the company can use OnStar to kill the car's engine and force it to stop – from remote – if contacted by police who suspect the car has been stolen. This means that GM now has the ability to track every one of its cars anywhere in the country in real time.

Both GM and OnStar promise not to misuse the data.

"We have an opt-out process where if for whatever reason you have an OnStar and you're uncomfortable with a particular capability, you can disable it," says Chet Huber, CEO of OnStar.

But large loopholes in both companies' contracts concern many privacy advocates.

"If you read the fine print, most of these contracts say that the company can change its policy at any time, so that's no guarantee for consumers," says Carmen Balber, an analyst for Consumer Watchdog, a California-based, non-profit consumer education and advocacy organization. "Inch by inch, Americans are losing their privacy to this type of surveillance."

Spying Beyond the Booth

In some states, government surveillance doesn't stop once you leave the toll booth. The Missouri Department of Transportation has a pilot project in which it accesses cell phone companies' records of phones passing by towers located along highways. The states say this is a low-cost way to monitor traffic patterns and look for bottlenecks. The companies involved say that the records are anonymous and scrubbed of personally identifying information.

But because the companies involved retain the right to change the contract at any time, privacy advocates say there is no guarantee that this data won't be misused in the future. In San Francisco, the city council rejected using cell phone data because of concerns that it may invade privacy, and instead spent $35 million to install roadside scanners.

The concern is less about traffic monitoring as it is with other ways such data could be used. For example, researchers at Massachusetts Institute of Technology are looking into ways to use students' cell phone location data to infer a variety of personal details, such as whom they're friends with. As such behavioral models become more advanced, they could also be used to predict where students like to shop and what products they'd like to buy.

"In the world of data mining, the general belief is that if the data is there, the miners will come," says Tien. "As these technologies become cheaper, all of their benefits and their dangers will rise."

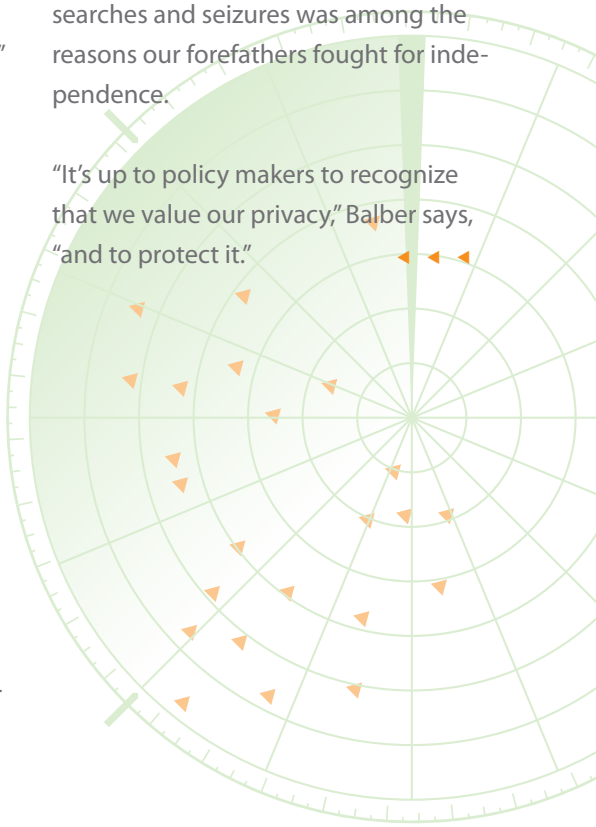
New Technology Requires a New Conversation

Precisely because the new generation of tracking technologies has so many potential uses, it's impossible to say which technologies are beneficial and which invade privacy. In reality, they all have the capability to do both. But at the moment, all of these new technologies and uses are dealt with ad hoc. Corporations, government and consumers generally push to expand the use of individual technologies for specific uses – easing traffic flow, for example, or connecting with friends – while privacy advocates combat the uses they find objectionable.

What is lacking so far is an overview that looks at all these new technologies collectively and recognizes them for what they are: A vast increase in the power to monitor human activities that heretofore remained mostly private. And beyond such generalities as the Fourth Amendment and subsequent legal decisions defining what privacy meant in a previous technological age, we have no rules, no line in the sand saying: You may surveil up to this point, but no farther.

The scientists, marketers and users who continue to pioneer new uses for these technologies are not going to stop. Nor should they. It is up to us as citizens, rather than as consumers, to have this conversation, to draw the boundaries, to write the rules. In so doing, we must remember Tanya Rider trapped at the bottom of a ravine. We also must remember why protection against unreasonable searches and seizures was among the reasons our forefathers fought for independence.

"It's up to policy makers to recognize that we value our privacy," Balber says, "and to protect it."



Who's Shadowing You?

The Dual Face of Tracking Technology

By Eduard Goodman, Chief Privacy Officer, Identity Theft 911

To the satellites above, those of us outfitted with a tracking device (and, lest we forget, with cell phones many of us are) are little more than small, anonymous points moving about the coordinates on a map. From on high, the satellites that follow the points are impartial witnesses as they collect, record and transmit the details of our daily activities in cold, mathematical terms to humans, who take that data and translate it into meaningful information. At turns, this information has saved lives, it has brought criminals to justice, it has potentially prevented crimes—and, according to some experts, threatens the very foundation of what we hold dear in a democratic society: our privacy.

The technology of tracking is changing so fast, sometimes it's easy to get enthralled with progress—it's practically addictive. Certainly, it's understandable. You can use your cell phone to track your friends in a crowd, or use wireless hotspots to help navigate a new city. Just when we've incorporated a new instrument in our lives, something new comes along that reinvents how we go about our day. The more technology advances, the more convenient—or more exciting—our lives become. And some technologies don't just make our lives easier or more exciting, they make them safer: GPS units capable of detecting a crime before it happens, anyone? Who wouldn't want that? (More on that in a minute.)

A new era

Even though the finer details of this new era have yet to be filled in, the broad strokes already are visible. Advances in GPS, cell phones and computing power make it possible to track people with greater accuracy than ever before.

Just as the last great expansion of computing power—the Internet—opened up vast new opportunities for good (finding friends on Facebook) and ill (stalking people on Facebook), so does the proliferation of bargain-priced tracking technology encourage both the best and worst sides of human nature. It can tell worried relatives the location of a lost Alzheimer's patient just as easily as tell a private investigator where you were last Wednesday night.

One Seattle-area company uses GPS to track semi trailers as a crime-prevention effort. If a truck stop has been placed off-limits because of the high number of shipments stolen there, and a trucker stops at that location anyway, the company knows immediately and calls local police to report a possible theft.

What's disturbing, however, is the potential for abuse of this technology by consumers, corporations and government.

Goodby, old school

Thirty years ago, the only way to track someone from a remote location was to place a bulky radio transmitter in his pocket and follow the signal by helicopter or plane, just as Jim Van Cleave's company, Spectrum Management, did to track American CEOs who were kidnapped abroad. Today, anyone can go to the website of Rocky Mountain Tracking, Inc., and buy a device the size of a D battery that gathers the location, date, time, speed, and direction of any moving thing for $199. How many jealous exes would consider that a small price to pay to keep tabs on their former spouses?

And how many police would like to use such cheap equipment to keep their suspects under constant surveillance? According to recent reports by the *Washington Post*, quite a few. In cases around the country, local and federal law enforcement agents are engaging in nonstop surveillance of suspects without proving probable cause or even asking for a warrant. Perhaps equally disturbing is the prospect of private companies gathering and selling information on our every movement in an effort to determine our buying habits. And of course, instead of simply knowing our names and account numbers, a criminal can use these technologies to learn our daily commutes, where we like to shop, and the times of day when we are never home. Bit by bit, these uses are eroding our privacy and endangering our identities.

Time for a conversation

Let's get one thing straight: Banning technology never works (consider the Luddites' effectiveness against the cotton mill). Besides, growing tracking technology companies have the power to boost our sagging economy, entertain us, and save lives, even as they threaten to undermine our privacy and our identities.

An intelligent response, therefore, is to set limits on uses, not the technology itself. For this, we will need a conversation about the basic principles of electronic tracking:

- **It requires a warrant.**

Unlike police officers, tracking devices never go home to sleep. And because they record all types of location and movement data in perpetuity, GPS trackers are much more invasive than traditional human surveillance. To guard against abuse, police and prosecutors need to prove in court they have reasonable doubt before using this technology to track a suspect.

- **It must be voluntary.**

Our cell phones have the power to track our every move, and those movements are saved in databases. What happens to that data then? Police and attorneys regularly subpoena it. But what's to stop the cell phone companies from selling that data to others who might use it to infer our private habits? Right now, nothing. That's wrong. We need laws requiring companies to ask our permission before selling our location data.

- **It must limit abuse by private citizens.**

Should a stalker or disgruntled ex be able to track his or her victim for $199 (or at any price, for that matter)? In coming years, we expect this will set off waves of alarms among organizations that protect victims of domestic abuse. Perhaps we need tracking control like we need gun control—laws that mandate a cool-down period before trackers can be purchased, or ban sales to felons.

- **It must be protected.**

Thieves who steal money or identities would love to hack into a trove of location data. We need laws requiring this data to be encrypted and stored securely.

Let's not go to the dark side

The new era of tracking technology is creating a mountain of information that never existed before. That data can help enrich our lives, but it also can be abused by governments, corporations and random delinquents who aim to gain power over innocent citizens. We must acknowledge that this mountain of information is more than cold data—in sum total, it's our *lives*—and we therefore must protect it accordingly. If we don't, we may find that a technology that could change our world for the better—by saving our loved ones and solving crimes—is broken and corrupt before we can truly reap its benefits. ■