

MORE ENCRYPTION, PLEASE

Sasha Cavender, Freelance Journalist

I'm delighted to be here, since I discovered a few years ago how much exhilaration and adventure I was missing by not spending more time with scientists. They experiment with ideas the way artists experiment with colors. They play with puzzles and problem-solving the way children play with blocks: "how high can I build this thing without it falling down? How about if I put them sideways ...?!"

I learned how to use the world wide web from the man who invented it, Tim Berners-Lee. What intrigued me more than the web, was the way Tim thinks: his very elastic and venturesome mind. And so encryption, once arcane and a bit remote to me, now seems fascinating and increasingly relevant. But it's like the yellow thread in a tweed jacket. No one sees it's there until you point it out to them. Then they **always** see it.

Every level of the Internet - from simple news headlines to serious research, financial investments, foreign sites, a friend's email - now poses problems for which encryption may have the answers. **How can we continue to be private people in this giant public space?**

How do we protect our income, investments, competitive research, original artwork, honest opinions, personal correspondence and so forth?

As a member of the media, I'd be the first to criticize what we do, and **do not** write about today. We over-cover sensational issues. But the vast majority of Internet users are directly affected - not by child pornography, say - but everyday problems we barely mention in print or on TV. As the web is growing at accelerating speed, so are many security and privacy issues, not just for governments and big business, but mom-and-pop shops who've been encouraged to jump on the web and start doing business there.

We all want to communicate privately, honestly, and not edit or whitewash our thoughts. We want to browse freely - **anywhere** on the internet - without being secretly watched, followed, or analyzed. We want to buy things safely. We want to sell things safely. We want to control our communications, and our finances, in

our own time and space which the Internet provides. It's incredible convenience 24 hours a day.

My understanding is, the technology to do this already exists; the algorithms are there. The most urgent problems facing encryption now are not technical; they're social, cultural, philosophical. We don't have the answers but we definitely need to start asking the right questions. This is a matter of opinions more than facts. And I'd like to say upfront, these are just my opinions unless I'm quoting someone else's. I don't like to say "I think" or "I believe" before every sentence because it sounds so tentative and apologetic. But as a journalist, I'm a bridge between two worlds: a fast-paced technology industry and everyday users of the Internet. Who don't really understand yet how most of it works: what the difference is between the Web and the Net, what VRML is, what HTML is, how programs work, and so on. Most days, I am trying to explain your work, your world to everyday newspaper readers. Today, I'm trying to explain their concerns to you. I travel about 50% of the time, and I spend most of my time listening, not writing. That may surprise you but it's true. Reporting is mostly research, careful listening, acute observation.

People often tune out when they hear the word "encryption" because it sounds so esoteric. It's not. I believe encryption is what makes possible the basis of all meaningful human transactions taking place electronically: it protects *trust*. Trust in personal relationships, financial relationships, medical - government - the list is endless.

For example, you trust that your bank is taking good care of your money; and the bank trusts that you're honest and won't use the ATM card they give you to hack into other customers accounts to steal. Wives and husbands, children and parents, employers and employees, government heads, academic researchers, friendships at every level depend on trust --- that we are who we say we are; and we do what we say we will do; we don't lie and misrepresent our behavior.

When there's betrayal - not honest mistakes, or miscommunication - but a deliberate betrayal of trust, you cannot restore it. I'm not a psychologist, I can't tell you why this is so, but in years of reporting what I've seen is this: when trust is broken it's like Humpty Dumpty - you can't put it back together again. Some long-term memory guards against it. Trust is precious, it's the coin of the realm. The

internet without it isn't really viable, I think, it can't keep growing in the amazing ways it's grown if people have good reason to mistrust their transactions there.

There's a growing backlash to a number of practices on the net right now, like banners, increased registration requests, new tollbooths being put up every day. People are starting to object. They want protection from all the noise, all the distraction, all the keeping score of what they're doing. They wish cryptographers would sew them capes to make them invisible on the net. "Just put on my coat and let me go out the door."

There's anxiety at best, paranoia at worst. There's larceny, there's invasion of privacy, deceit and sneaky behavior - and there's a potential for more serious abuse if we don't start discussing the social issues. American medicine has been grappling with parallel issues for decades. Technology continues to develop faster than social awareness, so we have incredible life-saving technology but we're not clear when and how to use it, or withhold it.

The "cookies" type of technology is just one example of quietly invasive technology that's being used. It's only the tip of the iceberg. The vast majority of web users have NO idea it exists, or that it's being used like a 'reverse encryption' to secretly tag them, fingerprint them as they travel around the Web. They think they're following their curiosity. They don't know that ISP's and web site owners are following *them*.

When consumers are told, they are often shocked. Outraged. First there's disbelief, then they feel violated. It's like schoolgirls who are suddenly told someone's been staring down at their black patent leather shoes, not out of shyness, but to see their underwear. Consider stepping out of the shower, and seeing an intruder right there, watching you. If you and I are talking, standing next to one another and I step forward, you will automatically step back - because I have invaded your personal space. It's psychological, not just physical.

People in the industry often say, "Oh, it's not that bad." People outside the industry - ordinary Internet users say "It's *that bad*". Because, they believe the net is a huge public open space and

marketplace, where they can wander unnoticed and anonymous as if they were on a busy street in Calcutta, or New York. They think they're window-shopping, and nobody knows or cares how long they look in each window. Or browsing in a bookstore. They have NO idea when cookies-type technology is being used and someone is tracking them - who cares, and plans to make use, perhaps commercial use, of that information.

One web developer told me: "Cookies aren't just okay, I think they're fabulous! Look, information isn't free. When you come to a web page, you are actually asking for information. In exchange, I want information about you. You better talk to me, and you better tell me the truth because this exchange is based on trust."

"Trust" is the word he used, by the way. He believes there is an implied agreement between the visitor and website owner. Consumers have a different perception altogether. Just as no one can see them in their bathrobe, on the internet at 3 o'clock in the morning, they think no one can "see" them on any website. Perceptions are real, and very hard to change.

The web developer explains, "You're getting the information you want. I'm getting the information about you that I want." "Wait a minute," I say. "I didn't know you were collecting data on me, you never told me that." "Well yes," he says, "It creates a database. Cookies are just a memory of a personalized relationship." Not if I don't know we're having one.

"Would you rather pay me \$5 or fill out a questionnaire?" he asks, to justify the "free exchange" of data that is taking place without my knowing it.

The problem is - at his and most other sites - we aren't given that choice. Some of us would actually rather pay, just to be left alone. Some of us would rather leave the site immediately, and not play the game. It's not a game, it's surveillance.

Technical people usually know how to turn off information-collection types of mechanisms. Can encryption shield the rest of us?

This type of technology has been around a long time. But when it's now embedded in browsers that most of the world is using - and

consumers aren't told, aren't warned - we need to discuss disclosure. It's a social issue, again, not a technical one. But technology - encryption - can offer consumers protection.

The owner of the site, or browsers - ideally both - have an obligation to inform users: information is being gathered about you. Who's doing the collecting? And what are they doing with it? How might it potentially be used? If you're out there trolling for data, I believe I have a right to know I'm being watched. And the right to avoid your site. There must be full disclosure, both parties must have equal knowledge otherwise they're not really both parties to the contract. You can't be tricked into it, lured onto the site because it's cool. As the website's owner, you must be sure the person visiting your site understands what you're asking of them, so they can make a rational decision. "By the way, we use cookies" is not sufficient.

When the telco's implemented "Caller ID" they notified customers of the option to "block" your number, if you preferred, for privacy. Maybe encryption can do the same thing here - block our digital presence so we can move unnoticed around the web.

The same technical experts who say tracking is "not that big a deal" cannot agree on what cookies-type technology can - and cannot - do. This is scary for an everyday user: if the experts don't know for sure, why should ordinary folks be reassured it's "no big deal"?

I've been told conflicting information. With existing monitoring technologies today:

- Each site where the technology is set knows only that you have been there --- nowhere else, no further information about you.
- Each site knows where you came *from*.
- Each site knows where you *go next* if you follow a link from their site.
- If they really want to they can compile information about your visits to *other sites* that have the same technology in place.

Well, which is it? And of course composite information is more dangerous if you want to protect privacy.

Watching data packets, traffic tracking - it's all going on and users of the Internet *outside* the industry are blissfully unaware. ISP's have a golden opportunity to see who's talking to whom, and profile the source and destination addresses. Of course, I'd argue all this information which website owners may be paying to get, and selling to marketing lists may be pointless. You know where I am but not why I'm there. And that's the only thing that matters. Sitting on a lake with hooks in the water all day trying to snag something, doesn't sound very productive

Other countries are more enlightened, I think, on the social and public policy issues. England, I believe and parts of Europe already have laws on the books about this. You can't combine seemingly unrelated information, whose value increases when you combine 2 or more facts. For example, I give my birth date to one company, my mother's maiden name to another. Neither is all that important. But combined, you may be able to get at data I don't want you to see.

STOLEN ART/CREATIVE WORK - WILL ENCRYPTION MAKE US DIGITAL
NAMETAGS? DIGITAL WATERMARKS?

I became very interested in a widespread application of encryption earlier this year, when I launched a website as a public forum to encourage debate about intellectual property and copyright violations, as more publishers move online. I expected writers to have controversial things to say. I was caught offguard by the visual artists who sent me email.

It's incredibly easy to steal original artwork over the net. A quick-click to save and it's yours. Theft is up, morality's down. Can I swipe what I want for my website? Who's gonna stop me? Should we encrypt Web graphics to prevent this?

I will read you some of the email I received with the actual names and objects removed:

" What about original artwork getting stolen? With a dearth of artists, and a proliferation of web sites, a lot of web-oriented art is being stolen on a regular basis. (I do not plead innocent here, I might

add.) I was cruising to an old URL a web page which is quite popular. I noticed the "car" on the title page looked similar, nay, EXACTLY like the one I created for my web page except it was a tiny bit smaller in size. So, I downloaded the file and did a color index check of the primary colors. It matched mine exactly. [the writer described to me how color indexes work]

"Coincidence? Doubtful- those are pretty tall odds for 2 sets of 3 numbers to match exactly AND in the correct order.

"Did I care? No. I was flattered they used it and told them so! I doubt if they even remembered where they got it (before I told them).

"BUT- I admit that "the car" was NOT my creation! (See? A lot of people do this.) I cut it out from someone else's , as the colors used were all wrong. I also admit I should have asked and informed who I got it from. In fact, I think I am going to check my bookmarked pages and track the person down. But they probably stole it from someone else!

"That's a small example of what I'm getting at. A bigger issue, are buttons, icons, backgrounds, etc. specifically created for pages and NOT part of the public domain.

"This is causing some concern among web site creators. We are in the midst of re-doing our site now with completely original artwork, rather than the public domain stuff which currently graces it. And I am sure some of that original work will find itself elsewhere."

Some artists spend hundreds of hours creating original designs. It's their livelihood. Should people rip them off for free? What about a digital watermark on original graphics? It can be done, I believe, so it's invisible and repeated throughout the image in a redundant fashion so the tag is everywhere. But it's not in public use yet.

Your homepage is your *electronic home*. I don't go into your real home and help myself to a Persian rug because I like it, and can't afford it, and it's easy to sneak it over to my house. Should I commit larceny at your electronic home? Or *isn't* it larceny? What is it?

Clearly we need to strike a balance between this free-for-all, anything goes; and identifying *everything* like children going off to summer camp with their nametags sewn on every single sock . That's excessive. But so is the amount of stolen graphics and text right now.

MONEY \$\$\$\$\$

Financial security is so fundamental and problematic we could talk for hours. I'll just say fraud is so much easier to commit on the internet with millions of ten-cent heists. Three-cent heists for that matter. Who's going to notice a 3 cent or 10 cent discrepancy on a bill? Since nearly everyone is being encouraged to put their business on the web, and shop there, this is a priority problem for cryptographers. Writers need help in explaining the issues to their readers.

Then there's the government export laws which seem to put a real damper on American business. They also sound like the agricultural laws we have which forbid American farmers to use certain pesticides because they're toxic. Meanwhile we sell those same pesticides to farmers in other countries whose produce we import. Allowing only 40 bit keys instead of the 128 bit keys people want to use makes little sense even to a common Internet user like myself. A well-known supercomputer company in Silicon Valley has, on a single machine, broken the 40 bit RC4 challenge in three days using old hardware. With their current line, they did it in less than three hours. And their next hardware product is that much faster. What's wrong with this picture? It's not in the news, for one thing, and it should be. Because the outcome affects everyone's business.

Lest this all sound like a laundry list of woes I want to end with a reminder of why we're all here, and hope to have the same reasons to meet again next year, maybe in Tahiti or the Seychelles Islands. It's a passionate interest in the Internet and its still-untested possibilities, uncharted waters. Right now the most popular use of the Internet is email and it's not about spams and flames. It's every users, like families, who have discovered email is the best way, sometimes only way to stay in touch with their college-bound children. It's cheap or free, it's convenient and you're never

interrupting anyone or waking them up. It's like sitting around the kitchen table and talking about everything under the sun.

You know no one's reading your postal mail, no one's slit open your love letters or bank statements unless you're a target of law enforcement. But email has no envelope and encryption is needed to protect the intimacy and privacy of our conversations. We don't want to just say, "hi mom, exams are over" or "it's snowing"- we want to say more personal things - just as we would at home to the people who know us best: "Your dad just got fired, he's so depressed I hope you can come home some weekend"... or "Grandma's surgery went okay, she's getting out of intensive care today..."

Part of the problem is, there is no consequence for invasive electronic practices.

If privacy is violated it may be hard to win consumers back if they feel they were burned badly enough. Like the senior citizens who use the net in large numbers --- for hobbies, like genealogy or quilting; and taking care of their own financial portfolios. You don't want to lose their trust in this new medium, because we're letting people spy and snoop and create secret databases because, "Gee, everyone has to earn a living." Not at the cost of our trust.

EN

I think the best and shortest description of the Internet's brilliance as a medium for communication was written by the author and environmentalist, Paul Hawken. In an email recently to someone he said:

"I can't see your eyes or your facial expressions or hear your laugh, but your mind and spirit come through in your words, and in some ways, it is what we sometimes miss when in someone's physical presence. There is that strange and wonderful story in Pilgrim at Tinker Creek where a blind person from birth, cured at middle age, scratches his eyes out to become blind again. He could see more without his eyes."

That's it! The Internet lets us hear better. Hear the truth, the intellectual idea, the personal vision, the point of view, much

better sometimes than in the real world. There's no designer t-shirts or regional accents or status-symbol trappings to get in the way of honest, direct communication.

I'm a writer and words are my tools, my jewels, my emotional bank balance. They have a wonderful integrity in simple ascii text - they don't change color or character the way they can, when they're handwritten. I don't want to lose the privilege or pleasure of communicating with friends and colleagues all over the world. I think more everyday encryption may be essential to do this. Not harsh, severe, locks and barrel-bolt encryption, but some kind of protective armor as light and strong as Tyvek. The same way a widow's veil grants her respect, privacy as she moves through the everyday world - a gentle buffer and reminder to please leave her alone.

I live on an island where a neighbor just told me, "We bought that house on Main Street, lived there for decades and raised our three children there, then sold it - without ever owning a front door key." The Internet used to be like that. Open, trusting, quite secure. Those days are over, on our island and on the Net.

Realistically, I think encryption is more a necessity, not an add-on. Our postal mail has a simple seal that locks up your letter when you lick the envelope. Can encryption give us something this simple in the Internet world? Digital sealing wax?

I leave you with Paul Hawken's quote and also a Chinese proverb:

"If we do not change direction, we'll end up where we're heading."

###