CNET News
Politics and Law
January 28, 2010 10:55 AM PST

It's been 10 years: Why won't people pay for privacy?

by Declan McCullagh

Share

An Internet startup wants to sell you the ability to protect your privacy, allowing you to create different online identities for different purposes and cloak your true self from prying eyes.

Early press coverage has been uniformly positive. CNN.com's review **says** "Total Digital Privacy May Be On The Horizon." The San Francisco Chronicle's **article** is titled "Online Disguises From Prying Eyes." To **BusinessWeek**, it's a "A Big Boost For Net Privacy."

"Think about how much business is predicated on the flow of personal information!" one of the founders predicts. "If you need to add privacy as a foundation under all of that, what is that industry worth? It's huge. Billions and billions and billions."

The year, of course, was 2000, and the company was named Zero Knowledge Systems. Even by the standards of that era, it spent staggering sums of money with virtually no sales: ZKS brought in only $400,000 in 2001 in license revenue from its flagship Freedom software, while losing $24 million a year, according to **documents** filed for its initial public offering. The IPO was cancelled two months later, and ZKS abandoned the idea of selling privacy for a profit; under a new name it sells IT services to Internet service providers.

Fast forward ten years, and a group of companies including Google, Microsoft, and Intel, along with some government agencies, have declared that January 28, 2010 is officially "**Data Privacy Day**." The idea, **according to** the group's Web site, is to spur the "development of technology tools to promote individual control over personally identifiable information."

Which sounds exactly like what ZKS tried, and failed, to convince the public was a good idea. And it's not just one company: a 2001 **article** in The Atlantic rattles off a list of companies that were hoping to attract privacy-sensitive Internet users. The list includes IDcide (dead), PrivacyX (defunct), American Express' Private Payments (**ditto**), and Disappearing.com (you guessed it).

The Atlantic article mentions ZipLip, founded to protect e-mail privacy; now, under the name ZL Technologies, it **offers** innovative ways to "find relevant information hidden in massive volumes of data" for legal discovery processes. Anonymizer.com was founded by cypherpunk Lance Cottrell to provide privacy-protective Web surfing to the public for a reasonable fee. It's now part of Abraxas Corporation, a northern Virginia firm that shares its name with a **comic book villain** and has close ties to the CIA and FBI. The Electronic Frontier Foundation, which **once enthusiastically recommended** Anonymizer.com, says it no longer does because of Abraxas' links to the U.S. national security apparatus.

Neither ZKS nor Cottrell responded to requests for interviews for this article.

Meanwhile, companies accused of invading privacy have prospered. Winning a **Big Brother Award** from the activists at Privacy International is closely correlated with marketplace success; savvy investors can be excused for cheering whenever a corporation is presented with the prize (which is, in a nod to George Orwell's **famous phrase**, a golden boot stomping on a human face).

After Privacy International **handed** Accenture a "Worst Corporate Invader" award in 2005, its share price has **roughly doubled**. So has **Oracle's** after Larry Ellison was given the sobriquet of "**Greatest Corporate Invader**." After activists **labeled** DoubleClick as uniquely horrible, it was **bought** by Google for a princely $3.1 billion. And so on.

That history raises the obvious question: Why won't people pay for privacy?

"A lot of people have thrown a lot of time, effort, and money into privacy protection business models," says **Jim Harper**, director of information policy studies at the free-market **Cato Institute** who specializes in privacy. "I don't think they understand privacy and I don't think they're likely to succeed."

Harper thinks that privacy is what economists call an "intermediate good," meaning that it's something like steel or a **car** engine, which consumers don't want to buy separately. "People expect it to be built in as a fireplace is built into a house," he says. "They don't want to go shopping for a fireplace when they buy a house."

One possibility, of course, is that Internet users actually don't care about privacy. Yes, they may tell pollsters they do, but more than 70 percent will reveal their computer password in exchange for a chocolate bar, as one BBC **report** described. Another informal survey, as **reported by** CNET News at the time, found that 66 percent of supposedly tech-savvy San Franciscans will give up their passwords (or at least a phrase that might be their password) for a coffee at Starbucks.

Alessandro Acquisti, an associate professor at Carnegie Mellon who researches the behavioral economics of privacy, says: "People want privacy at the same time as they want publicity. This is no contradiction whatsoever. We are complex creatures."

Another explanation is that people once cared more about privacy, and entrepreneurs circa 2000 properly captured that sentiment. But then as the Internet became more familiar, and as social networking sites proliferated, everyone pretty much came to agree that the benefits of disclosure outweighed the privacy risks.

That's what Facebook CEO Mark Zuckerberg believes. In the seven years since he started the company, he **recently said** at a technology conference, "people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people -- and that social norm is just something that has evolved over time."

"For all the talk, the true revealed privacy interests are quite a bit less," says Harper, the Cato Institute analyst. "It doesn't mean that people have no privacy interests -- that they don't care at all -- it means that they're not sensitive to much of the stuff everyone expected them to be sensitive to."

Zuckerberg defended the company's decision in December to **push users to reveal more**, saying "we decided that these would be the social norms now and we just went for it." (Think of it as an updated version of Scott McNealy's **quip** in 1999: "You already have zero privacy--get over it.")

Acquisti, the Carnegie Mellon professor, says that "if you provide a tool that is usable and provides a way to control privacy, to find a right balance, maybe there will be more adoption." He points to laboratory experiments, including those by his colleague **Lorrie Cranor**, that show Internet users were willing to spend "a little more" to buy from a privacy-protecting merchant.

"In some cases, when it's very salient and very easy to understand what level of privacy protection a merchant will offer, a consumer may choose a privacy-protecting merchant," Acquisiti says. "When you face the real world, where there is so much information and more complications, the problem becomes that there are a number of behavioral cognitive biases."

One, he believes, is **hyperbolic discounting**, meaning that Internet users tend to discount the value of protecting their information if the possible privacy benefit is far enough in the future. "You don't realize that that photo of yourself in Cancun, which you're uploading now, will 10 or 15 years later bring down your possibility of being a candidate" for a top political office, Acquisiti says.

But paying for privacy is not the only expense with a payoff years or even decades later. Life insurance is as well. On a car or truck, anti-lock brakes, electronic stability control, active headrests, or features on some Infiniti models like a "**pop-up hood**" used in pedestrian collisions (ignited with a small pyrotechnic charge), surely fall into that category as well. Few car buyers plan on having an accident so damaging those safety mechanisms are needed, but plenty buy them anyway.

Peter Eckersley, a staff technologist at the **Electronic Frontier Foundation**, says on privacy: "There are dozens of companies that are making a garage living or maybe more. The problem is if you choose to do business with one of those companies, there's so little to guarantee you're actually getting real privacy." Online privacy is really hard to achieve, he says, and a programming error you don't know about could expose your personal data to the world.

And in fact it turns out that the privacy-protecting technologies that have prospered are non-commercial. There's Adblock Plus, for which the source code **is available** at no cost. The **Tor** network, which offers reasonably strong anonymity, is free software using a network run by volunteers.

"If you want privacy from a piece of software, you want to be able to see inside it and see how it works," Eckersley says. "You have that level of assurance with open source that you don't have with a Windows executable." He thinks that a for-profit privacy business could sell a service retrospectively: "If there's a way you could fix privacy problems afterwards, there may be a very good business model."

Could a final possibility be that, when it comes to privacy, Internet users have a terribly short memory or a keen appreciation of irony? Take Lexis-Nexis, which the Electronic Privacy Information Center **says** has a "history of wrongfully disclosing consumers' sensitive personal information" and which **sells the Accurint** product that "explores the connections between people" and lets police "instantly locate" someone. Today Lexis-Nexis is one of the sponsors of -- with its logo proudly gracing the home page -- **Data Privacy Day 2010**.

Declan McCullagh is a contributor to CNET News and a correspondent for

CBSNews.com who has covered the intersection of politics and technology for over a decade. Declan writes a regular feature called Taking Liberties, focused on individual and economic rights; you can bookmark his CBS News Taking Liberties site, or subscribe to the RSS feed. You can e-mail Declan at declan@cbsnews.com.