188-5

As Debate On Privacy Heats Up, Sales Don't

By JOHN SCHWARTZ

SOFTWARE that helps Internet users protect their privacy has received a great deal of attention since Sept. 11. Some say the government's new powers to snoop on the Web could lead to a boom for such services. Others say regulators will crack down on these tools, which can help terrorists hide.

So, when Zero-Knowledge Systems announced last month that it was shutting down a service that ensures anonymity for Internet users, speculation ran high that the company had been pressured by law enforcement officials to do so. One participant in a discussion on Slashdot, an online news service frequented by the technoscenti, wrote, "Maybe in the wake of all this terrorist brou-ha-ha about encryption and anonymity, someone (or more likely, some government entity) approached them, and they, ahem, decided to stop."

Hamnett Hill, an executive of Zero-Knowledge, had a more mundane explanation — the company could not make its gold-plated privacy tool pay. Zero-Knowledge's decision came just as another company, Network Associates, said that it was looking for a buyer for a subsidiary, PGP Security, which sells a leading encryption product.

What law enforcement officials have been unable to do, the market has done for them. Bottom-line considerations have dictated that these companies get out of these segments of the privacy business.

These examples underscore a gap between the discussions surrounding the anti-terrorism bill signed by President Bush last month, which have tended to focus on what individuals or terror networks could do, and what business and investigative experience suggested people actually do.

Companies that provide tools that ensure privacy on the Internet have been criticized since the attacks, as security experts and commentators all but accuse them of abetting terrorists by selling tools that can cloak their acts, from encryption to steganography, a more arcane technology that hides messages within pictures.

Investigators working on unraveling the network of terrorists involved in the Sept. 11 attacks, however, have not said whether the suspects used encryption or steganography. Investigators in France said that steganography was used by terrorists who were recently apprehended and planning an attack on the United States Embassy in Paris. But other experts said there were good reasons why these groups had restricted important messages to face-to-face communication.

Lance Cottell, the founder of Anonymizer .com, another company that sells tools for Web visitors to surf anonymously, said that smart terrorists would avoid using encryption, which would stand out in monitored Internet traffic. "So, what you're going to do instead is try to stay under the radar; the last thing you want to do is make yourself conspicuous," he said.

In fact, the investigation so far suggests that terrorist groups use the Internet the same way the rest of the world uses it, to send basic messages and provide information. When federal investigators temporarily shut down the InfoCom Corporation, a Texas company that hosts hundreds of Arab-themed Web sites for organizations around the world, it said that it was determining whether the sites were being used for fund-raising for groups tied to terrorists, like the Palestinian group Hamas.

In writing the new law, Congress stopped short of restricting encryption itself, an action that had been proposed by Senator Judd Gregg, a Republican of New Hampshire. As the government's ability to monitor grows, efforts to limit the ability of companies to watch what their customers do online have stalled. The chairman of the Federal Trade Commission, Timothy J. Muris, said in a speech last month that he would not pursue increased legislative authority over companies that violate users' privacy online, an initiative that had been a priority under the previous administration.

The response from companies that sell privacy tools has been to refine their focus. For instance, Zero-Knowledge announced that it would shut down its top-of-the-line Freedom Network mostly because operating it required the company to maintain the Internet servers on which the service functioned. That is a much larger expense than selling less comprehensive but useful tools to safeguard privacy that customers can run on their own PC's.

The new tools, sold as Freedom 3.0, is for consumers who want help dealing with "the more benign day-to-day threats" to privacy, Mr. Hill said, including banner advertising (which generally relies on "cookie" technology to know which ads to send to which visitors) and computer intrusion by malicious Internet programs like viruses.

"We stopped selling Hummers and started selling 4Runners," Mr. Hill joked. He said that while the new product did not offer the kind of "bulletproof" privacy protection of Freedom Network, it had been well received by customers. (The company does not release figures on sales, profit or loss.)

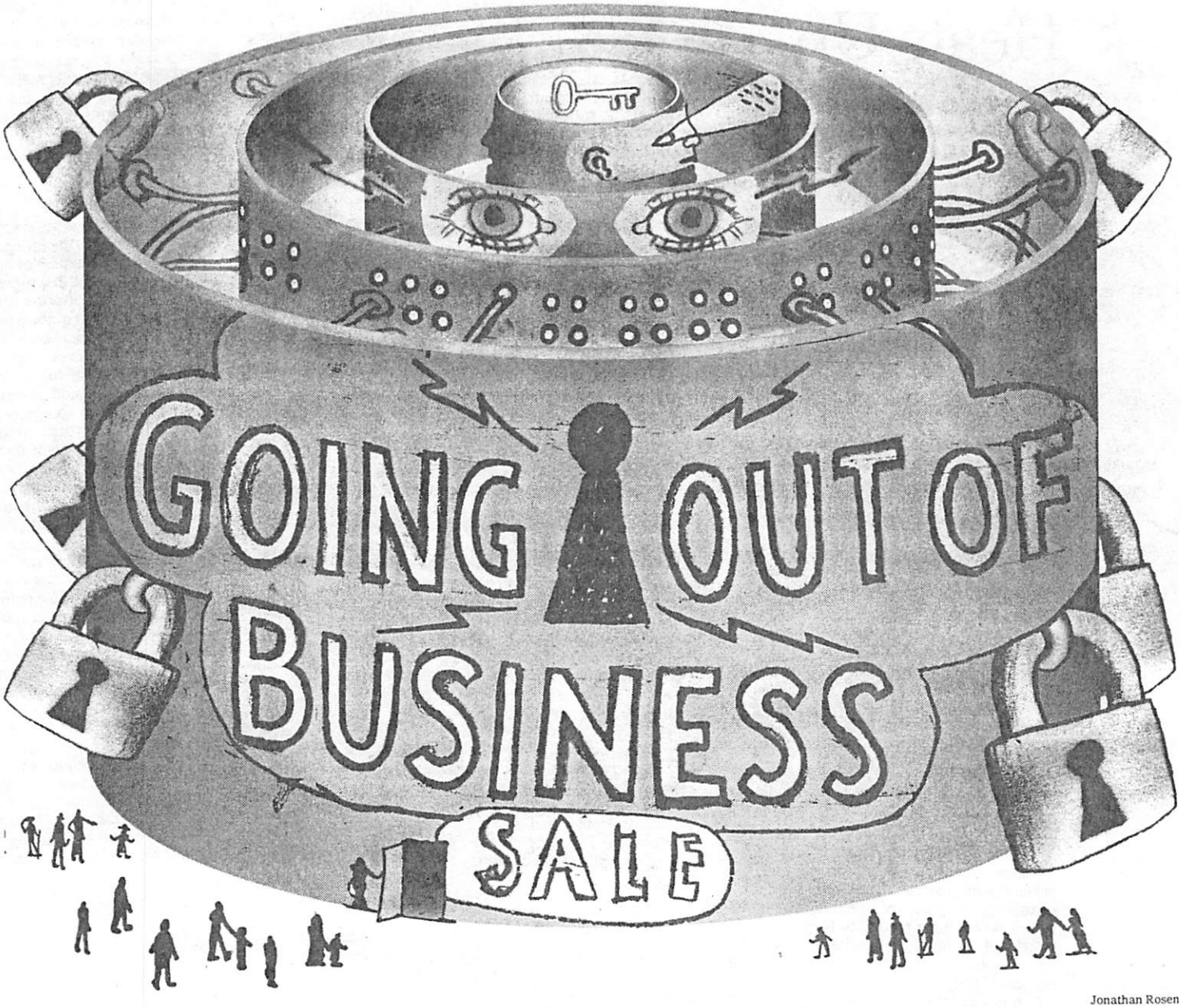
As for Network Associates, the decision to find a buyer for PGP was simple, said Sandra England, the president of the security business unit. "The individual consumers, though they do buy our product, are not our target market," she said.

PGP had its origins in ideology and activism: the tool, which became a landmark, was developed 10 years ago by Phil Zimmermann, a computer programmer who drew the initials from the words "pretty good privacy." After Mr. Zimmermann created the program, it was distributed free over the Internet, attracting scrutiny from law enforcement officials, who suggested that Mr. Zimmermann was violating laws that sharply restricted the export of powerful encryption programs. Mr. Zimmermann later started a company to market a more polished commercial version of the product, then sold it to Network Associates in 1997.

The larger company, however, found that few consumers were willing to spend the money or the time buying and learning a cryptography program. The company does a brisk business selling encryption products to businesses that want to protect data on their central computers, Ms. England said.

The shifts in corporate strategy and moves by the government do not mean that the issue of privacy is going away, Mr. Cottrell said. "In many ways, personal privacy is, if anything, more important than before," he said. His company has tried to show that its products can help law enforcement by creating an anonymous online tip site. Mr. Cottrell says that the police and investigators are "quite heavy users of our service — they use it to keep tabs on the bad-guy sites, without leaving 'FBI.gov' fingerprints on the servers."

Mr. Zimmermann, who now works for Hush Communications, an e-mail company specializing in encryption technology, said that the public would turn to tools like PGP software when it becomes more worried about privacy. At the moment, he said, "There is a lack of awareness among the public." That, he said, is about to change.



Jonathan Rosen