New technology lets users set data to self-destruct

September 30 2009, By Scott Canon

What if you could send an e-mail to a co-worker, text a friend or post something on Facebook confident that it would eventually self-destruct?

So long, immortality. Hello, peace of mind.

Consider the technology that a quartet of computer scientists at the University of Washington introduced to the world in July. It's called Vanish, and it's designed to make your electronic messages do just that.

"With self-destructing data, users can regain control over the lifetimes of their Web objects, such as private messages on Facebook, documents on Google Docs, or private photos on Flickr," the researchers wrote in the paper announcing their work.

They suggested the scenario of a fictitious Anne confiding to a friend the details of her troubled marriage. Anne might want to confide in her buddy, but as soon as the message had been read by that friend it could only pose trouble. Anne's complaints about her husband might later prove embarrassing, damaging in a divorce or an obstacle to reconciliation.

Even if she had used robust encryption, a court order might someday subpoena the key -- and with it, her secrets.

But what if she sent a message encrypted by software, and the key to unlocking it -- an almost impossibly large number -- would be scattered across the Internet?

Inevitably, a piece of the key would become lost over time, erasing hopes of reopening the message at a later date.

Such technology challenges the Digital Age adage that removing something from the Internet is like getting pee out of a swimming pool. In this case, however, some things could actually evaporate in cyberspace.

A trick like that would have spared then-lawmaker Mark Foley from revelation of the sexually loaded text messages he thumbed out to a congressional page. It could mean a college freshman could post drunken half-naked self-portraits without worry that the same images might foul a future job interview. It could mean a new sense of online privacy.

Yet, like almost every new information technology, it poses its share of fresh dilemmas.

Criminals with a touch of computer know-how already can encrypt messages as they plot their schemes. But they could be legally compelled to unlock their messages. With a concept like Vanish, the key to unscrambling the coding would be lost.

"Anything that impedes law enforcement's ability to track e-mails could be a problem," said former FBI agent and security consultant Jeff Lanza.

Even innocent users might need to be careful.

"You can end up with unintended consequences," warned Robert Gezelter, a contributing editor to the Computer Security Handbook.

First, he said, beware of trusting the technology. Just because e-mails or text messages have a limited shelf life doesn't mean their contents will necessarily disappear. The recipients could cut and paste the missives into other files. They could take screen shots. Or they could simply print them out.

Next, he said digital documents are as likely to exonerate as to convict. They can establish alibis, state of mind, knowledge or ignorance of facts that might swing a lawsuit or turn a criminal case.

"It doesn't quite do what you think it does," Gezelter said, "and it does what you don't want it to do."

The self-destroying data remain a seductive idea for people concerned about privacy. Nearly all of us have hit the send button on something we regret -- whether we regretted it immediately or years later.

No less than Google, the behemoth that charts our Internet existence, recognizes that we don't necessarily want to pass on even what we just wrote.

Its Gmail service can promise to routinely delay sending your e-mail for a few seconds while you consider what you're sending. It even offers "mail goggles" to users who don't trust themselves to always be sober enough to man a keyboard, forcing senders to answer math problems before delivering their outgoing e-mail.

Yet firms such as Google also serve as repositories for what many people consider private, with its Web-based e-mail and its so-called cloud computing services that store untold numbers of files in its server farms around the world.

Even when a user deletes a file, it doesn't mean that the company that hosted the file kills it as well, or that it doesn't exist on a backup tape somewhere in the firm's network.

"That's why these self-deleting things could be helpful," said Robert Gellman, a privacy and information policy consultant to government agencies, trade associations and businesses. "There's the question of what happens to your data when you delete it."

Many of the oft-overlooked terms of service for Web-based computing services retain the right to use the data how and when they fit the companies' needs, he said, rather than their customers'. And because data storage is fast becoming so inexpensive, Gellman said it might be cheaper to continue saving digital files than to sort through what to delete and what to keep.

Gellman said you need not be paranoid or criminal to want to keep your secrets. He said someone running for the city council shouldn't be haunted by a text from his teens. Nor should an adult have to worry about a health insurance company sorting through messages to uncover a pre-existing medical condition.

"We have lots of legitimate reasons to protect our privacy," he said.

Even with Vanish, however, it might not be so easy to do.

Two months after Vanish was introduced to the world, computer scientists from the University of Texas, the University of Michigan and Princeton University collaborated to create Unvanish.

Vanish's creators had never actually contended that it would be impossible to revive a self-deleted message, just impractical, and said that it would cost more than $850,000 to comb through enough Internet databases to put the encryption key back together.

But this month the makers of Unvanish said they could make a few computers appear to look like several and gather enough data to restore the key, and the documents it could resuscitate.

Within days, the Vanish creators said they had modified their software, again making it ever harder to crack.

In fact, such jousting matches are at the very heart of the computer security and cryptography fields. Defenses go up. Hackers outwit them. More clever defenses are put in place. And the game goes on.

"As computer scientists, we all want to use the best ideas to build the best systems," said Emmett Witchel, a University of Texas-Austin computer scientist who helped make Unvanish. "We all want to test each other."

• Join PhysOrg.com on Facebook!
• Follow PhysOrg.com on Twitter!

(c) 2009, The Kansas City Star.
Visit The Star Web edition on the World Wide Web at www.kcstar.com
Distributed by McClatchy-Tribune Information Services.

Citation: New technology lets users set data to self-destruct (2009, September 30) retrieved 25 April 2024 from https://phys.org/news/2009-09-technology-users-self-destruct.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.